T Security

DORA-Compliance

Operative Resilienz stärken, IKT-Risiken steuern und DORA-Compliance sicherstellen.

Was ist DORA und warum ist es relevant?

Der Digital Operational Resilience Act (DORA) ist der Regulierungsrahmen der Europäischen Union zur Stärkung der Fähigkeit von Finanzinstituten, IKT-Störungen vorzubeugen, darauf zu reagieren und sich davon zu erholen. Da Finanzdienstleistungen heute stark von digitaler Infrastruktur und Drittanbietern abhängig sind, ist operative Resilienz entscheidend für Geschäftskontinuität, Vertrauen und Compliance.

Wer ist von DORA betroffen?

DORA gilt für eine Vielzahl von Finanzunternehmen innerhalb der EU, darunter:

Banken und Kreditinstitute | Versicherungs- und Rückversicherungsunternehmen | Wertpapierfirmen und Handelsplattformen | Zahlungsdienstleister und Fin.Tech-Unternehmen | IKT-Dienstleister für den Finanzsektor.

Die Verordnung erhöht zudem die Verantwortung von Drittanbietern und Technologiepartnern, die an finanziellen Geschäftsprozessen beteiligt sind.

Wie wird die Einhaltung von DORA sichergestellt?

DORA führt strengere Anforderungen an Aufsicht und Verantwortlichkeit für Finanzinstitute sowie IKT-Dienstleister ein.

Die Einhaltung wird durch Aufsichtsbehörden sichergestellt. Diese können Audits durchführen, IKT-Risikomanagement-Frameworks prüfen, Resilienztests bewerten und den Umgang von Unternehmen mit betrieblichen Vorfällen beurteilen. Zudem sind Organisationen verpflichtet, schwerwiegende IKT-Vorfälle innerhalb festgelegter Fristen zu melden.

Sanktionen und Geschäftsauswirkungen

Die Nichteinhaltung von DORA kann zu finanziellen Sanktionen, verstärkter behördlicher Aufsicht, betrieblichen Einschränkungen und Reputationsschäden führen.

Finanzinstitute können mit Geldbußen von bis zu **2% ihres weltweiten Jahresumsatzes** belegt werden. Kritische IKT-Dienstleister müssen bei fortgesetzter Nichteinhaltung mit zusätzlichen Sanktionen und Korrekturmaßnahmen rechnen.

Was wird von Finanzinstituten erwartet?

Von Finanzinstituten wird erwartet, ein strukturiertes Framework für operative Resilienz zu etablieren, das folgende Bereiche umfasst:

- IKT-Risikomanagement und Governance
- Erkennung und Meldung von Vorfällen
- Tests der operativen Resilienz
- Third-party Risiko Management
- Kontinuierliche Überwachung und Kontrolle

Unternehmen müssen die Resilienz ihrer Systeme, Prozesse, Nutzer und externen Dienstleister sicherstellen.

Typische Herausforderungen in Finanzumgebungen

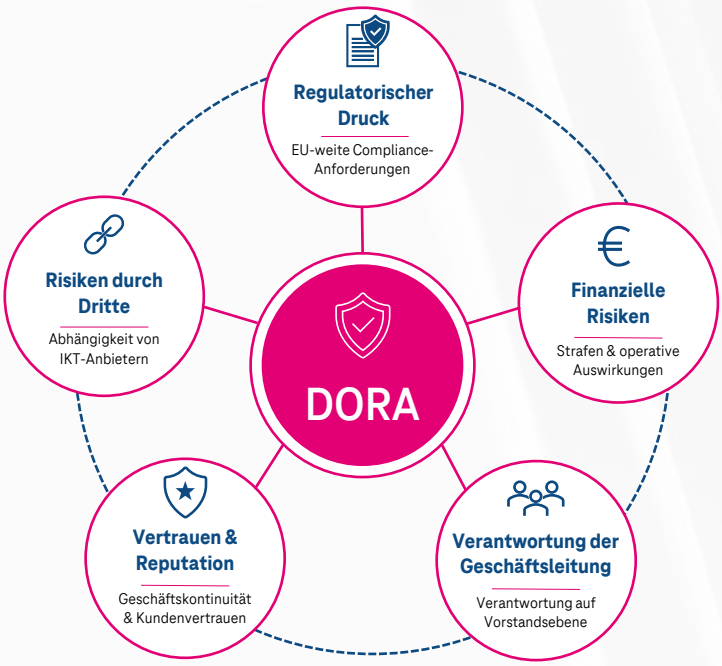
Viele Unternehmen stehen weiterhin vor Herausforderungen wie:

- Eingeschränkte Transparenz über IKT-Systeme und Dienstleister hinweg
- Zunehmende Abhängigkeit von Drittanbietern
- Verzögerte Reaktion auf Vorfälle und mangelnde Koordination
- Uneinheitliche Resilienztests und Governance-Strukturen

Der Weg zur DORA-Compliance

1. **Top-down-Governance und -Strategie etablieren**
   - Risikobereitschaft definieren
   - Verantwortlichkeiten festlegen
2. **Abhängigkeiten erfassen und Assets identifizieren**
   - Implementierung einer CMDB
   - End-to-End-Mapping
3. **Risiko- und Incident-Management etablieren**
   - Kontinuierliches Monitoring
   - Klassifizierung von Vorfällen
   - Regulatorisches Reporting
4. **Bedrohungsorientierte Tests und Geschäftskontinuität sicherstellen**
   - Kontinuität sicherstellen
   - Jährliche Tests
   - Threat-Led Penetration Testing (TLPT)
   - Disaster Recovery
5. **Konzentrationsrisiken bei Drittanbietern steuern**
   - Vertragliche Verantwortlichkeiten
   - Konzentrationsrisiken
   - Ausstiegsstrategien

Warum DORA eine Priorität für Führungskräfte ist



So unterstützt T Security Ihre DORA Readiness

DORA-Readiness Assessment
Compliance-Lücken, IKT-Risiken und operative Abhängigkeiten identifizieren

Sichere IKT-Infrastruktur und Cloud
Resiliente, regelkonforme und sichere digitale Umgebungen aufbauen

Identity and Access Management
Zugriffskontrollen durch Zero-Trust-Prinzipien stärken

Threat Detection and Response
Kontinuierliches Monitoring, Bedrohungserkennung und Incident Response ermöglichen

Compliance & Audit Support
Reporting, Governance und Audit-Readiness vereinfachen

Resilienzplanung
Klare Workflows, Reporting-Prozesse und Wiederherstellungsstrategien im Einklang mit den NIS2-Vorgaben etablieren.

Unsere Expert:innen beraten Sie gerne
cyber.security@t-systems.com

Herausgeber
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn, Germany
security.telekom.de
t-systems.com