HSW | RECHTSANWÄLTE HARDER SEDLMEIER WEITZEL

DORA Erstmaßnahmen

Nr.	Maßnahme	Schritte	Quelle
Projektvorbereitung und -initialisierung			
1.	Ein Projekt zur Vorbereitung auf die Anwendung der DORA ab Januar 2025 ist aufgesetzt.	Planung Start	*Vorkehrungen zur Umsetzung von DORA in Art. 5 Abs. 2 DORA vorgeschrieben*
2.	Das Projekt ist mit ausreichend Ressourcen und Know-How (extern/intern) besetzt, um die Vorbereitung bis zum 31.12.2024 abzuschließen.	Planung Start	*Wirksames und umsichtiges Management in Art. 5 Abs. 1 DORA vorgeschrieben*
3.	Die Projektleitung berichtet direkt an Vorstand/GF.	Erledigt	*Überwachung durch Leitungsorgan in Art. 5 Abs. 2 DORA vorgeschrieben*
4.	Geschäftsleitung bzw. Vorstand, CIO und leitende Angestellte in der IT sind über die neuen Pflichten, Risiken, Bußgelder und Straftaten nach der DORA ausreichend und umfassend informiert worden.	Erledigt	*Pflicht aus §§ 91 Abs. 2, 161 AktG*
5.	Ein Lenkungsausschuss unter Beteiligung von GF/Vorstand sowie effiziente Terminüberwachung sind implementiert.	Eingerichtet	*Überwachung durch Leitungsorgan in Art. 5 Abs. 2 DORA vorgeschrieben*
6.	Geschäftsführung bzw. Vorstand haben auf Unternehmenswege Meldekanäle eingerichtet, mit denen sie über alle mit IKT-Drittdienstleistern geschlossene Verträge und deren geplante wesentliche Änderung informiert werden sowie die Auswirkungen gemäß Art. 5 Abs. 2 lit. i) iii) DORA	Eingerichtet	*Ausdrücklich vorgeschrieben in Art. 5 Abs. 2 lit. i) DORA.*
7.	Die interne Revision bzw. Compliance begleitet das Vorbereitungsprojekt, übernimmt regelmäßige Prüfungen und erstellt eine Findings List.	Aufgesetzt	*Art. 6 Abs. 6 DORA schreibt regelmäßige Revisionen vor, deshalb am besten frühzeitig beteiligen*
8.	Zur Vermeidung von Drohverlustrückstellungen werden Informationen zum Projekt, Revisionsbericht und Findings List mit Steuerberatern / Wirtschaftsprüfern ausgetauscht.	Erledigt	*Zur Vorbereitung des Risikoabschnittes im Lagebericht (§§ 289, 321 Abs. 4 HGB) und zur Prüfung des Risikoüberwachungs-systems, § 317 Abs. 4 HGB*

Nr.	Maßnahme	Schritte	Quelle
Vorbereitung der Unternehmensorganisation			
9.	Vorstand/GF haben die unabhängige Kontrollfunktion zur Überwachung des IKT-Risikos eingerichtet	Konzept Eingerichtet	*Art. 6 Abs. 4 DORA, Ausnahme: Kleinstunternehmen*
10.	Interne Revision ist mit ausreichend Wissen und Fähigkeiten im Bereich IKT-Risiken ausgestattet	Lücken identifiziert Lücken geschlossen	*Art. 6 Abs. 6 DORA*
11.	Bei AG: Aufsichtsrat bzw. dessen Prüfungsausschuss für Risikomanagement ist eingebunden	Angefragt Umgesetzt	*Folgt aus § 116 i.V.m. § 93 sowie § 107 Abs. 3 AktG*
12.	Strenge Unabhängigkeit der Kontrollfunktionen nach Modell der drei Verteidigungslinien sichergestellt	Umgesetzt	*Art. 6 Abs. 4 und 6 DORA*
13.	Schulungsmaßnahmen für ausreichende Fähigkeiten und Kenntnisse des Leitungsorganes geplant und aufgesetzt	Bedarf analysiert Schulungsplan	*Art. 5 Abs. 4 DORA*
14.	Ausreichend Ressourcen und Kapazitäten zur Überwachung von Nutzeraktivitäten und das Auftreten von IKT-Anomalien und IKT-Vorfällen	Konzept Verabschiedet Eingerichtet	*Art. 10 Abs. 3 DORA*
15.	*Außer Kleinstunternehmen:* Krisenmanagementfunktion zur Festlegung klarer Verfahre für Abwicklung interner und externer Krisenkommunikation gemäß Art. 14 DORA	Konzept Verabschiedet Eingerichtet	*Art. 11 Abs. 7 DORA*
16.	*Nur Zentralverwahrer:* Mindestens ein sekundärer Verarbeitungsstandort gemäß Art. 12 Abs. 5 DORA	Geplant Operativ	*Art. 12 Abs. 5 DORA*
17.	Ausreichend Kapazitäten und Personal, um Informationen über Schwachstellen und Cyberbedrohungen, IKT-Vorfälle, insbesondere Cyberangriffe, zu sammeln und ihre wahrscheinlichen Auswirkungen auf digitale operative Resilienz zu untersuchen	Konzept Verabschiedet Eingerichtet	*Art. 13 Abs. 1 DORA*
18.	Mindestens eine Person mit Umsetzung der Kommunikationsstrategie für IKT-bezogene Vorfälle beauftragt	Beauftragt	*Art. 14 Abs. 3 DORA*
19.	Meldewesen für schwerwiegende IKT-Vorfälle an zuständige Behörde	Eingerichtet	*Art. 19 Abs. 1 DORA*

Nr.	Maßnahme	Schritte	Quelle
20.	Mechanismen zur Information über schwerwiegende IKT-Vorfälle mit Auswirkungen auf finanzielle Interessen von Kunden (inkl. deren Prüfung) und ergriffene Maßnahmen an Kunden	Eingerichtet	*Art. 19 Abs. 3 DORA*
21.	Mechanismen zur Information potenziell betroffener Kunden über angemessene Schutznahmen, die jene ergreifen können, wenn erhebliche Cyberbedrohungen vorliegen	Eingerichtet	*Art. 19 Abs. 3 DORA*
22.	*Vorstand und AR:* Regelmäßige Prüfung von Risiken im Zusammenhang mit den vertraglichen Vereinbarungen über Nutzung von IKT-Dienstleistungen und zur Unterstützung kritischer oder wichtiger Funktionen	Konzept Verabschiedet Eingerichtet	*Art. 28 Abs. 2 DORA*
23.	*Einkauf:* Berichtswesen zur Übermittlung der Anzahl neuer Vereinbarungen über IKT-Dienstleistungen sowie über zeitnahe Unterrichtung über jede geplante vertragliche Vereinbarung über IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß Art. 28 Abs. 3 DORA an zuständige Behörden	Konzept Verabschiedet Eingerichtet	*Art. 28 Abs. 3 DORA*
24.	*Einkauf:* Prozesse zur Beurteilung, Ermittlung und Bewertung vor Abschluss von Verträgen über IKT-Dienstleistungen gemäß Art. 28 Abs. 4 und 5 DORA	Konzept Verabschiedet Eingerichtet	*Art. 28 Abs. 4 und 5 DORA*
25.	*Bei Bedarf:* Einrichtung/Ausbau von Auditfunktionen für IKT-Dienstleistern gemäß Anforderungen von Art. 28 Abs. 6 DORA	Konzept Verabschiedet Eingerichtet	*Art. 28 Abs. 6 DORA*
26.	*Einkauf:* Einführung der Ermittlung und Bewertung des IKT-Konzentrationsrisikos gemäß Art. 29 Abs. 1, 28 Abs. 4 lit. c DORA	Konzept Verabschiedet Eingerichtet	*Art. 29 Abs. 1, 28 Abs. 4 lit. c) DORA*
Budget- und Ressourcenplanung			
27.	Geschäftsführung bzw. Vorstand hat angemessene Budgetmittel für das Vorbereitungsprojekt und die laufenden DORA-Anforderungen zugewiesen	Mittel geplant Bereitgestellt	*Art. 5 Abs. 2 lit. g) DORA*

Nr.	Maßnahme	Schritte	Quelle
28.	Anpassungen an Segmentierung und Abschottung der Netzinfrastruktur (HW, SW und DL) sind geplant	Mittel geplant Bereitgestellt	*Art. 9 Abs. 3 DORA*
29.	Anpassung an Mechanismen zur frühzeitigen Erkennung von Anomalien und Leistungsengpässen sind geplant	Mittel geplant Bereitgestellt	*Art. 10 Abs. 1 DORA*
30.	Ausreichend Ressourcen und Kapazitäten zur Überwachung von Nutzeraktivitäten und das Auftreten von IKT-Anomalien und IKT-Vorfällen sind geplant	Mittel geplant Bereitgestellt	*Art. 10 Abs. 3 DORA*
31.	Mittel zur Aufzeichnung von und jederzeitigen Einsicht in Tätigkeiten nach Aktivierung von IKT-Geschäftsführungsplänen oder IKT-Reaktions- und Wiederherstellungsplänen	Mittel geplant Bereitgestellt	*Art. 11 Abs. 8 DORA*
32.	Datensicherungssysteme gemäß Art. 12 DORA	Mittel geplant Bereitgestellt	*Art. 12 Abs. 2 DORA*
33.	Systeme zur Wiedergewinnung von Daten, die vom Quellsystem physisch und logisch getrennt sind	Mittel geplant Bereitgestellt	*Art. 12 Abs. 3 DORA*
34.	Sicherer Schutz der Systeme zur Wiedergewinnung von Daten vor unbefugtem Zugriff und IKT-Manipulation	Mittel geplant Bereitgestellt	*Art. 12 Abs. 3 DORA*
35.	*Nur für Datenbereitstellungsdienste:* Angemessene Ressourcen und Sicherungs- und Wiederherstellungseinrichtungen, um Dienste jederzeit anzubieten und aufrechtzuerhalten	Mittel geplant Bereitgestellt	*Art. 12 Abs. 3 DORA*
36.	*Bis auf Kleinstunternehmen mit geringem Risikoprofil:* Redundanz aller IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen zur Deckung des Geschäftsbedarfs	Mittel geplant Bereitgestellt	*Art. 12 Abs. 4 DORA*
37.	*Nur Zentralverwahrer:* Mindestens ein sekundärer Verarbeitungsstandort gemäß Art. 12 Abs. 5 DORA	Mittel geplant Bereitgestellt	*Art. 12 Abs. 5 DORA*
38.	Kapazitäten und Personal, um Informationen über Schwachstellen und Cyberbedrohungen, IKT-Vorfälle, insbesondere Cyberangriffe, zu sammeln und ihre wahrscheinlichen Auswirkungen auf digitale operative Resilienz zu untersuchen	Mittel geplant Bereitgestellt	*Art. 13 Abs. 1 DORA*

Nr.	Maßnahme	Schritte	Quelle
39.	Ausreichend komplexe, obligatorische Programme der Mitarbeiterschulung zur Sensibilisierung für IKT-Sicherheit und digitalen operationellen Resilienz	Mittel geplant Bereitgestellt	*Art. 13 Abs. 6 DORA*
40.	Solides und umfassendes Programm für das Testen der digitalen operationellen Resilienz (kostet ein großes Versicherungsunternehmen allein 30 Mio € p.a.) Außer bei Kleinstunternehmen: Durch unabhängige, interne oder externe Parteien	Mittel geplant Bereitgestellt	*Art. 24 Abs. 1 DORA*
41.	Ersterstellung Informationsregister über alle vertraglichen Vereinbarungen mit IKT-Drittdienstleistern	Mittel geplant Bereitgestellt	*Art. 28 Abs. 3 DORA*
42.	Berichtswesen zur Übermittlung der Anzahl neuer Vereinbarungen über IKT-Dienstleistungen sowie über zeitnahe Unterrichtung über jede geplante vertragliche Vereinbarung über IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß Art. 28 Abs. 3 DORA an zuständige Behörden	Mittel geplant Bereitgestellt	*Art. 28 Abs. 3 DORA*
43.	Prozesse zur Beurteilung, Ermittlung und Bewertung vor Abschluss von Verträgen über IKT-Dienstleistungen gemäß Art. 28 Abs. 4 und 5 DORA	Mittel geplant Bereitgestellt	*Art. 28 Abs. 4 und 5 DORA*
44.	*Bei Bedarf:* Einrichtung/Ausbau von Auditfunktionen für IKT-Dienstleistern gemäß Anforderungen von Art. 28 Abs. 6 DORA	Mittel geplant Bereitgestellt	*Art. 28 Abs. 6 DORA*
Dokumentation			
45.	Umfassende IKT-Geschäftsfortführungsleitlinie als eigenständige spezielle Leitlinie	Entwurf Verabschiedet	*Art. 11 Abs. 1 DORA*
46.	*Als Teil der IKT-Geschäftsfortführungsleitlinie:* Spezielle Pläne für Eindämmungsmaßnahmen, Prozesse und Technologien für IKT-bezogene Vorfälle und Vermeidung weiterer Schäden	Entwurf Verabschiedet	*Art. 11 Abs. 2 lit. c) DORA*
47.	*Als Teil der IKT-Geschäftsfortführungsleitlinie:* Maßgeschneiderte Verfahren zur Reaktion und Wiederherstellung gemäß Art. 12 DORA	Entwurf Verabschiedet	*Art. 11 Abs. 2 lit. c) DORA*

Nr.	Maßnahme	Schritte	Quelle
48.	*Als Teil der IKT-Geschäftsfortführungsleitlinie:* Kommunikations- und Krisenmanagement-maßnahmen zur effektiven Informations-übermittlung gemäß Art. 14 und Meldung an zuständige Behörden gemäß Art. 19 DORA	Entwurf Verabschiedet	*Art. 11 Abs. 2 lit. e), Art. 14 Abs. 1 DORA*
49.	IKT-Reaktions- und Wiederherstellungspläne	Entwurf Verabschiedet	*Art. 11 Abs. 3 DORA*
50.	Business-Impact-Analyse (BIA) der bestehenden Risiken für schwerwiegende Betriebsstörungen	Entwurf Verabschiedet	*Art. 11 Abs. 5 DORA*
51.	Richtlinien und Verfahren für die Datensicherung	Entwurf Verabschiedet	*Art. 12 Abs. 1 lit a) DORA*
52.	Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung von Daten	Entwurf Verabschiedet	*Art. 12 Abs. 1 lit b) DORA*
53.	*Für IKT-Systeme und Daten mit minimaler Ausfallzeit:* Zeitvorgaben für Wiederherstellungszeit und Wiederherstellungspunkte jeder Funktion zur Sicherstellung der vereinbarten Dienstleistungsgüte in Extremszenarien	Entwurf Verabschiedet	*Art. 12 Abs. 6 DORA*
54.	Entwicklung der IKT-Risiken im Zeitverlauf, insbesondere Häufigkeit, Art, Ausmaß und Entwicklung von IKT-Vorfällen um Risikoausmaß zu verstehen und Cyberreife und Abwehrbereitschaft des Unternehmens zu verbessern	Entwurf Verabschiedet	*Art. 13 Abs. 4 DORA*
55.	Ausreichend komplexe, obligatorische Programme der Mitarbeiterschulung zur Sensibilisierung für IKT-Sicherheit und digitalen operationellen Resilienz	Entwurf Verabschiedet	*Art. 13 Abs. 6 DORA*
56.	*Außer Kleinstunternehmen:* Ergebnisse der Überwachung einschlägiger technischer Entwicklungen und neuester Prozesse für IKT-Risikomanagement zur wirksamen Abwehr von Cyberangriffen	Entwurf Verabschiedet	*Art. 13 Abs. 7 DORA*
57.	Prozess für die Behandlung IKT-bezogener Vorfälle	Entwurf Verabschiedet	*Art. 17 Abs. 1 DORA*
58.	Prozess für die Erfassung von IKT-Vorfällen und erheblichen Cyberbedrohungen mit allen Anforderungen nach Art. 17 Abs. 3 DORA	Entwurf Verabschiedet	*Art. 17 Abs. 2 DORA*
59.	Klassifizierung von IKT-Vorfällen und Bestimmung ihrer Auswirkungen nach Kriterien in Art. 18 Abs. 1 DORA	Entwurf Verabschiedet	*Art. 18 Abs. 1 DORA*

Nr.	Maßnahme	Schritte	Quelle
60.	Einstufung von Cyberbedrohungen nach Kritikalität gemäß Art. 18 Abs. 2 DORA	Entwurf Verabschiedet	*Art. 18 Abs. 2 DORA*
61.	Details zum Meldewesen für schwerwiegende IKT-Vorfälle an zuständige Behörde	Entwurf Verabschiedet	*Erforderlich für Art. 19 Abs. 1 DORA*
62.	Mechanismen zur Information über schwerwiegende IKT-Vorfälle mit Auswirkungen auf finanzielle Interessen von Kunden (inkl. deren Prüfung) und ergriffene Maßnahmen an Kunden	Konzept Verabschiedet	*Art. 19 Abs. 3 DORA*
63.	Mechanismen zur Information potenziell betroffener Kunden über angemessene Schutznahmen, die jene ergreifen können, wenn erhebliche Cyberbedrohungen vorliegen	Konzept Verabschiedet	*Art. 19 Abs. 3 DORA*
64.	Solides und umfassendes Programm für das Testen der digitalen operationellen Resilienz gemäß Art. 25 bis 27 DORA	Entwurf Verabschiedet	*Art. 24 Abs. 1 DORA*
65.	*Außer Kleinstunternehmen:* Verfahren und Leitlinien zur Priorisierung, Klassifizierung und Behebung aller bei Tests der digitalen operationellen Resilienz gemäß Art. 25 bis 27 DORA auftretenden Probleme	Entwurf Verabschiedet	*Art. 24 Abs. 5 DORA*
66.	*Außer Kleinstunternehmen:* Interne Validierungsmethoden um sicherzustellen, dass alle bei Tests der digitalen operationellen Resilienz gemäß Art. 25 bis 27 DORA ermittelten Schwächen, Mängel oder Lücken vollständig angegangen werden	Entwurf Verabschiedet	*Art. 24 Abs. 5 DORA*
67.	Strategie für das IKT-Drittparteienrisiko mit einer Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die durch IKT-Drittdienstleister bereitgestellt werden	Entwurf Beschlossen	*Art. 28 Abs. 2 DORA*
68.	Informationsregister über alle vertraglichen Vereinbarungen mit IKT-Drittdienstleistern mit angemessener Dokumentation	Entwurf Fertiggestellt	*Art. 28 Abs. 3 DORA*
69.	Auditplan inkl. Art und Frequenz von IKT-Dienstleister-Audits auf Grundlage risikobasierten Ansatzes	Entwurf Fertiggestellt	*Art. 28 Abs. 6 DORA*
70.	IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen	Identifiziert	*Art. 28 Abs. 8 DORA* *Art. 29 Abs. 2 DORA*

Nr.	Maßnahme	Schritte	Quelle
71.	Ausstiegsstrategie für alle IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen	Entwurf Fertiggestellt	*Art. 28 Abs. 8 DORA*
72.	Umfassend dokumentierte Ausstiegspläne für alle IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen	DL identifiziert Pläne erstellt	*Art. 28 Abs. 8 DORA*
73.	Planung von Alternativlösungen und Übergangsplänen, um IKT-Dienstleistern Dienstleistungen und Daten zu entziehen und sicher und vollständig an andere Dienstleister oder in eigene Systeme zu überführen	Entwurf Fertiggestellt	*Art. 28 Abs. 8 DORA*
74.	Angemessene Notfallmaßnahmen zur Fortführung der Geschäftstätigkeit wenn bei IKT-Drittdienstleistern Risiken oder Fehler auftreten	Entwurf Verabschiedet	*Art. 28 Abs. 8 DORA*
Krisenmanagement			
75.	Mechanismen zur Aufzeichnung von und jederzeitigen Einsicht in Tätigkeiten nach Aktivierung von IKT-Geschäftsführungsplänen oder IKT-Reaktions- und Wiederherstellungsplänen	Eingerichtet	*Art. 11 Abs. 8 DORA*
76.	Prozess für die Behandlung IKT-bezogener Vorfälle	Eingerichtet	*Art. 17 Abs. 1 DORA*
77.	Prozess für die Erfassung von IKT-Vorfällen und erheblichen Cyberbedrohungen mit allen Anforderungen nach Art. 17 Abs. 3 DORA	Eingerichtet	*Art. 17 Abs. 2 DORA*
Anpassung von Verträgen mit IKT-Providern			
78.	Vereinbarung von Tests der IKT-Geschäftsfortführungspläne mit Providern, die kritische oder wichtige Funktionen übernehmen	Provider identifiziert Verträge angepasst	*Art. 11 Abs. 4 DORA*
79.	Vereinbarung von Zeitvorgaben für Wiederherstellungszeit und Wiederherstellungspunkte jeder Funktion zur Sicherstellung der vereinbarten Dienstleistungsgüte in Extremszenarien	Provider identifiziert Verträge angepasst	*Art. 12 Abs. 6 DORA*
80.	Ausreichend Zugangs-, Inspektions- und Auditrechte entsprechend dem Auditplan	Provider identifiziert Verträge angepasst	*Art. 28 Abs. 6 DORA*
81.	Sicherstellung von Sonderkündigungsrechten gemäß Art. 28 Abs. 7 DORA	Provider identifiziert Verträge angepasst	*Art. 28 Abs. 7 DORA*

Nr.	Maßnahme	Schritte	Quelle
82.	Vereinbarung von Exit-Support und Übergangszeiträumen gemäß Art. 28 Abs. 8 und 30 Abs. 3 lit. f) DORA bei IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen	Provider identifiziert Exit-Support definiert Verträge angepasst	*Art. 28 Abs. 8 DORA* *Art. 30 Abs. 3 lit. f) DORA*
83.	*Bei allen Verträgen über kritische oder wesentliche Funktionen:* Abwägung der Risiken einer zugelassenen Untervergabe mit entsprechenden Vorgaben an Hauptunternehmer mit entsprechenden Vorgaben	Provider identifiziert Abwägung durchgeführt Verträge angepasst	*Art. 29 Abs. 2, 30 Abs. 2 lit a) DORA*
84.	Eindeutige, schriftliche Zuweisung von Rechten und Pflichten in jedem Vertrag mit IKT-Drittdienstleistern (= vollständige, detaillierte Leistungsbeschreibung)	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 1 und 2 lit. a) DORA*
85.	Genaue Vereinbarung zu Standorten (Regionen/Länder), an denen IKT-Dienstleistungen bereitzustellen sind, Daten verarbeitet oder gespeichert werden sowie Pflicht zur Vorabnachricht bei Änderung dieser Standorte	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 2 lit. b) DORA*
86.	Genaue Vereinbarung zu Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf Datenschutz und Datensicherheit (Vorsicht: weitergehend als DSGVO-Anforderungen!)	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 2 lit. c) DORA*
87.	Genaue Vereinbarung zur Sicherstellung des Zugangs zu Daten bei Insolvenz, Abwicklung oder Ausfällen des IKT-Drittdienstleisters (erfordert meist Escrow-Vereinbarungen!)	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 2 lit. d) DORA*
88.	Vereinbarung zur Dienstleistungsgüte (= SLA) einschließlich Aktualisierung und Überarbeitung	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 1 und 2 lit. e) DORA*
89.	Vereinbarung zu Unterstützungsleistungen bei IKT-Vorfällen bei vertragsrelevanten Dienstleistungen	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 2 lit. f) DORA*

Nr.	Maßnahme	Schritte	Quelle
90.	Vereinbarung zu vollumfänglicher Zusammenarbeit mit zuständigen DORA-Behörden	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 2 lit. g) DORA*
91.	Prüfung und Anpassung von Kündigungsrechten und Mindestkündigungsfristen gemäß Art. 30 Abs. 2 lit h) DORA	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 2 lit. h) DORA*
92.	Vereinbarung von Bedingungen für Teilnahme an Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationellen Resilienz	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 2 lit. i) DORA*
93.	*Bei Verträgen zur Unterstützung kritischer oder wichtiger Funktionen:* SLA mit präzisen quantitativen und qualitativen Leistungszielen, wirksame Überwachung (Reporting!) und Korrekturmaßnahmen bei SLA-Verletzung	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 3 lit. a) DORA*
94.	*Bei Verträgen zur Unterstützung kritischer oder wichtiger Funktionen:* Kündigungsfristen, Melde- und Berichtspflichten zu Entwicklungen beim IKT-Drittdienstleister, die sich wesentlich auf dessen Fähigkeit zur Vertragserfüllung auswirken könnten	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 3 lit. b) DORA*
95.	*Bei Verträgen zur Unterstützung kritischer oder wichtiger Funktionen:* Implementierung und Tests von Notfallplänen und ausreichend Sicherheitsmaßnahmen	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 3 lit. c) DORA*
96.	*Bei Verträgen zur Unterstützung kritischer oder wichtiger Funktionen:* Pflicht zur Beteiligung und uneingeschränkten Mitwirkung an TLPTs	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 3 lit. d) DORA*
97.	*Bei Verträgen zur Unterstützung kritischer oder wichtiger Funktionen:* Umfassende Audit- und Überwachungsrechte nach Art. 30 Abs. 3 lit. e) DORA	Provider identifiziert Gap-Analyse Verträge angepasst	*Art. 30 Abs. 3 lit. e) DORA*

Nr.	Maßnahme	Schritte	Quelle
Testplanung			
98.	Regelmäßige Tests der Mechanismen zur frühzeitigen Erkennung von Anomalien und Leistungsengpässen gemäß Art. 25 DORA sind geplant	Plan erstellt	*Art. 10 Abs. 1 DORA*
99.	1x jährlich sowie bei jeder wesentlichen Änderung an IKT-Systemen: IKT-Geschäftsführungsplan, insbesondere in Bezug auf ausgelagerte kritische/wichtige Funktionen	Plan erstellt	*Art. 11 Abs. 4 sowie Art. 11 Abs. 6 lit. a) DORA*
100.	1x jährlich sowie bei jeder wesentlichen Änderung an IKT-Systemen: IKT-Reaktions- und Wiederherstellungspläne	Plan erstellt	*Art. 11 Abs. 4 sowie Art. 11 Abs. 6 lit. a) DORA*
101.	Krisenkommunikationspläne nach Art. 14 DORA	Plan erstellt	*Art. 11 Abs. 4 sowie Art. 11 Abs. 6 lit. b) DORA*
102.	Mechanismen zur Aufzeichnung von und jederzeitigen Einsicht in Tätigkeiten nach Aktivierung von IKT-Geschäftsführungsplänen oder IKT-Reaktions- und Wiederherstellungs-plänen gemäß Art. 11 Abs. 8 DORA	Plan erstellt	*Nicht vorgeschrieben, aber sinnvoll*
103.	Regelmäßig: Datensicherungssysteme gemäß Art. 12 DORA	Plan erstellt	*Art. 12 Abs. 2 DORA*
104.	Mehrfachprüfungen und Abgleiche, um größtmögliche Datenintegrität bei Wiederherstellung nach IKT-Vorfällen sicherzustellen	Plan erstellt	*Art. 12 Abs. 7 DORA*
105.	Prozess für die Behandlung IKT-bezogener Vorfälle	Plan erstellt	*Letztlich aus Art. 17 Abs. 1 DORA*
106.	Prozess für die Erfassung von IKT-Vorfällen und erheblichen Cyberbedrohungen mit allen Anforderungen nach Art. 17 Abs. 3 DORA	Plan erstellt	*Letztlich aus Art. 17 Abs. 2 DORA*
107.	Meldung schwerwiegender IKT-Vorfälle an zuständige Behörde	Plan erstellt	*Nicht zwingend, aber sinnvoll zur Einhaltung von Art. 19 Abs. 1 DORA*
108.	Information über schwerwiegende IKT-Vorfälle mit Auswirkungen auf finanzielle Interessen von Kunden (inkl. deren Prüfung) und ergriffene Maßnahmen an Kunden	Plan erstellt	*Nicht zwingend, aber sinnvoll zur Einhaltung von Art. 19 Abs. 3 DORA*
109.	Mechanismen zur Information potenziell betroffener Kunden über angemessene Schutznahmen, die jene ergreifen können, wenn erhebliche Cyberbedrohungen vorliegen	Plan erstellt	*Nicht zwingend, aber sinnvoll zur Einhaltung Art. 19 Abs. 3 DORA*

Nr.	Maßnahme	Schritte	Quelle
110.	Solides und umfassendes Programm für das Testen der digitalen operationellen Resilienz gemäß Art. 25 bis 27 DORA	Entwurf Verabschiedet	*Art. 24 Abs. 1 DORA*
111.	Außer Kleinstunternehmen: 1xjährlich angemessene Tests aller IKT-Systeme und -Anwendungen, die kritische oder wichtige Funktionen unterstützen	Plan erstellt	*Folge aus Art. 24 Abs. 6 DORA*
112.	Ausreichende Tests der Ausstiegspläne für alle IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen	Plan erstellt	*Art. 28 Abs. 8 DORA*
Planung der Prüfung und Aktualisierung von Dokumenten			
113.	IKT-Geschäftsfortführungsleitlinie	Plan erstellt	*Art. 11 Abs. 6 DORA*
114.	Business-Impact-Analyse (BIA) der bestehenden Risiken für schwerwiegende Betriebsstörungen	Plan erstellt	*Nicht vorgeschrieben, aber letztlich erforderlich*
115.	IKT-Reaktions- und Wiederherstellungspläne	Plan erstellt	*Art. 11 Abs. 6 DORA*

DORA Fortlaufende Maßnahmen nach Ersteinrichtung

Nr.	Maßnahme	Schritte	Quelle
Prüfung durch GF/Vorstand			
1.	Regelmäßig: Risiken im Zusammenhang mit den vertraglichen Vereinbarungen über Nutzung von IKT-Dienstleistungen und zur Unterstützung kritischer oder wichtiger Funktionen		*Art. 28 Abs. 2 DORA*
Tests			
2.	Regelmäßige Tests der Mechanismen zur frühzeitigen Erkennung von Anomalien und Leistungsengpässen gemäß Art. 25 DORA sind geplant		*Art. 10 Abs. 1 DORA*
3.	1x jährlich sowie bei jeder wesentlichen Änderung an IKT-Systemen: IKT-Geschäftsführungsplan, insbesondere in Bezug auf ausgelagerte kritische/wichtige Funktionen		*Art. 11 Abs. 4 sowie Art. 11 Abs. 6 lit. a) DORA*
4.	1x jährlich sowie bei jeder wesentlichen Änderung an IKT-Systemen: IKT-Reaktions- und Wiederherstellungspläne		*Art. 11 Abs. 4 sowie Art. 11 Abs. 6 lit. a) DORA*
5.	Krisenkommunikationspläne nach Art. 14 DORA		*Art. 11 Abs. 4 sowie Art. 11 Abs. 6 lit. b) DORA*
6.	Mechanismen zur Aufzeichnung von und jederzeitigen Einsicht in Tätigkeiten nach Aktivierung von IKT-Geschäftsführungsplänen oder IKT-Reaktions- und Wiederherstellungsplänen gemäß Art. 11 Abs. 8 DORA		*Nicht vorgeschrieben, aber sinnvoll*
7.	Prozess für die Behandlung IKT-bezogener Vorfälle		*Letztlich aus Art. 17 Abs. 1 DORA*
8.	Prozess für die Erfassung von IKT-Vorfällen und erheblichen Cyberbedrohungen mit allen Anforderungen nach Art. 17 Abs. 3 DORA		*Letztlich aus Art. 17 Abs. 2 DORA*
9.	Meldung schwerwiegender IKT-Vorfälle an zuständige Behörde		*Nicht zwingend, aber sinnvoll zur Einhaltung von Art. 19 Abs. 1 DORA*
10.	Information über schwerwiegende IKT-Vorfälle mit Auswirkungen auf finanzielle Interessen von Kunden (inkl. deren Prüfung) und ergriffene Maßnahmen an Kunden		*Nicht zwingend, aber sinnvoll zur Einhaltung von Art. 19 Abs. 3 DORA*

Nr.	Maßnahme	Schritte	Quelle
11.	Information potenziell betroffener Kunden über angemessene Schutznahmen, die jene ergreifen können, wenn erhebliche Cyberbedrohungen vorliegen		*Nicht zwingend, aber sinnvoll zur Einhaltung Art. 19 Abs. 3 DORA*
12.	Solides und umfassendes Programm für das Testen der digitalen operationellen Resilienz gemäß Art. 25 bis 27 DORA		*Art. 24 Abs. 1 DORA*
13.	Außer Kleinstunternehmen: 1xjährlich angemessene Tests aller IKT-Systeme und -Anwendungen, die kritische oder wichtige Funktionen unterstützen		*Art. 24 Abs. 6 DORA*
14.	Ausreichende Tests der Ausstiegspläne für alle IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen		*Art. 28 Abs. 8 DORA*
Vor Abschluss einer geplanten Vereinbarung zu IKT-Dienstleistungen			
15.	Ermittlung und Bewertung des IKT-Konzentrationsrisikos gemäß Art. 29 Abs. 1, 28 Abs. 4 lit. c DORA		*Art. 29 Abs. 1, 28 Abs. 4 lit. c DORA*
Audits von IKT-Dienstleistern			
16.	Gemäß Auditplan		*Art. 28 Abs. 6 DORA*
Prüfung und Aktualisierung von Dokumenten			
17.	IKT-Geschäftsfortführungsleitlinie		*Art. 11 Abs. 6 DORA*
18.	Business-Impact-Analyse (BIA) der bestehenden Risiken für schwerwiegende Betriebsstörungen		
19.	IKT-Reaktions- und Wiederherstellungspläne		*Art. 11 Abs. 6 DORA*
20.	Entwicklung der IKT-Risiken im Zeitverlauf, insbesondere Häufigkeit, Art, Ausmaß und Entwicklung von IKT-Vorfällen um Risikoausmaß zu verstehen und Cyberreife und Abwehrbereitschaft des Unternehmens zu verbessern		*Art. 13 Abs. 4 DORA*
21.	Laufend außer Kleinstunternehmen: Ergebnisse der Überwachung einschlägiger technischer Entwicklungen und neuester Prozesse für IKT-Risikomanagement zur wirksamen Abwehr von Cyberangriffen		*Art. 13 Abs. 7 DORA*

Nr.	Maßnahme	Schritte	Quelle
22.	Regelmäßig außer bestimmte Finanzinstitute und Kleinstunternehmen: Strategie für das IKT-Drittparteienrisiko mit einer Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die durch IKT-Drittdienstleister bereitgestellt werden		*Art. 28 Abs. 2 DORA*
23.	Tests der Ausstiegspläne für alle IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen		*Art. 28 Abs. 8 DORA*
Interne Revision von Dokumentationen/Maßnahmen			
24.	IKT-Reaktions- und Wiederherstellungspläne		*(Außer Kleinstunternehmen:) Art. 11 Abs. 3 DORA*
Berichte an GF/Vorstand			
25.	1x jährlich: Bericht der leitenden IKT-Mitarbeiter über Erkenntnisse aus Tests zur digitalen operationellen Resilienz und aus realen IKT-Vorfällen		*Art. 13 Abs. 5 DORA*
Berichte an Behörden			
26.	*Nur Zentralverwahrer:* Ergebnisse aller Tests der IKT-Geschäftsfortführung oder ähnlicher Vorgänge		*Art. 11 Abs. 9 DORA*
27.	*Außer Kleinstunternehmen und nur auf Anfrage:* Geschätzte aggregierte jährliche Kosten und Verluste, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden		*Art. 11 Abs. 10 DORA*
28.	*Außer Kleinstunternehmen und nur auf Anfrage:* Änderungen an IKT-Vorgängen oder IKT-Geschäftsfortführungsrichtlinie nach Prüfung IKT-bezogener Vorfälle		*Art. 13 Abs. 2 DORA*
29.	Erstmeldung jedes schwerwiegenden IKT-Vorfalles		*Art. 19 Abs. 4 lit. a) DORA*
30.	Zwischenmeldung, wenn sich Status eines schwerwiegenden IKT-Vorfalles erheblich geändert hat		*Art. 19 Abs. 4 lit. b) DORA*
31.	Abschlussmeldung, wenn Ursachenanalyse eines schwerwiegenden IKT-Vorfalles abgeschlossen ist		*Art. 19 Abs. 4 lit. c) DORA*

Nr.	Maßnahme	Schritte	Quelle
32.	Mindestens 1xjährlich Bericht zur Anzahl neuer Vereinbarungen über IKT-Dienstleistungen gemäß Art. 28 Abs. 3 DORA		*Art. 28 Abs. 3 DORA*
33.	*Auf Verlangen:* Vollständiges Informationsregister oder bestimmte Teile		*Art. 28 Abs. 3 DORA*
34.	*Bei jeder geplanten vertraglichen Vereinbarung* über IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen oder wenn eine solche kritisch oder wichtig geworden ist		*Art. 28 Abs. 3 DORA*
Bei jedem IKT-Vorfall			
35.	Klassifizierung und Bestimmung der Auswirkungen nach Kriterien in Art. 18 Abs. 1 DORA		*Art. 18 Abs. 1 DORA*
Bei jeder Wiederherstellung nach IKT-Vorfällen			
36.	Mehrfachprüfungen und Abgleiche, um größtmögliche Datenintegrität nach Wiederherstellung sicherzustellen		*Art. 12 Abs. 7 DORA*
Nach jeder Störung von Haupttätigkeiten infolge schwerwiegender IKT-Vorfälle			
37.	Nachträgliche Prüfung der Ursachen für die Störung und erforderlicher Verbesserungen an IKT-Vorgängen oder IKT-Geschäftsfortführungs-richtlinie		*Art. 13 Abs. 2 DORA*
38.	Angemessene Prüfung relevanter Komponenten des IKT-Risikomanagementrahmens		*Art. 13 Abs. 3 DORA*