DORA-Grundverordnung (vereinfachte Übersicht)

frobese × g2c | governance 2 compliance

KAPITEL #1 Allgemeine Bestimmungen

- Geltungsbereich (2*)
- Proportionalitäts-Prinzip (4)

KAPITEL #2 ITK-Risikomanagement

- Governance- und Organisation (5)
- Risiko-Managementrahmen (6 & 15/16)
- Asset-Management (7/8)
- Informationsverbund (7/8)
- resiliente IT-Systeme/ -Protokolle/ -Tools (7)
- Identifizierung (8)
- Schutz und Prävention (9)
- Netzwerksicherheit (9)
- Verschlüsselung und Kryptografie (9)
- Erkennung von Anomalien (Detection) (10)
- Reaktion & Wiederherstellung (Response) (11)
- Backup & Wiederherstellung (Recovery) (12)
- Lernprozesse & Nachsorge (Improvement) (13)
- Kommunikation bei Eskalationen & Krisen (14)
- Harmonisierung Orga, Doku, Prozesse (15)
- vereinfachter Risikomanagementrahmen (16)

DETAILLIERUNG DURCH RTS 2024/1774

KAPITEL #3 Security Incident Mangement

- Security-Incident Prozesse (17)
- Klassifizierung von Cyber-Bedrohungen (18)
- Klassifizierung Security Incidents (18 & 23)
- Meldung von Security Incidents (19 & 23)
- regelmäßiges Reporting zu Sec. Incidents (19)

KAPITEL #4 Testen der digitalen Resilienz

- Identifikation notwendiger Resilienz-Tests (24)
- Planung von Tests (24)
- Roll out und Operationalisierung von Tests (25)
- Threat Led Penetration Tests – TLPT (26)
- Anforderungen an Tester (27)

*** ARTIKEL-REFERENZ IN KLAMMERN**

KAPITEL #5 Risiken von Drittparteien

- Identifikation int. & ext. Zuständigkeiten (28)
- Provider Risiko-Management (28/29)
- Provider-Register (28)
- Provider-Audits (28)
- Provider Exit-Strategie (30)
- Provider-Verträge (30)
- Weiterverlagerung (30)
- kritische Provider (31)
- Überwachungsrahmen (32-42)
- Kostenübernahme von Assessments (43)

DETAILLIERUNG DURCH RTS 2024/1502 UND 2024/1773

KAPITEL #6 Austausch zu Cybergefahren

- Erfahrungsaustausch (45)
- Communities (45)