Checkliste: DORA-Dokumentationsanforderungen

Leitner & Associates
Solutions for the financial industry

Dokument	Rechtsgrundlage	Erstellt?	Aktuell?	Umgesetzt?
Strategie	**Rechtsgrundlage**	**Erstellt?**	**Aktuell?**	**Umgesetzt?**
DOR-Strategie	Art. 6 Abs. 8 i.V.m. Art. 5 Abs. 2 lit. d DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Kommunikationsstrategie für IKT-bezogene Vorfälle	Art. 14 Abs. 3 i.V.m. Art. 6 Abs. 8 lit. h DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Strategie für das IKT-Drittparteienrisiko	Art. 28 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
(Optionale) Strategie zur Nutzung mehrerer IKT-Anbieter	Art. 28 Abs. 2 i.V.m. Art. 6 Abs. 9 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Leit-/ Richtlinie	**Rechtsgrundlage**	**Erstellt?**	**Aktuell?**	**Umgesetzt?**
Informationssicherheitsleitlinie	Art. 9 Abs. 4 lit. a DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für das IKT-Risikomanagement	Art. 3 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinie für das Management von IKT-Assets	Art. 4 RTS RMF i.V.m. Art. 9 Abs. 2 und 4 lit. c DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinie für Verschlüsselung und kryptografische Kontrollen	Art. 6 und 7 RTS RMF i.V.m. Art. 9 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für das Management der IKT-Vorgänge (Betrieb)	Art. 8 RTS RMF i.V.m. Art. 9 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für Patches und Updates	Art. 9 Abs. 4 lit. f DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für das Management der Netzwerksicherheit	Art. 13 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien zum Schutz von Informationen bei der Übermittlung	Art. 14 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für das IKT-Projektmanagement (inkl. IKT-Projektrisikobewertung)	Art. 15 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für die Beschaffung, die Entwicklung und die Wartung von IKT-Systemen	Art. 16 Abs. 1 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für das IKT-Änderungsmanagement	Art. 9 Abs. 4 lit. e DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für die physische Sicherheit und die Sicherheit vor Umweltereignissen	Art. 18 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für Personalpolitik	Art. 19 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für das Identitätsmanagement	Art. 20 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien im Rahmen der Kontrolle der Zugangs- und Zugriffsrechte	Art. 21 RTS RMF i.V.m. Art. 9 Abs. 4 lit. c DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
IKT-Geschäftsfortführungsleitlinie	Art. 11 DORA i.V.m. Art. 5 Abs. 2 lit. e und Art. 8 DORA; Art. 24 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für die Datensicherung (Backup)	Art. 12 Abs. 1 lit. a und Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*

Dokument	Rechtsgrundlage	Erstellt?	Aktuell?	Umgesetzt?
Kommunikationsleitlinien für Mitarbeiter (in Bezug auf den IKT-Risikomanagementrahmen)	Art. 14 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Richtlinien für die Behandlung IKT-bezogener Vorfälle	Art. 22 und 23 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Leitlinien zur Priorisierung, Klassifizierung und Behebung aller während der Durchführung der Tests zutage getretenen Probleme	Art. 24 Abs. 5 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer o. wichtiger Funktionen	Art. 28 Abs. 2 und 10 DORA; Art. 1-11 RTS TPPol	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Weitere Dokumentationsanforderungen	**Rechtsgrundlage**	**Erstellt?**	**Aktuell?**	**Umgesetzt?**
Bericht über die Überprüfung des IKT-Risikomanagementrahmens	Art. 6 Abs. 5 DORA i.V.m. Art. 27 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
(IKT-)Revisionspläne inkl. Follow-up Verfahren bei kritischen Erkenntnissen	Art. 6 Abs. 6 und 7 i.V.m. Art. 5 Abs. 2 lit. f DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Inventar aller IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten	Art. 8 Abs. 1 und 6 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Inventar aller (kritischen) Informations- und IKT-Assets	Art. 8 Abs. 1, 4 und 6 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Inventar aller Prozesse, die von IKT-Drittdienstleistern abhängen	Art. 8 Abs. 5 und 6 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren für das IKT-Risikomanagement	Art. 3 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren für das Management von IKT-Assets	Art. 5 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Schutzmaßnahmen für kryptografische Schlüssel	Art. 9 Abs. 4 lit. d DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Register aller Zertifikate und Zertifikatspeicher für diejenigen IKT-Assets, die kritische o. wichtige Funktionen unterstützen	Art. 7 Abs. 4 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren für das Management der IKT-Vorgänge (Betrieb)	Art. 8 RTS RMF i.V.m. Art. 9 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren für das Kapazitäts- und Leistungsmanagement (inkl. Überwachung)	Art. 9 RTS RMF i.V.m. Art. 9 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren für das Schwachstellen-Management	Art. 10 Abs. 1 und 2 RTS RMF i.V.m. Art. 9 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren für das Patch-Management	Art. 10 Abs. 3 und 4 RTS RMF i.V.m. Art. 9 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*

Dokument	Rechtsgrundlage	Erstellt?	Aktuell?	Umgesetzt?
Verfahren für die Daten- und Systemsicherheit	Art. 11 RTS RMF i.V.m. Art. 9 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren, Protokolle und Tools für die Datenaufzeichnung (Logging)	Art. 12 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren, Protokolle und Tools für das Management der Netzwerksicherheit	Art. 13 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren, Protokolle und Tools zum Schutz von Informationen bei der Übermittlung	Art. 14 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren für die Beschaffung, die Entwicklung und die Wartung von IKT-Systemen	Art. 16 Abs. 2 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren und Kontrollen für das IKT-Änderungsmanagement	Art. 9 Abs. 4 lit. e DORA; Art. 17 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren für das Identitätsmanagement	Art. 20 Abs. 1 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren für Zugangs- und Zugriffsrechte	Art. 9 Abs. 4 lit. c DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Erkennungsmechanismen von anomalen Aktivitäten	Art. 10 DORA i.V.m. Art. 23 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
IKT-Geschäftsfortführungspläne (IKT-GFP)	Art. 11 Abs. 6 lit. a DORA; Art. 24 und 25 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Dokumentation der Tests der IKT-GFP	Art. 25 Abs. 5 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
IKT-Reaktions- und Wiederherstellungspläne	Art. 11 Abs. 3 DORA i.V.m. Art. 5 Abs. 2 lit. e DORA; Art. 24 u. 26 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Aufzeichnungen über die Tätigkeiten vor und während Störungen bei Aktivierung der IKT-GFP oder der IKT-Reaktions- und Wiederherstellungspläne	Art. 11 Abs. 8 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren für die Datensicherung (Backup)	Art. 12 Abs. 1 lit. a und Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren, Protokolle und Tools zum Schutz von Informationen bei der Übermittlung	Art. 14 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden	Art. 12 Abs. 1 lit. b und Abs. 2 DORA i.V.m. Art. 11 Abs. 2 lit. c DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Programme zur Sensibilisierung für IKT-Sicherheit	Art. 13 Abs. 6 DORA i.V.m. Art. 5 Abs. 2 lit. g DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Schulungen zur digitalen operationalen Resilienz	Art. 13 Abs. 6 DORA i.V.m. Art. 5 Abs. 2 lit. g DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Kommunikationspläne	Art. 14 Abs. 1 DORA i.V.m. Art. 11 Abs. 2 lit. e, Abs. 6 lit. b und 7 DORA; Art. 24 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Prozess für die Behandlung IKT-bezogener Vorfälle	Art. 17 DORA; Art. 23 RTS RMF	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*

Dokument	Rechtsgrundlage	Erstellt?	Aktuell?	Umgesetzt?
Dokumentation IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen	Art. 17 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Verfahren zur Priorisierung, Klassifizierung und Behebung aller während der Durchführung der Tests zutage getretenen Probleme	Art. 24 Abs. 5 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Validierungsmethoden	Art. 24 Abs. 5 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Informationsregister	Art. 28 Abs. 3 DORA i.V.m. ITS RoI	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Ausstiegspläne	Art. 28 Abs. 8 DORA; Art. 10 RTS TPPol	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Übergreifendes Dokument	**Rechtsgrundlage**	**Erstellt?**	**Aktuell?**	**Umgesetzt?**
Geschäftsstrategie	Art. 6 Abs. 8 lit. a DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
(Allgemeine) Geschäftsfortführungsleitlinie (inkl. BIA)	Art. 11 Abs. 1 und 5 i.V.m. Art. 5 Abs. 2 lit. e DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Programm für die Tests der digitalen operationalen Resilienz	Art. 25 Abs. 1 DORA i.V.m. Art. 24 Abs. 2 DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*
Leitlinie für die Nutzung von IKT-Dienstleistungen	Art. 5 Abs. 2 lit. h DORA	*Ja/Nein*	*Ja/Nein*	*Ja/Teilweise/Nein*