DORA-Tempel 2.0

- Übersicht über Strategien, Leitlinien, IKT-Sicherheitsrichtlinien und Verfahren -

Strategie
Richtlinie
Leitlinie
Verfahren

Geschäftsstrategie *Art. 6 Abs. 8 lit. a DORA*

Strategie für die digitale operationale Resilienz (DOR-Strategie) *Art. 6 Abs. 8 DORA*

Strategie für das IKT-Drittparteienrisiko *Art. 28 Abs. 2 DORA*

Multi-Vendor-Strategie optional, *Art. 6 Abs. 9 DORA*

Kommunikationsstrategie für IKT-Vorfälle *Art. 14 Abs. 3 i. V. m. Art. 6 Abs. 8 lit. h DORA*

Exitstrategie für kwF-relevante IKT-Dienstleistungen *Art. 28 Abs. 8 DORA i. V. m. Art. 10 RTS TPRM*

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16*	17	18	19	20	21	22	23	24	25	26
Informationssicherheits-leitlinie	IKT-Risikomanagement	IKT-Assetmanagement	Personalsicherheit/ Personalpolitik	Identitätsmanagement	Berechtigungsmanagement	Physische Sicherheit	Verschlüsselung und Kryptografie	Sicherer IKT-Betrieb	Netzwerksicherheit	Schutz von Informationen bei der Übermittlung	Patch- und Update-Management	IKT-Änderungsmanagement	IKT-Projektmanagement	Beschaffung, Entwicklung und Wartung von IKT-Systemen	Beschaffung, Entwicklung und Wartung von IDV	Behandlung IKT-bezogener Vorfälle	Kommunikationsleitlinie (intern und extern)	Allgemeine Geschäftsfortführungsleitlinie	IKT-Geschäftsfort-führungsleitlinie	Datensicherung (Backup)	Programm zum Testen der digitalen Resilienz	Leitlinie zur Behandlung von Feststellungen aus Tests	TLPT-Richtlinie	Leitlinie zur Nutzung von IKT-Dienstleistungen	Leitlinie zur Nutzung kwF-relevanter IKT-Dienstleistungen
Art. 9 Abs. 4 lit. a DORA	Art. 3 RTS RMF	Art. 4 RTS RMF	Art. 19 RTS RMF	Art. 20 RTS RMF	Art. 21 RTS RMF	Art. 18 RTS RMF	Art. 6 und 7 RTS RMF	Art. 8 RTS RMF	Art. 13 RTS RMF	Art. 14 RTS RMF	Art. 9 Abs. 4 lit. f DORA	Art. 9 Abs. 4 lit. e DORA	Art. 15 RTS RMF	Art. 16 Abs. 1 RTS RMF	Art. 16 Abs. 9 RTS RMF	Art. 22 und 23 RTS RMF	Art. 14 Abs. 2 DORA	Art. 11 Abs. 1 und 5 DORA	Art. 11 DORA, Art. 24 RTS RMF	Art. 12 Abs. 1 lit. a DORA	Art. 24 Abs. 1 DORA	Art. 24 Abs. 5 DORA	Art. 26 DORA	Art. 5 Abs. 2 lit. h DORA	Art. 28 Abs. 2 DORA, RTS TPRM
V1	V4		V5	V6		V7	V11	V12	V13	V15		V16		V17		V19	V21		V23					
V2						V8			V14					V18		V20	V22							
V3						V9																			
						V10																			

*praxisnahe Auslegung zu Säule 15

Die Verfahrensdokumente zu den Säulen

V1 IKT-Risikobewertung (Art. 3 lit. b RTS RMF)
V2 IKT-Risikobehandlung (Art. 3 lit. c RTS RMF)
V3 Follow-up-Prozess (Art. 6 Abs. 7 DORA)
V4 IKT-Assetmanagement (Art. 5 RTS RMF)
V5 Identitätsmanagement (Art. 20 Abs. 1 RTS RMF)
V6 Zugangs-/Zugriffsrechte (Art. 9 Abs. 4 lit. c DORA)

V7 Management IKT-Vorgänge (Art. 8 RTS RMF)
V8 Kapazitäts-/Leistungsmgmt. (Art. 9 RTS RMF)
V9 Protokollierung (Art. 12 RTS RMF)
V10 Daten-/Systemsicherheit (Art. 11 RTS RMF)
V11 Netzwerksicherheitsmgmt. (Art. 13 RTS RMF)
V12 Schutz bei Übermittlung (Art. 14 RTS RMF)

V13 Schwachstellenmanagement (Art. 10 Abs. 1 und 2 RTS RMF)
V14 Patch-Management (Art. 10 Abs. 3 und 4 RTS RMF)
V15 IKT-Änderungsmanagement (Art. 9 Abs. 4 lit. e DORA)
V16 Beschaffung/Entw./Wartung (Art. 16 Abs. 2 RTS RMF)
V17 Vorfallmanagementprozess (Art. 17 DORA)
V18 Vorfallsklassifizierung (Art. 17 Abs. 3 lit. b DORA)

V19 IKT-BCM (Art. 11 Abs. 2 DORA)
V20 Krisenkommunikation/ Krisenmanagement (Art. 11 Abs. 7 DORA)
V21 Datensicherung (Art. 12 Abs. 1 lit. a DORA)
V22 Wiedergewinnung/-herst. (Art. 12 Abs. 1 lit. b DORA)
V23 Behebung Feststellungen aus Tests (Art. 24 Abs. 5 DORA)

Eigene Darstellung, zum Teil mit Hilfe von KI