

DORA-Artefakt-Landkarte



Auszug aus dem Buch

DORA für Nicht-Finanzexperten

Resilienz-Anforderungen verstehen und umsetzen

Umfang: 180 Seiten

ISBN:

978-3-95444-324-6 (Buch)

978-3-95444-325-3 (E-Book)

Buch: 19,99 EUR

E-Book: 9,99 EUR

More Info: www.brain-media.de

Die folgende Landkarte zeigt die typischen Mindestnachweise, die in DORA-Prüfungen regelmäßig angefordert werden. Entscheidend ist weniger die Menge der Dokumente als deren Konsistenz und Aktualität.

Governance & Risk

- ICT-Risikoregister (aktuell, priorisiert)
- definierte Rollen und Verantwortlichkeiten
- dokumentierte Management-Reviews
- Risiko-Reporting an die Leitungsebene

Incident Management

- klare Incident-Definition und Klassifizierung
- strukturierte Incident-Reports
- getestete Eskalationswege
- Nachweise zu Meldefähigkeit

Third-Party Risk

- konsolidierte Lieferantenübersicht
- Kritikalitätsbewertung
- Transparenz über Sub-Dienstleister
- Nachweis regelmäßigen Monitorings
- Exit-Überlegungen für kritische Services

Technische Resilienz

- Backup-Konzept und aktuelle Restore-Tests
- grundlegendes Security-Monitoring
- Zugriffskontrollen für privilegierte Accounts
- Segmentierungslogik kritischer Komponenten
- Resilienz- bzw. Testplan

Nachweisstruktur

- zentrale Evidence-Ablage
- klare Versionierung
- konsistente Terminologie
- Wiederverwendbare Kundenantworten

Typischer Prüfungs-Reality-Check

Wenn ein Prüfer innerhalb von 60 Minuten keine klare Sicht auf Risiken, Incidents und kritische Lieferanten bekommt, gilt die Organisation meist als unreif — unabhängig von der tatsächlichen Technikqualität.

Weitere nützliche Quellen sind Bestandteil von KaaS
(Knowledge as a Service, <https://www.brain-media.de>).