DORA-Anforderungen für kritische oder wichtige Funktionen

- Ein Cheatsheet aus der DORA-Werkstatt -

DISCLAIMER: Dieses Cheatsheet bietet eine erste Orientierung, welche operativen Anforderungen sich aus DORA ergeben, wenn eine Funktion als kritisch oder wichtig eingestuft wird. Das Cheatsheet ist nicht rechtsverbindlich und ersetzt keine juristische Prüfung.

Relevanz der kritischen oder wichtigen Funktionen

Kritische oder wichtige Funktionen (kwF) eines Finanzunternehmens haben zentrale Bedeutung für die Stabilität des europäischen Finanzmarkts. Daher müssen sie besonders geschützt und abgesichert werden.

Sobald eine Funktion als kritisch oder wichtig eingestuft ist, gelten daher für die unterstützenden IKT-Assets, IKT-Dienstleister und weiteren Ressourcen zusätzliche Anforderungen und Pflichten nach DORA.

Das Cheatsheet:

Das Cheatsheet bietet einen kompakten Überblick über die operativen DORA-Anforderungen, die sich direkt aus der kwF-Relevanz von Prozessen, IKT-Assets und IKT-Dienstleistungen ergeben. Es unterstützt dabei, erste Auswirkungen und Handlungsbedarfe strukturiert zu erkennen.

IKT-Risikomanagement

#	DORA-Anforderung	Referenz
IRM_1	Es ist eine Methodik und ein Verfahren festzulegen, um die kritischen oder wichtigen Funktionen zu ermitteln.	Art. 8 (1) DORA
IRM_2	Die Aufsicht ist zu informieren, sobald eine Funktion als kritisch oder wichtig eingestuft wird.	Art. 28 (3) DORA
IRM_3	Die Entwicklung von IKT-Risiken mit Bezug zu kritischen oder wichtigen Funktionen ist kontinuierlich auszuwerten.	Art. 13 (4) DORA
IRM_4	Im Bericht zur Überprüfung des IKT-Risikomanagementrahmens sind kwF-relevante IKT-Risiken und IKT-Vorfälle darzulegen.	Art. 27 (2a, ii) RTS risk mgt.
IRM_5	IKT-Projekte, die kritische oder wichtige Funktionen betreffen, sind einschließlich ihrer Risiken regelmäßig an das Leitungsorgan zu berichten.	Art. 15 (5) RTS risk mgt.

IKT-Vorfallsmanagement

#	DORA-Anforderung	Referenz
Inc_1	IKT-Vorfälle mit Bezug zu kritischen oder wichtigen Funktionen, IKT-Assets oder IKT-Systemen sind systematisch auszuwerten und zu analysieren.	Art. 13 (4) DORA
Inc_2	IKT-Vorfälle, die IKT-Services oder Netz- und Informationssysteme mit Relevanz für kritische oder wichtige Funktionen betreffen, sind potenziell als schwerwiegende IKT-bezogene Vorfälle einzustufen.	Art. 6 (a) RTS incident classification
Inc_3	Der Ausfall von IKT-Services, die kritische oder wichtige Funktionen unterstützen, stellt ab einer Dauer von mehr als zwei Stunden einen potenziell schwerwiegenden IKT-bezogenen Vorfall dar.	Art. 9 (3b) RTS incident classification

Testen der digitalen operationalen Resilienz

#	DORA-Anforderung	Referenz
Test_1	Für alle IKT-Systeme und Anwendungen, die kritische oder wichtige Funktionen unterstützen, sind mindestens jährlich geeignete Sicherheitstests durchzuführen.	Art. 24 (6) DORA
Test_2	TLPT-pflichtige Finanzunternehmen müssen ein Assessment durchführen, um festzulegen, welche kritischen oder wichtigen Funktionen sowie kwF-relevanten IKT-Systeme und IKT-Dienstleistungen im Rahmen von TLPTs zu überprüfen sind. Produktive IKT-Systeme sind in den TLPTs zu berücksichtigen.	Art. 26 (2) DORA/ Art. 8 (6) RTS TLPT

IKT-Drittparteienrisikomanagement

#	DORA-Anforderung	Referenz
TPRM_1	Es ist eine Richtlinie zur Nutzung von IKT-Dienstleistungen mit Relevanz für die kritischen oder wichtigen Funktionen zu erstellen	Art. 28 (2) DORA
TPRM_2	Es ist eine Methodik zur Bestimmung von kwF-relevanten IKT-Dienstleistungen festzulegen.	Art. 3 (2) RTS "3P-policy"
TPRM_3	Es sind alle kwF-relevanten IKT-Dienstleister und IKT-Dienstleistungen zu bestimmen.	Art. 28 (3) DORA/ Art. 8 (5) DORA
TPRM_4	Vor jedem Vertragsabschluss ist zu prüfen, ob die geplante IKT-Dienstleistung eine kritische oder wichtige Funktion unterstützten soll.	Art. 28 (4a) DORA
TPRM_5	Im Informationsregister sind alle kwF-relevanten IKT-Dienstleistungen, IKT-Dienstleister und ggf. kwF-relevante Subunternehmer zu dokumentieren.	Art. 3 (1) ITS Information register
TPRM_6	Die Aufsicht ist über geplante kwF-relevante IKT-Verträge vorab und proaktiv zu informieren.	Art. 28 (3) DORA
TPRM_7	Das Leitungsorgan ist angemessen bei Entscheidungen zum Einsatz von kwF-relevanten IKT-Dienstleistungen einzubeziehen.	Art. 4 (a) RTS "3P-policy"
TPRM_8	Das Leitungsorgan muss regelmäßig die Risiken aus kwF-relevanten IKT-Verträgen überprüfen.	Art. 28 (2) DORA
TPRM_9	Das Leitungsorgan muss regelmäßig über IKT-Verträge, geplante Änderungen und deren Auswirkungen auf kritische oder wichtige Funktionen informiert werden.	Art. 5 (2i) DORA
TPRM_10	Vertragsänderungen an kwF-relevanten IKT-Verträgen, die sich aus den neuen regulatorischen Anforderungen nach DORA ergeben, sind zeitnah und auf Basis einer Umsetzungsplanung durchzusetzen.	Art. 4 (2) RTS Subcontracting
TPRM_11	Sollen kwF-relevante IKT-Dienstleistungen durch gruppeninterne IKT-Dienstleister in Anspruch genommen werden, müssen objektive Entscheidungen über Vertragsbedingungen sichergestellt werden.	Art. 7 (2) RTS "3P-policy"
TPRM_12	Vor Abschluss von kwF-relevanten IKT-Verträgen ist im Rahmen der Due Diligence die Eignung des IKT-Dienstleisters zu bewerten.	Art. 6 (2) RTS "3P-policy"/ Art. 6 (1a) RTS "3P-policy"
TPRM_13	Vor Abschluss von kwF-relevanten IKT-Verträgen ist eine Risikobewertung (Ex-ante Risk Assessment) durchzuführen, um Risiken in Verbindung mit der IKT-Dienstleistung zu identifizieren.	Art. 5 (2) RTS "3P-policy"/ Art. 29 (1) DORA
TPRM_14	IKT-Dienstleister, die mit der Erbringung von kwF-relevanten IKT-Dienstleistungen beauftragt werden, müssen über ausreichende Ressourcen verfügen, um die rechtlichen und regulatorischen Anforderungen erfüllen zu können.	Art. 3 (4) RTS "3P-policy"
TPRM_15	Vor Vertragsabschluss von kwF-relevanten IKT-Verträgen ist sicherzustellen, dass der	Art. 28 (5) DORA

	Dienstleister die aktuellsten und hochwertigsten Sicherheitsstandards berücksichtigt.	
TPRM_16	Es ist sicherzustellen, das kwF-relevante IKT-Dienstleister die Dienstleistungen gemäß vereinbarter Leistungs- und Qualitätsstandards sowie unter Berücksichtigung der internen Vorgaben des Finanzunternehmens erbringen.	Art. 9 (2) RTS "3P-policy"
TPRM_17	Das Finanzunternehmen muss bei kwF-relevanten IKT-Dienstleistungen regelmäßige Leistungsberichte, Incident-Berichte, Berichte zur Serviceerbringung, zur IKT-Sicherheit sowie zu Notfallmaßnahmen und deren Tests einfordern und auswerten.	Art. 9 (2a) RTS "3P-policy"/ Art. 9 (2b) RTS "3P-policy" Art. 9 (2c) RTS "3P-policy"
TPRM_18	Das Finanzunternehmen muss von kwF-relevanten IKT-Dienstleistern über IKT-bezogene Vorfälle sowie operative oder sicherheitsrelevante Zahlungsverkehrsvorfälle informiert werden.	Art. 9 (2d) RTS "3P-policy"
TPRM_19	KwF-relevante IKT-Dienstleistungen müssen unabhängigen Prüfungen und Audits unterzogen werden, um die Einhaltung der Vorgaben zu überprüfen.	Art. 9 (2e) RTS "3P-policy"/ Art. 3 (7) RTS "3P-policy"
TPRM_20	Bei Mängeln in Bezug auf kwF-relevante IKT-Dienstleister oder IKT-Dienstleistungen, müssen die Finanzunternehmen geeignete Maßnahmen ergreifen und die Beseitigung der Mängel nachverfolgen.	Art. 9 (4) RTS "3P-policy"
TPRM_21	Bei kwF-relevanten IKT-Dienstleistungen ist sicherzustellen, dass das Finanzunternehmen, seine Prüfer und die Aufsichtsbehörden Zugang zu allen relevanten Daten und Räumlichkeiten erhalten.	Art.3 (8d) RTS "3P-policy"
TPRM_22	Für kwF-relevante IKT-Dienstleistungen ist festzulegen, ob und unter welchen Bedingungen eine Weitervergabe (Subcontracting) zulässig ist.	Art. 4 (1) RTS Subcontracting/. Art. 30 (2a) DORA/ Art. 3 (1) RTS Subcontracting
TPRM_23	Vor Vertragsabschluss eines kwF-relevanten IKT-Vertrags ist zu prüfen, ob der IKT-Dienstleister beabsichtigt, Unterauftragnehmer für die Erbringung des IKT-Service einzubeziehen.	Art. 6 (1c) RTS "3P-policy"
TPRM_24	Bei der Zulassung von Unterauftragnehmern zur Erbringung von kwF-relevanten IKT-Dienstleistungen, ist die Einhaltung der erforderlichen Mindestvertragsinhalte sicherzustellen.	Art. 5 (1 - 4) RTS subcontracting/ Art. 7 (1) RTS subcontracting Art. 30 (3) DORA
TPRM_25	Bei wesentlichen Änderungen in der Unterauftragnehmerkette für kwF-relevante IKT-Dienstleistungen, muss das Finanzunternehmen die Änderungen genehmigen.	Art. 6 (1- 3) RTS subcontracting
TPRM_26	Für kwF-relevante IKT-Dienstleistungen sind Exit-Strategien und Exit-Pläne zu erstellen. Die Exit-Pläne müssen regelmäßig getestet und aktualisiert werden.	Art. 28 (8) DORA

IKT-BCM und IKT-SCM

#	DORA-Anforderung	Referenz
BCM_1	Für kritische oder wichtige Funktionen sowie kwF-relevante IKT-Dienstleistungen müssen angemessene IKT-BCM Pläne eingerichtet, gepflegt und regelmäßig getestet werden.	Art. 11 (4) DORA
BCM_2	Es sind geeignete und dokumentierte IKT-BCM-Vorkehrungen umzusetzen, um die Kontinuität der kritischen oder wichtigen Funktionen sicherzustellen.	Art. 11 (2a) DORA
BCM_3	Zentralverwahrer müssen sicherstellen, dass kritische oder wichtige Funktionen innerhalb von maximal 2 Stunden wiederhergestellt werden können.	Art. 24 (3b) RTS risk mgt.
BCM_4	Für kwF-relevante IKT-Systeme müssen die IKT-BCM-Pläne sowie die IKT-Response- und Recovery-Pläne mindestens jährlich und bei jeder wesentlichen Änderung getestet werden.	Art. 11 (6) DORA

BCM_5	Die IKT-BCM-Pläne müssen getestet werden, um sicherzustellen, dass kritische oder wichtige Funktionen im Notfall aufrechterhalten und abgesichert werden können. Dabei sind auch kwF-relevante IKT-Dienstleistungen einzubeziehen.	Art. 25 (2) RTS risk mgt.
BCM_6	Die IKT-Response- und Recovery-Pläne müssen Szenarien abdecken, in denen eine kritische oder wichtige Funktion ausfällt oder untragbar beeinträchtigt ist, einschließlich der möglichen Insolvenz oder des Ausfalls des IKT-Dienstleisters.	Art. 26 (2b) RTS risk mgt.
BCM_7	Die IKT-Reaktions- und Wiederherstellungspläne müssen Maßnahmen vorsehen, um Ausfälle von kwF-relevanten IKT-Dienstleistern abzufedern und festlegen, welche Maßnahmen erforderlich sind, um Verfügbarkeit, Integrität, Kontinuität und Wiederherstellung der kwF-relevanten IKT-Systeme und -Services sicherzustellen.	Art. 26 (4) RTS risk mgt./ Art. 26 (1b) RTS risk mgt.
BCM_8	Für kritische oder wichtige Funktionen ist bei der Festlegung von Wiederherstellungszeiten (RTO) und Wiederherstellungszeitpunkten (RPO) zu berücksichtigen, ob und welchen Einfluss ein Ausfall der Funktion auf die Marktstabilität hätte. RTO und RPO sind so auszulegen, dass vereinbarte Servicelevel auch in Extremszenarien eingehalten werden.	Art. 12 (6) DORA
BCM_9	Zentralverwahrer müssen einen sekundären Verarbeitungsstandort vorhalten, der die Kontinuität kritischer oder wichtiger Funktionen sicherstellt.	Art. 12 (5) DORA

Operative IKT-Sicherheit

#	DORA-Anforderung	Referenz
Sec_1	Für kwF-relevante IKT-Services ist die Nutzung von Drittanbieter-Bibliotheken einschließlich Open Source Bibliotheken zu überwachen. Verwendete Bibliotheken und Versionen sind zu dokumentieren sowie verfügbare Updates und Sicherheitskorrekturen zu verfolgen.	Art. 8 (6) DORA/ Art. 10 (2d) RTS risk mgt.
Sec_2	Es sind IKT-Sicherheitsrichtlinien und Sicherheitstools zu implementieren, um kwF-relevante IKT-Systeme zu schützen. Dabei sind hohe Standards für Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten sicherzustellen.	Art. 9 (2) DORA
Sec_3	Es ist ein aktuelles Register aller Zertifikate und zertifikatsspeichernden Geräte für IKT-Assets zu führen, die kritische oder wichtige Funktionen unterstützen.	Art. 7 (4) RTS risk management
Sec_4	Für IKT-Systeme, die kritische oder wichtige Funktionen unterstützen, ist die Angemessenheit der Firewall-Regeln und Verbindungsfilter mindestens alle 6 Monate zu überprüfen.	Art. 13 (h) RTS risk management
Sec_5	Für IKT-Assets, die kritische oder wichtige Funktionen unterstützen, sind mindestens wöchentlich automatisierte Schwachstellenscans und -bewertungen durchzuführen.	Art. 10 (2b) RTS risk management
Sec_6	Zentralverwahrer und zentrale Gegenparteien müssen vor jedem Deployment neuer oder aktualisierter Anwendungen, Infrastrukturkomponenten und IKT-Services, die kritische oder wichtige Funktionen unterstützen, Schwachstellenbewertungen durchführen.	Art. 25 (2) DORA
Sec_7	Cyberbedrohungen, die kritische oder wichtige Funktionen beeinträchtigen könnten, sind als signifikant einzustufen und sind damit potenziell melderelevant.	Art. 10 (a) RTS incident classification
Sec_8	Für IKT-Assets und Informationswerte, die kritische oder wichtige Funktionen unterstützen, sind Werkzeuge zur Anomalie-Erkennung zu implementieren, die automatisierte Warnmeldungen auf Basis vordefinierter Regeln erzeugen.	Art. 23 (2b) RTS risk mgt.
Sec_9	Für den Zugriff auf IKT-Assets, die kritische oder wichtige Funktionen unterstützen, sind starke Authentifizierungsverfahren nach anerkannten Sicherheitsstandards einzusetzen.	Art. 21 (1f, ii) RTS risk mgt.
Sec_10	Für IKT-Systeme, die kritische oder wichtige Funktionen unterstützen, sind Zugriffsrechte mindestens alle 6 Monate zu überprüfen und bei Bedarf anzupassen.	Art. 21 (1e, iv) RTS risk mgt.