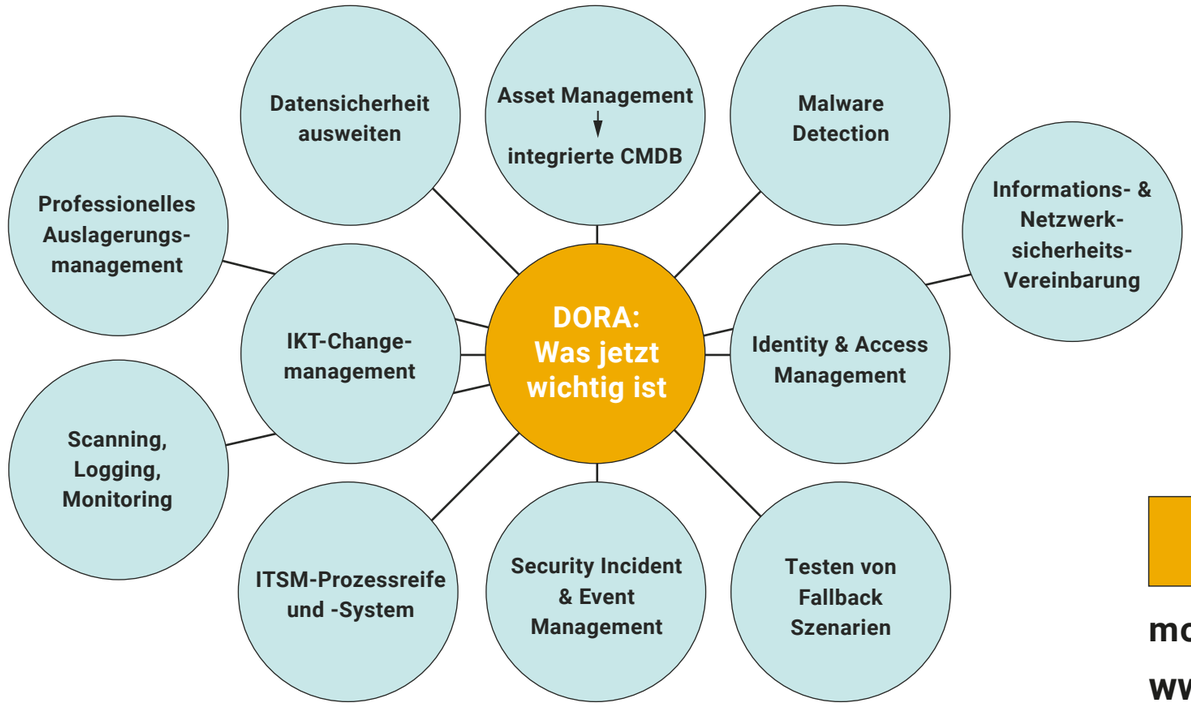
Was ist **DORA?**

DORA (Digital Operational Resilience Act) ist eine EU-Verordnung mit Gesetzescharakter, die im Januar 2025 verbindlich wird. Das Ziel ist, die Cybersicherheit und Risikomanagement im Finanzsektor zu vereinheitlichen, um die Widerstandsfähigkeit von Finanzinstituten gegen Cyberangriffe zu stärken und die Stabilität des Finanzsystems zu gewährleisten.



Sprechen Sie mit unseren Experten

mobility@7p-group.com
www.7p-mobility.com

Die **Kernelemente** von **DORA**

1. IKT-Risikomanagement
Kapitel II, Artikel 5 bis 16

Dieses Kapitel legt den grundlegenden Rahmen für das IKT-Risikomanagement fest und definiert die Verantwortlich-keiten der Unternehmen.

_ IKT-Governance
_ DOR Strategie
_ Risikoprofil
_ IKT-Risikomanagement Tools
_ Leitlinie zur IKT Geschäftsfortführung
_ Verantwortung der Geschäftsleitung
_ Persönliche Haftung
_ Funktion zur Überwachung von IKT-Dienstleistungen
_ Schulungen des Managements
_ Kommunikationsleitlinie
_ Testen von Kommunikationsplänen

2. Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle
Kapitel III, Artikel 17 bis 23

Hier geht es um die Behandlung, Klassifizierung und Meldung von IKT-bezogenen Vorfällen. Unternehmen müssen Vorfälle erkennen, bewerten und entsprechend handeln.

_ Prozess
_ Klassifizierung (kritische oder wichtige Funktionen || schwerwiegender Vorfall?)
_ Wesentlichkeitsschwellen
_ Meldewesen
_ Vorlagen

3. Testen der digitalen operationellen Resilienz einschließlich Threat Led Penetration Testing (TLPT)
Kapitel IV, Artikel 24 bis 27

Dieses Kapitel befasst sich mit der Überprüfung der digitalen Widerstandsfähigkeit, einschließlich der Durchführung von Penetrationstests, um Schwachstellen aufzudecken.

_ Testprogramm
_ Identify, Protect, Detect, Respond, Recover
_ TLPT

4. Management des IKT-Drittparteienrisikos
Kapitel V, Abschnitt I, Artikel 28 bis 30

Unternehmen müssen ihre externen Dienstleister genau unter die Lupe nehmen, um potenzielle Risiken zu erkennen und zu minimieren.

_ Konzentrationsrisiko
_ Vertragsgestaltung, Exitpläne und Tests
_ Überwachung kritischer IKT-Drittdienstleister
_ ITS (Art. 28.9): Informationsregister
_ RTS (Art. 28.10): Nutzung von IKT-Drittdienstleistungen für kritische und wichtige Funktionen
_ RTS (Art. 30.5) Umgang mit Subdienstleistern

5. Überwachungsrahmen für kritische IKT-Drittdienstleister
Kapitel V, Abschnitt II, Artikel 31 bis 44

Wichtige IT-Dienstleister werden besonders genau beobachtet, um sicherzustellen, dass sie hohe Sicherheitsstandards einhalten und Störungen schnell beheben können.

6. Vereinbarungen über den Austausch von Informationen sowie Cyberkrisen- und Notfallübungen
Kapitel VI, Artikel 44 und Kapitel VII, Artikel 49

Zielt darauf ab, die Zusammenarbeit und den Informationsaustausch zwischen Finanzinstituten und zur Aufsicht (z. B. BaFin) zu stärken.