DORA-Sollmaßnahmenkatalog

Eine praxisnahe Interpretation der regulatorischen DORA-Vorgaben

Strukturiert nach ISO/IEC 27001:2022

Dr. Marlen Hofmann

info@marlen-hofmann.de | www.marlen-hofmann.de

Version 1.0 | März 2026

Vorwort

Die rasante Digitalisierung hat den Finanzsektor in den letzten Jahren tiefgreifend verändert. Finanzunternehmen stützen sich zunehmend auf Informations- und Kommunikationstechnologien (IKT), um ihre Kernprozesse zu betreiben und ihre Dienstleistungen effizient sowie sicher zu erbringen. Diese Abhängigkeit bringt jedoch erhebliche Risiken mit sich: Cyberangriffe, IKT-Ausfälle und technische Störungen bedrohen nicht nur einzelne Institute, sondern können die Stabilität des gesamten Finanzsystems gefährden.

Um diesen Risiken zu begegnen, hat die Europäische Union die Verordnung (EU) 2022/2554 - den Digital Operational Resilience Act (DORA) - erlassen. DORA legt verbindliche Anforderungen an das IKT-Risikomanagement, die Sicherheitsarchitektur und die Steuerung von IKT-Drittdienstleistern fest.

Zielsetzung des DORA-Sollmaßnahmenkatalogs

Der vorliegende DORA-Sollmaßnahmenkatalog interpretiert die regulatorischen Anforderungen der DORA-Verordnung sowie der zugehörigen technischen Regulierungsstandards (RTS) und Durchführungsstandards (ITS) und übersetzt sie in konkrete, praxisnah formulierte Sollmaßnahmen. Ziel ist es, Finanzunternehmen ein Instrument an die Hand zu geben, das die Brücke zwischen Rechtstext und operativer Umsetzung schlägt.

Methodik

Der Katalog wurde in einem systematischen, mehrstufigen Verfahren erstellt:

- **Dekomposition.** Ausgangspunkt waren die offiziellen Rechtstexte der DORA-Verordnung und der zugehörigen delegierten Verordnungen. Diese wurden zunächst in ihre einzelnen Regelungsgehalte zerlegt.
- **Praxisinterpretation.** Aus jedem Regelungsgehalt wurde abgeleitet, welche praktischen Anforderungen sich ergeben — etwa ob eine Anforderung schriftlich angewiesen werden muss, prozessual zu verankern oder technisch zu operationalisieren ist. Dabei wurde die juristische Sprache in praxisnahe Formulierungen überführt und dort, wo der Gesetzestext abstrakt bleibt, durch etablierte Begriffe der IT-Governance konkretisiert.
- **Typklassifikation.** Jede Sollmaßnahme wurde einem von acht Anforderungstypen zugeordnet, der die Umsetzungsebene bestimmt:
    - Anforderungen an Strategien,
    - Anforderungen an Richtlinien und Leitlinien
    - Anforderungen an Governance-Verfahren und -Methoden,
    - Anforderungen an Pläne,
    - Anforderungen an technische Konzepte und Verfahren
    - Anforderungen an die Operationalisierung
    - Anforderungen an Berichte sowie
    - Anforderungen an Mindestinhalte in IKT-Verträgen.
- **ISO-Strukturierung.** Um die Integration in bestehende Informationssicherheits-Managementsysteme (ISMS) zu erleichtern, wurde der Katalog entlang der Kontrollstruktur der ISO/IEC 27001:2022 gegliedert. Jede Sollmaßnahme ist einem ISO-Control zugeordnet, sodass unmittelbar erkennbar wird, welche DORA-Anforderungen auf bereits implementierte Controls einzahlen - und wo zusätzlicher Handlungsbedarf besteht.

Ergebnis

Das Ergebnis sind 1.039 Sollmaßnahmen, strukturiert entlang von 86 ISO-Referenzpunkten. Diese setzen sich zusammen aus 71 der 93 Annex-A-Controls sowie 15 der 40 Managementklauseln aus dem Normkörper der ISO/IEC 27001:2022 (Kapitel 4–10). Die verbleibenden 48 ISO-Referenzpunkte ohne DORA-Mapping wurden als Strukturelemente beibehalten und spiegeln wider, dass DORA diese Themenfelder nicht explizit adressiert.

Ich wünsche Ihnen eine gewinnbringende Arbeit mit diesem Katalog und freue mich über Ihr Feedback.

Dr. Marlen Hofmann

März 2026

Urheberrechtshinweis

Hinweis zur Autorenschaft und Nebentätigkeit

Der DORA-Sollmaßnahmenkatalog wurde im Rahmen einer privaten Nebentätigkeit erstellt. Sämtliche Analysen, Interpretationen und Einschätzungen in diesem Dokument spiegeln ausschließlich die persönliche fachliche Sichtweise der Autorin wider. Sie stehen in keinem Zusammenhang mit den Ansichten, Richtlinien oder Vorgaben ihres Arbeitgebers und stellen keine offizielle Stellungnahme ihres Arbeitgebers dar.

Hinweis zur Verwendung und rechtlichen Einordnung

Die dargestellten Sollmaßnahmen basieren auf einer intensiven fachlichen Auseinandersetzung mit der DORA-Verordnung sowie den dazugehörigen Regulierungsstandards. Der DORA-Sollmaßnahmenkatalog dient ausschließlich als fachliche Orientierungshilfe für die praktische Umsetzung der regulatorischen Anforderungen und erhebt keinen Anspruch auf Vollständigkeit oder rechtliche Verbindlichkeit.

Die Inhalte dieses Dokuments stellen keine Rechtsberatung dar und können eine solche nicht ersetzen. Für die konkrete Umsetzung regulatorischer Anforderungen im jeweiligen Einzelfall sollten bei Bedarf qualifizierte rechtliche oder fachliche Beratungen eingeholt werden. Die Herausgeberin übernimmt keine Haftung für Entscheidungen, Maßnahmen, Schäden oder Verluste, die unmittelbar oder mittelbar aus der Nutzung oder Interpretation dieses Dokuments entstehen.

Hinweis zur Aktualisierung

Für die Erstellung der Anforderungen in diesem Sollmaßnahmenkatalog wurden die nachstehend aufgeführten Quellen herangezogen. Die Inhalte wurden zuletzt mit Stand vom 31.12.2025 auf ihre Aktualität geprüft.

Da sich regulatorische Anforderungen sowie technische und aufsichtsrechtliche Standards kontinuierlich weiterentwickeln, kann eine regelmäßige Aktualisierung dieses Anforderungskatalogs erforderlich sein. Dieser Katalog erhebt daher keinen Anspruch auf dauerhafte Vollständigkeit oder Aktualität.

Es liegt in der Verantwortung der Nutzerinnen und Nutzer, sich eigenständig über Änderungen relevanter Rechtsvorschriften, regulatorischer Vorgaben und technischer Standards zu informieren und diese bei der Umsetzung entsprechend zu berücksichtigen.

Quellen

DORA (EU 2022/2554)
Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011

RTS IKT-Risikomanagement (2024/1774)
Delegierte Verordnung (EU) 2024/1774 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 durch technische Regulierungsstandards zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens

RTS Incident-Klassifizierung (2024/1772)
Delegierte Verordnung (EU) 2024/1772 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 durch technische Regulierungsstandards zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen, der Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle

RTS IKT-Drittparteien (2024/1773)
Delegierte Verordnung (EU) 2024/1773 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 durch technische Regulierungsstandards zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden

ITS Informationsregister (2024/2956)
Durchführungsverordnung (EU) 2024/2956 der Kommission zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2022/2554 im Hinblick auf Standardvorlagen für das Informationsregister

RTS Incident-Meldung (2025/301)
Delegierte Verordnung (EU) 2025/301 der Kommission vom 23. Oktober 2024 zur Ergänzung der Verordnung (EU) 2022/2554 durch technische Regulierungsstandards zur Festlegung des Inhalts und der Fristen für die Erstmeldung, die Zwischenmeldung und die Abschlussmeldung schwerwiegender IKT-bezogener Vorfälle sowie des Inhalts der freiwilligen Meldung erheblicher Cyberbedrohungen

ITS Incident-Reporting (2025/302)
Durchführungsverordnung (EU) 2025/302 der Kommission vom 23. Oktober 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2022/2554 bezüglich der Standardformulare, Vorlagen und Verfahren für die Meldung schwerwiegender IKT-bezogener Vorfälle und die Benachrichtigung über erhebliche Cyberbedrohungen

RTS TLPT (2025/1190)
Delegierte Verordnung (EU) 2025/1190 der Kommission vom 13. Februar 2025 zur Ergänzung der Verordnung (EU) 2022/2554 durch technische Regulierungsstandards zur Festlegung der Kriterien für die Bestimmung der Finanzunternehmen, die zur Durchführung von bedrohungsorientierten Penetrationstests verpflichtet sind, der Anforderungen und Standards für den Einsatz interner Tester, der Anforderungen hinsichtlich des Testumfangs, der Testmethodik und des Testkonzepts

RTS Untervergabe (2025/532)
Delegierte Verordnung (EU) 2025/532 der Kommission vom 24. März 2025 zur Ergänzung der Verordnung (EU) 2022/2554 durch technische Regulierungsstandards zur Präzisierung der Aspekte, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss

GL Kosten & Verluste (JC 2024 34)
Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents under Regulation (EU) 2022/2554 (JC 2024 34)

Mapping-Übersicht DORA-Artikel zu ISO-Control

Die folgende Übersicht zeigt alle Artikel der 10 DORA-Rechtsquellen und deren Zuordnung zu den ISO 27001:2022-Controls des Sollmaßnahmenkatalogs. 107 Artikel sind mit ISO-Controls gemappt. 72 Artikel (grau hinterlegt) enthalten keine unmittelbaren Anforderungen an Finanzunternehmen, sodass daraus keine Sollmaßnahmen abgeleitet wurden – dies betrifft insbesondere Begriffsbestimmungen, Übergangs- und Schlussbestimmungen, behördliche Zuständigkeiten sowie Regelungen zum Überwachungsrahmen.

Rechtsquelle / Artikel	Artikelüberschrift	ISO-Controls
DORA (EU 2022/2554) – Art. 1 – 3	*Es wurden keine eigenständigen Sollmaßnahmen abgeleitet, da die jeweiligen Rechtstexte übergeordneter Natur sind.*	
DORA (EU 2022/2554) – Art. 4	Grundsatz der Verhältnismäßigkeit	ISMS-4.1 – Verstehen der Organisation und ihres Kontextes ISMS-4.3 – Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems
DORA (EU 2022/2554) – Art. 5	Governance und Organisation	ISMS-5.1 – Führung und Verpflichtung ISMS-5.3 – Rollen, Verantwortlichkeiten und Befugnisse in der Organisation ISMS-7.1 – Ressourcen ISMS-7.2 – Kompetenz ISMS-7.3 – Bewusstsein A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.2 – Informationssicherheitsrollen und -verantwortlichkeiten A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.3 – Aufgabentrennung A-5.4 – Verantwortlichkeiten der Leitung A-6.3 – Informationssicherheitsbewusstsein, -ausbildung und -schulung
DORA (EU 2022/2554) – Art. 6	IKT-Risikomanagementrahmen	ISMS-4.4 – Informationssicherheitsmanagementsystem ISMS-5.2 – Politik ISMS-6.2 – Informationssicherheitsziele und Planung zu deren Erreichung ISMS-8.3 – Informationssicherheitsrisikobehandlung ISMS-9.2 – Internes Audit ISMS-10.1 – Fortlaufende Verbesserung A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.2 – Informationssicherheitsrollen und -verantwortlichkeiten A-5.3 – Aufgabentrennung A-5.35 – Unabhängige Überprüfung der Informationssicherheit A-5.5 – Kontakt mit Behörden
DORA (EU 2022/2554) – Art. 7	IKT-Systeme, -Protokolle und -Tools	A-5.1 – Informationssicherheitspolitik und -richtlinien
DORA (EU 2022/2554) – Art. 8	Identifizierung	ISMS-8.2 – Informationssicherheitsrisikobeurteilung A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.12 – Klassifizierung von Informationen A-5.7 – Informationen über die Bedrohungslage A-5.9 – Inventar der Informationen und damit verbundenen Werte A-8.32 – Änderungssteuerung A-8.8 – Handhabung von technischen Schwachstellen A-8.9 – Konfigurationsmanagement
DORA (EU 2022/2554) – Art. 9	Schutz und Prävention	A-5.1 – Informationssicherheitspolitik und -richtlinien A-7.2 – Physischer Zutritt A-8.22 – Trennung von Netzwerken A-8.32 – Änderungssteuerung ISMS-4.4 – Informationssicherheitsmanagementsystem ISMS-5.2 – Politik
DORA (EU 2022/2554) – Art. 10	Erkennung	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.26 – Reaktion auf Informationssicherheitsvorfälle A-5.30 – IKT-Bereitschaft für Business-Continuity A-8.16 – Überwachung von Aktivitäten
DORA (EU 2022/2554) – Art. 11	Reaktion und Wiederherstellung	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.2 – Informationssicherheitsrollen und -verantwortlichkeiten A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse A-5.30 – IKT-Bereitschaft für Business-Continuity A-5.35 – Unabhängige Überprüfung der Informationssicherheit
DORA (EU 2022/2554) – Art. 12	Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.26 – Reaktion auf Informationssicherheitsvorfälle A-5.30 – IKT-Bereitschaft für Business-Continuity A-8.13 – Sicherung von Informationen A-8.14 – Redundanz von informationsverarbeitenden Einrichtungen
DORA (EU 2022/2554) – Art. 13	Lernprozesse und Weiterentwicklung	ISMS-5.1 – Führung und Verpflichtung ISMS-5.2 – Politik ISMS-7.2 – Kompetenz ISMS-7.3 – Bewusstsein ISMS-8.2 – Informationssicherheitsrisikobeurteilung ISMS-9.1 – Überwachung, Messung, Analyse und Bewertung A-5.1 – Informationssicherheitspolitik und -richtlinien

Rechtsquelle / Artikel	Artikelüberschrift	ISO-Controls
		A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.27 – Erkenntnisse aus Informationssicherheitsvorfällen A-5.30 – IKT-Bereitschaft für Business-Continuity A-5.4 – Verantwortlichkeiten der Leitung A-5.7 – Informationen über die Bedrohungslage A-6.3 – Informationssicherheitsbewusstsein, -ausbildung und -schulung A-6.8 – Meldung von Informationssicherheitsereignissen A-8.8 – Handhabung von technischen Schwachstellen
DORA (EU 2022/2554) – Art. 14	Kommunikation	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.24 – Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen A-5.30 – IKT-Bereitschaft für Business-Continuity A-8.8 – Handhabung von technischen Schwachstellen
DORA (EU 2022/2554) – Art. 15 und 16	*Art. 15 - Keine unmittelbaren Anforderungen an Finanzunternehmen enthalten – daher wurden keine Sollmaßnahmen abgeleitet, Art. 16 (Vereinfachter IKT-Risikomanagementrahmen) wurde nicht explizit beleuchtet.*	
DORA (EU 2022/2554) – Art. 17	Prozess für die Behandlung IKT-bezogener Vorfälle	A-5.24 – Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen A-5.26 – Reaktion auf Informationssicherheitsvorfälle
DORA (EU 2022/2554) – Art. 18	Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse
DORA (EU 2022/2554) – Art. 19	Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-6.8 – Meldung von Informationssicherheitsereignissen
DORA (EU 2022/2554) – Art. 20 – 22	*Keine unmittelbaren Anforderungen an Finanzunternehmen – keine Sollmaßnahmen abgeleitet*	
DORA (EU 2022/2554) – Art. 23	Zahlungsbezogene Betriebs- oder Sicherheitsvorfälle	A-5.24 – Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
DORA (EU 2022/2554) – Art. 24	Allgemeine Anforderungen für das Testen der digitalen operationalen Resilienz	A-5.1 – Informationssicherheitspolitik und -richtlinien ISMS-9.1 – Überwachung, Messung, Analyse und Bewertung
DORA (EU 2022/2554) – Art. 25	Testen von IKT-Tools und -Systemen	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.30 – IKT-Bereitschaft für Business-Continuity A-5.36 – Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit A-5.37 – Dokumentierte Betriebsabläufe A-7.4 – Physische Sicherheitsüberwachung A-8.20 – Netzwerksicherheit A-8.28 – Sichere Codierung A-8.29 – Sicherheitsprüfung bei Entwicklung und Abnahme A-8.6 – Kapazitätssteuerung A-8.8 – Handhabung von technischen Schwachstellen ISMS-8.2 – Informationssicherheitsrisikobeurteilung
DORA (EU 2022/2554) – Art. 26	Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT	A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen Kein Treffer – —
DORA (EU 2022/2554) – Art. 27	Anforderungen an Tester bezüglich der Durchführung von TLPT	Kein Treffer – —
DORA (EU 2022/2554) – Art. 28	Allgemeine Prinzipien	ISMS-5.1 – Führung und Verpflichtung ISMS-8.2 – Informationssicherheitsrisikobeurteilung A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.12 – Klassifizierung von Informationen A-5.19 – Informationssicherheit in Lieferantenbeziehungen A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.23 – Informationssicherheit für die Nutzung von Cloud-Diensten A-5.4 – Verantwortlichkeiten der Leitung A-5.5 – Kontakt mit Behörden
DORA (EU 2022/2554) – Art. 29	Vorläufige Bewertung des IKT-Konzentrationsrisikos auf Unternehmensebene	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.19 – Informationssicherheit in Lieferantenbeziehungen A-5.21 – Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)
DORA (EU 2022/2554) – Art. 30	Wesentliche Vertragsbestimmungen	A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen
DORA (EU 2022/2554) – Art. 31 – 44	*Keine unmittelbaren Anforderungen an Finanzunternehmen – keine Sollmaßnahmen abgeleitet*	
DORA (EU 2022/2554) – Art. 45	Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.5 – Kontakt mit Behörden A-5.6 – Kontakt mit speziellen Interessensgruppen
DORA (EU 2022/2554) – Art. 46 – 64	*Keine unmittelbaren Anforderungen an Finanzunternehmen – keine Sollmaßnahmen abgeleitet*	
RTS IKT-Risikomanagement (2024/1774) – Art. 1	Gesamtrisikoprofil und -komplexität	ISMS-4.1 – Verstehen der Organisation und ihres Kontextes ISMS-4.3 – Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems A-5.1 – Informationssicherheitspolitik und -richtlinien
RTS IKT-Risikomanagement (2024/1774) – Art. 2	Allgemeine Elemente der Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit	ISMS-5.2 – Politik ISMS-7.5 – Dokumentierte Information A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.10 – Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten

Rechtsquelle / Artikel	Artikelüberschrift	ISO-Controls
		A-8.16 – Überwachung von Aktivitäten A-8.20 – Netzwerksicherheit A-8.24 – Verwendung von Kryptographie
RTS IKT-Risikomanagement (2024/1774) – Art. 3	IKT-Risikomanagement	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.7 – Informationen über die Bedrohungslage A-8.8 – Handhabung von technischen Schwachstellen ISMS-6.1.2 – Informationssicherheitsrisikobeurteilung ISMS-6.1.3 – Informationssicherheitsrisikobehandlung
RTS IKT-Risikomanagement (2024/1774) – Art. 4	Richtlinie für das Management von IKT-Assets	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.9 – Inventar der Informationen und damit verbundenen Werte A-8.9 – Konfigurationsmanagement
RTS IKT-Risikomanagement (2024/1774) – Art. 5	Verfahren für das Management von IKT-Assets	A-5.12 – Klassifizierung von Informationen
RTS IKT-Risikomanagement (2024/1774) – Art. 6	Verschlüsselung und Kryptografie	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.7 – Informationen über die Bedrohungslage A-8.24 – Verwendung von Kryptographie
RTS IKT-Risikomanagement (2024/1774) – Art. 7	Management kryptografischer Schlüssel	A-5.1 – Informationssicherheitspolitik und -richtlinien A-8.24 – Verwendung von Kryptographie
RTS IKT-Risikomanagement (2024/1774) – Art. 8	IKT-Betriebssicherheit	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.10 – Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten A-5.35 – Unabhängige Überprüfung der Informationssicherheit A-5.37 – Dokumentierte Betriebsabläufe A-5.9 – Inventar der Informationen und damit verbundenen Werte A-8.13 – Sicherung von Informationen A-8.15 – Protokollierung A-8.31 – Trennung von Entwicklungs-, Test- und Produktionsumgebungen A-8.34 – Schutz der Informationssysteme während Tests im Rahmen von Audits
RTS IKT-Risikomanagement (2024/1774) – Art. 9	Kapazitäts- und Leistungsmanagement	A-5.37 – Dokumentierte Betriebsabläufe A-8.6 – Kapazitätssteuerung
RTS IKT-Risikomanagement (2024/1774) – Art. 10	Schwachstellen- und Patch-Management	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.9 – Inventar der Informationen und damit verbundenen Werte A-8.8 – Handhabung von technischen Schwachstellen
RTS IKT-Risikomanagement (2024/1774) – Art. 11	Daten- und Systemsicherheit	ISMS-7.2 – Kompetenz ISMS-8.2 – Informationssicherheitsrisikobeurteilung A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.10 – Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten A-5.19 – Informationssicherheit in Lieferantenbeziehungen A-5.2 – Informationssicherheitsrollen und -verantwortlichkeiten A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.9 – Inventar der Informationen und damit verbundenen Werte A-6.7 – Remote-Arbeit A-7.10 – Speichermedien A-7.14 – Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln A-8.1 – Endpunktgeräte des Benutzers A-8.10 – Löschung von Informationen A-8.12 – Verhinderung von Datenlecks A-8.19 – Installation von Software auf Systemen im Betrieb A-8.26 – Anforderungen an die Anwendungssicherheit A-8.27 – Sichere Systemarchitektur und Entwicklungsgrundsätze A-8.3 – Informationszugangsbeschränkung A-8.7 – Schutz gegen Schadsoftware A-8.9 – Konfigurationsmanagement
RTS IKT-Risikomanagement (2024/1774) – Art. 12	Datenaufzeichnung	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.33 – Schutz von Aufzeichnungen A-8.15 – Protokollierung A-8.17 – Uhrensynchronisation A-8.32 – Änderungssteuerung
RTS IKT-Risikomanagement (2024/1774) – Art. 13	Management der Netzwerksicherheit	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.9 – Inventar der Informationen und damit verbundenen Werte A-8.20 – Netzwerksicherheit A-8.21 – Sicherheit von Netzwerkdiensten A-8.22 – Trennung von Netzwerken A-8.24 – Verwendung von Kryptographie A-8.5 – Sichere Authentisierung A-8.9 – Konfigurationsmanagement
RTS IKT-Risikomanagement (2024/1774) – Art. 14	Sicherung von Informationen bei der Übermittlung	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.14 – Informationsübermittlung A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von

Rechtsquelle / Artikel	Artikelüberschrift	ISO-Controls
		Lieferantendienstleistungen A-8.12 – Verhinderung von Datenlecks A-8.20 – Netzwerksicherheit
RTS IKT-Risikomanagement (2024/1774) – Art. 15	IKT-Projektmanagement	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.8 – Informationssicherheit im Projektmanagement
RTS IKT-Risikomanagement (2024/1774) – Art. 16	Beschaffung, Entwicklung und Wartung von IKT-Systemen	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.8 – Informationssicherheit im Projektmanagement A-8.11 – Datenmaskierung A-8.25 – Lebenszyklus einer sicheren Entwicklung A-8.26 – Anforderungen an die Anwendungssicherheit A-8.27 – Sichere Systemarchitektur und Entwicklungsgrundsätze A-8.28 – Sichere Codierung A-8.29 – Sicherheitsprüfung bei Entwicklung und Abnahme A-8.30 – Ausgegliederte Entwicklung A-8.31 – Trennung von Entwicklungs-, Test- und Produktionsumgebungen A-8.33 – Testdaten A-8.4 – Zugriff auf den Quellcode A-8.8 – Handhabung von technischen Schwachstellen
RTS IKT-Risikomanagement (2024/1774) – Art. 17	IKT-Änderungsmanagement	A-5.3 – Aufgabentrennung A-8.29 – Sicherheitsprüfung bei Entwicklung und Abnahme A-8.32 – Änderungssteuerung
RTS IKT-Risikomanagement (2024/1774) – Art. 18	Physische Sicherheit und Sicherheit vor Umweltereignissen	A-5.1 – Informationssicherheitspolitik und -richtlinien A-7.1 – Physische Sicherheitsperimeter A-7.13 – Instandhaltung von Geräten und Betriebsmitteln A-7.5 – Sicherheit von Geräten und Werten außerhalb der Räumlichkeiten A-7.7 – Aufgeräumte Arbeitsumgebung und Bildschirmsperren A-7.9 – Sicherheit von Werten außerhalb der Räumlichkeiten
RTS IKT-Risikomanagement (2024/1774) – Art. 19	Richtlinien für Personalpolitik	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.11 – Rückgabe von Werten A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-6.8 – Meldung von Informationssicherheitsereignissen
RTS IKT-Risikomanagement (2024/1774) – Art. 20	Identitätsmanagement	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.16 – Identitätsmanagement A-5.17 – Authentisierungsinformationen A-5.33 – Schutz von Aufzeichnungen
RTS IKT-Risikomanagement (2024/1774) – Art. 21	Zugangskontrolle	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.15 – Zugangssteuerung A-5.18 – Zugangsrechte A-5.3 – Aufgabentrennung A-5.33 – Schutz von Aufzeichnungen A-6.5 – Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung A-7.2 – Physischer Zutritt A-7.4 – Physische Sicherheitsüberwachung A-8.15 – Protokollierung A-8.2 – Privilegierte Zugangsrechte A-8.5 – Sichere Authentisierung
RTS IKT-Risikomanagement (2024/1774) – Art. 22	Richtlinien für die Behandlung IKT-bezogener Vorfälle	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse A-5.26 – Reaktion auf Informationssicherheitsvorfälle A-5.33 – Schutz von Aufzeichnungen
RTS IKT-Risikomanagement (2024/1774) – Art. 23	Erkennung anormaler Aktivitäten und Kriterien für die Erkennung IKT-bezogener Vorfälle und die Reaktion	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.33 – Schutz von Aufzeichnungen A-8.15 – Protokollierung A-8.16 – Überwachung von Aktivitäten
RTS IKT-Risikomanagement (2024/1774) – Art. 24	Komponenten der IKT-Geschäftsfortführungsleitlinie	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.29 – Informationssicherheit bei Störungen A-5.30 – IKT-Bereitschaft für Business-Continuity
RTS IKT-Risikomanagement (2024/1774) – Art. 25	Test des IKT-Geschäftsfortführungsplans	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.30 – IKT-Bereitschaft für Business-Continuity
RTS IKT-Risikomanagement (2024/1774) – Art. 26	IKT-Reaktions- und Wiederherstellungspläne	A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.29 – Informationssicherheit bei Störungen A-5.30 – IKT-Bereitschaft für Business-Continuity
RTS IKT-Risikomanagement (2024/1774) – Art. 27	Format und Inhalt des Berichts über die Überprüfung des IKT-Risikomanagementrahmens	A-5.35 – Unabhängige Überprüfung der Informationssicherheit ISMS-9 – Bewertung der Leistung
RTS IKT-Risikomanagement (2024/1774) – Art. 28 – 42	*Keine unmittelbaren Anforderungen an Finanzunternehmen – keine Sollmaßnahmen abgeleitet*	

Rechtsquelle / Artikel	Artikelüberschrift	ISO-Controls
RTS IKT-Drittparteien (2024/1773) – Art. 1	Gesamtrisikoprofil und -komplexität	A-5.1 – Informationssicherheitspolitik und -richtlinien
RTS IKT-Drittparteien (2024/1773) – Art. 2	*Keine Sollmaßnahmen abgeleitet – Fokus auf Anwendung in Finanzgruppen*	
RTS IKT-Drittparteien (2024/1773) – Art. 3	Governance-Regelungen	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.35 – Unabhängige Überprüfung der Informationssicherheit
RTS IKT-Drittparteien (2024/1773) – Art. 4	Hauptphasen des Lebenszyklus mit Blick auf die Annahme und Nutzung vertraglicher Vereinbarungen	A-5.1 – Informationssicherheitspolitik und -richtlinien
RTS IKT-Drittparteien (2024/1773) – Art. 5	Ex-ante-Risikobewertung	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.19 – Informationssicherheit in Lieferantenbeziehungen
RTS IKT-Drittparteien (2024/1773) – Art. 6	Sorgfaltspflicht	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.19 – Informationssicherheit in Lieferantenbeziehungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.35 – Unabhängige Überprüfung der Informationssicherheit
RTS IKT-Drittparteien (2024/1773) – Art. 7	Interessenkonflikte	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen
RTS IKT-Drittparteien (2024/1773) – Art. 8	Vertragsklauseln	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-5.35 – Unabhängige Überprüfung der Informationssicherheit
RTS IKT-Drittparteien (2024/1773) – Art. 9	Überwachung der vertraglichen Vereinbarungen	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A-6.8 – Meldung von Informationssicherheitsereignissen
RTS IKT-Drittparteien (2024/1773) – Art. 10	Ausstieg aus und Beendigung von vertraglichen Vereinbarungen	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
RTS IKT-Drittparteien (2024/1773) – Art. 11	*Inkrafttreten – keine Sollmaßnahmen abgeleitet*	
RTS Untervergabe (2025/532) – Art. 1	Gesamtrisikoprofil und Komplexität	A-5.21 – Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)
RTS Untervergabe (2025/532) – Art. 2	Anwendung auf eine Gruppe	A-5.21 – Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)
RTS Untervergabe (2025/532) – Art. 3	Sorgfaltspflicht und Risikobewertung in Bezug auf den Einsatz von Unterauftragnehmern	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.21 – Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)
RTS Untervergabe (2025/532) – Art. 4	Bedingungen für die Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen	A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
RTS Untervergabe (2025/532) – Art. 5	Wesentliche Änderungen an Unterauftragsvereinbarungen über IKT-Dienstleistungen	A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen A-5.22 – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen ISMS-8.2 – Informationssicherheitsrisikobeurteilung
RTS Untervergabe (2025/532) – Art. 6	Kündigung des Vertrags zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister	A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen
RTS Untervergabe (2025/532) – Art. 7	*Inkrafttreten – keine Sollmaßnahmen abgeleitet*	
RTS Incident-Klassifizierung (2024/1772) – Art. 1	Kunden, finanzielle Gegenparteien und Transaktionen	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse
RTS Incident-Klassifizierung (2024/1772) – Art. 2	Reputationsschaden	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse
RTS Incident-Klassifizierung (2024/1772) – Art. 3	Dauer und Ausfallzeit des Dienstes	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse
RTS Incident-Klassifizierung (2024/1772) – Art. 4	Geografische Ausbreitung	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse
RTS Incident-Klassifizierung (2024/1772) – Art. 5	Verluste von Daten	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse
RTS Incident-Klassifizierung (2024/1772) – Art. 6	Kritikalität der betroffenen Dienste	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse
RTS Incident-Klassifizierung (2024/1772) – Art. 7	Wirtschaftliche Auswirkungen	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse
RTS Incident-Klassifizierung (2024/1772) – Art. 8	Schwerwiegende Vorfälle	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse

Rechtsquelle / Artikel	Artikelüberschrift	ISO-Controls
RTS Incident-Klassifizierung (2024/1772) – Art. 9	Wesentlichkeitsschwellen für die Bestimmung schwerwiegender Vorfälle	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse
RTS Incident-Klassifizierung (2024/1772) – Art. 10	Hohe Wesentlichkeitsschwellen für die Bestimmung erheblicher Cyberbedrohungen	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse
RTS Incident-Klassifizierung (2024/1772) – Art. 11 – 13	*(Relevanz schwerwiegender Vorfälle für die zuständigen Behörden in anderen Mitgliedstaaten) - Keine unmittelbaren Anforderungen an Finanzunternehmen – keine Sollmaßnahmen abgeleitet*	
RTS Incident-Meldung (2025/301) – Art. 1	Allgemeine Informationen in Erst-, Zwischen- und Abschlussmeldungen	A-6.8 – Meldung von Informationssicherheitsereignissen
RTS Incident-Meldung (2025/301) – Art. 2	Spezifische Informationen in Erstmeldungen	A-6.8 – Meldung von Informationssicherheitsereignissen
RTS Incident-Meldung (2025/301) – Art. 3	Spezifische Informationen in Zwischenmeldungen	A-6.8 – Meldung von Informationssicherheitsereignissen
RTS Incident-Meldung (2025/301) – Art. 4	Spezifische Informationen in Abschlussmeldungen	A-6.8 – Meldung von Informationssicherheitsereignissen
RTS Incident-Meldung (2025/301) – Art. 5	Fristen für die Erst-, Zwischen- und Abschlussmeldung	A-6.8 – Meldung von Informationssicherheitsereignissen
RTS Incident-Meldung (2025/301) – Art. 6	Inhalt der freiwilligen Meldung erheblicher Cyberbedrohungen	A-6.8 – Meldung von Informationssicherheitsereignissen
RTS Incident-Meldung (2025/301) – Art. 7	*Inkrafttreten – keine Sollmaßnahmen abgeleitet*	
RTS TLPT (2025/1190) – Art. 1	Begriffsbestimmungen	Kein Treffer – —
RTS TLPT (2025/1190) – Art. 2 und 3	*Keine unmittelbaren Anforderungen an Finanzunternehmen – keine Sollmaßnahmen abgeleitet*	
RTS TLPT (2025/1190) – Art. 4	Von den Finanzunternehmen zu treffende organisatorische Vorkehrungen	Kein Treffer – —
RTS TLPT (2025/1190) – Art. 5	Risikomanagement bei TLPT	Kein Treffer – —
RTS TLPT (2025/1190) – Art. 6	Risikomanagement bei gebündelten oder gemeinsamen TLPT	Kein Treffer – —
RTS TLPT (2025/1190) – Art. 7	Auswahl der TLPT-Anbieter	Kein Treffer – —
RTS TLPT (2025/1190) – Art. 8	*(Besondere Anforderungen bei gebündelten oder gemeinsamen TLPT) - Keine unmittelbaren Anforderungen an Finanzunternehmen – keine Sollmaßnahmen abgeleitet*	
RTS TLPT (2025/1190) – Art. 9	Vorbereitungsphase	Kein Treffer – —
RTS TLPT (2025/1190) – Art. 10	Testphase: Bedrohungsanalyse	Kein Treffer – —
RTS TLPT (2025/1190) – Art. 11	Testphase: Red-Team-Test	Kein Treffer – —
RTS TLPT (2025/1190) – Art. 12	Abschlussphase	Kein Treffer – —
RTS TLPT (2025/1190) – Art. 13	Plan mit Abhilfemaßnahmen	Kein Treffer – —
RTS TLPT (2025/1190) – Art. 14	*(Bescheinigung) Keine unmittelbaren Anforderungen an Finanzunternehmen – keine Sollmaßnahmen abgeleitet*	
RTS TLPT (2025/1190) – Art. 15	Einsatz interner Tester	A-5.1 – Informationssicherheitspolitik und -richtlinien Kein Treffer – —
RTS TLPT (2025/1190) – Art. 16 und 17	*Keine unmittelbaren Anforderungen an Finanzunternehmen – keine Sollmaßnahmen abgeleitet*	
ITS Incident-Reporting (2025/302) – Art. 1	Vorlage für die Meldung schwerwiegender IKT-bezogener Vorfälle	A-6.8 – Meldung von Informationssicherheitsereignissen
ITS Incident-Reporting (2025/302) – Art. 2	Gleichzeitige Übermittlung der Erst-, Zwischen- und Abschlussmeldung	A-6.8 – Meldung von Informationssicherheitsereignissen
ITS Incident-Reporting (2025/302) – Art. 3	Wiederholte IKT-bezogene Vorfälle	A-6.8 – Meldung von Informationssicherheitsereignissen
ITS Incident-Reporting (2025/302) – Art. 4	Nutzung sicherer elektronischer Kanäle	A-6.8 – Meldung von Informationssicherheitsereignissen
ITS Incident-Reporting (2025/302) – Art. 5	Rückstufung schwerwiegender IKT-bezogener Vorfälle	A-6.8 – Meldung von Informationssicherheitsereignissen
ITS Incident-Reporting (2025/302) – Art. 6	Unterrichtung über die Auslagerung der Berichtspflichten	A-6.8 – Meldung von Informationssicherheitsereignissen
ITS Incident-Reporting (2025/302) – Art. 7	Aggregierte Meldung	A-6.8 – Meldung von Informationssicherheitsereignissen
ITS Incident-Reporting (2025/302) – Art. 8	Meldung erheblicher Cyberbedrohungen	A-6.8 – Meldung von Informationssicherheitsereignissen
ITS Incident-Reporting (2025/302) – Art. 9	*Inkrafttreten – keine Sollmaßnahmen abgeleitet*	
ITS Informationsregister (2024/2956) – Art. 1	*Begriffsbestimmungen – keine Sollmaßnahmen abgeleitet*	

Rechtsquelle / Artikel	Artikelüberschrift	ISO-Controls
ITS Informationsregister (2024/2956) – Art. 2	Erstellung einer Rangfolge von IKT-Drittdienstleistern in der Dienstleistungskette	A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen
ITS Informationsregister (2024/2956) – Art. 3	Allgemeine Anforderungen an die Vorlagen des Informationsregisters	A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen
ITS Informationsregister (2024/2956) – Art. 4	Anforderung an das Datenformat	A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen
ITS Informationsregister (2024/2956) – Art. 5	Inhalt des Informationsregisters	A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen
ITS Informationsregister (2024/2956) – Art. 6	Anwendungsbereich des Informationsregisters auf teilkonsolidierter und konsolidierter Ebene	A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen
ITS Informationsregister (2024/2956) – Art. 7	*Inkrafttreten – keine Sollmaßnahmen abgeleitet*	
ITS Informationsregister (2024/2956) – Annex III	Anhang – Vorlagen für das Informationsregister	A-5.1 – Informationssicherheitspolitik und -richtlinien A-5.20 – Behandlung von Informationssicherheit in Lieferantenvereinbarungen
GL Kosten & Verluste (JC 2024 34) – Leitlinie	Schätzung aggregierter Kosten und Verluste	A-5.25 – Beurteilung und Entscheidung über Informationssicherheitsereignisse

DORA-Sollmaßnahmenkatalog

ISMS-4 – Kontext der Organisation

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
	Kein DORA-Mapping vorhanden – siehe A-5.1.003	

ISMS-4.1 – Verstehen der Organisation und ihres Kontextes

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
Proportionalitätsprinzip | *Anforderung an die Operationalisierung*		
ISMS-4.1.001	Das Finanzunternehmen soll die DORA-Anforderungen verhältnismäßig umsetzen und bei der Entwicklung und Implementierung von IKT-Sicherheitsrichtlinien, -verfahren, -protokollen und -tools die Größe des Finanzunternehmens, das Gesamtrisikoprofil sowie die Komplexität der Dienstleistungen, Aktivitäten und Geschäftsprozesse berücksichtigen. *(Vgl. Art. 1 RTS IKT-Risikomanagement, Art. 4 (1 & 2) DORA)*	ISMS-4.3

ISMS-4.2 – Verstehen der Erfordernisse und Erwartungen interessierter Parteien

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
	Kein DORA-Mapping vorhanden	

ISMS-4.3 – Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
	Kein DORA-Mapping vorhanden	

ISMS-4.4 – Informationssicherheitsmanagementsystem

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
Implementierung des IKT-Risikomanagementrahmens | *Anforderung an die Operationalisierung*		
ISMS-4.4.001	Das Finanzunternehmen soll einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen als Bestandteil des Gesamtrisikomanagementsystems implementieren, um IKT-Risiken wirksam zu steuern und eine hohe digitale operationale Resilienz sicherzustellen. *(Vgl. Art. 6 (1) DORA)*	
Komponenten des IKT-Risikomanagementrahmens | *Anforderung an die Operationalisierung*		
ISMS-4.4.002	Das Finanzunternehmen soll sicherstellen, dass der IKT-Risikomanagementrahmen geeignete Strategien, Richtlinien, Verfahren sowie IKT-Protokolle und -Tools umfasst, um Informations- und IKT-Assets sowie relevante physische Komponenten wie Gebäude, Rechenzentren und sensible Bereiche vor Risiken wie Beschädigung, unbefugtem Zugriff oder Missbrauch zu schützen. *(Vgl. Art. 6 (2) DORA)*	
Zielsetzung des IKT-Risikomanagementrahmens | *Anforderung an die Operationalisierung*		
ISMS-4.4.003	Das Finanzunternehmen soll die Sicherheit und Funktionsfähigkeit der IKT-Systeme durch IKT-Sicherheitsrichtlinien, IKT-Sicherheitsverfahren und unterstützende Sicherheitstools gewährleisten und dadurch die unmittelbaren Auswirkungen von IKT-Risiken auf den laufenden IKT-Betrieb begrenzen. *(Vgl. Art. 9 (1) DORA)*	

ISMS-5 – Führung

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
	Kein DORA-Mapping vorhanden	

ISMS-5.1 – Führung und Verpflichtung

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
	Kein DORA-Mapping vorhanden	

ISMS-5.2 – Politik

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
DOR-Strategie | *Anforderung an die Strategien*		
ISMS-5.2.001	Das Finanzunternehmen soll eine Strategie für digitale operative Resilienz (DOR-Strategie) dokumentieren und pflegen, die die Umsetzung des IKT-Risikomanagementrahmens beschreibt und Methoden zur Bewältigung von IKT-Risiken sowie zur Erreichung spezifischer IKT-Ziele festlegt. *(Vgl. Art. 6 (8) DORA)*	ISMS-6.2, A-5.1
Informationssicherheitsleitlinie | *Anforderung an die Richtlinien und Leitlinien*		
ISMS-5.2.002	Das Finanzunternehmen soll eine Informationssicherheitsleitlinie entwickeln und dokumentieren, die Vorgaben zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten, Informationswerten und IKT-Assets, einschließlich der Kundendaten, festlegt. *(Vgl. Art. 9 (4a) DORA, Art. 2 (2) RTS IKT-Risikomanagement)*	A-5.1

ISMS-5.3 – Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
Governance- und Kontrollrahmen | *Anforderung an die Operationalisierung*		
ISMS-5.3.001	Das Finanzunternehmen soll klare Steuerungs-, Kontroll- und Überwachungsstrukturen für IKT-Risiken etablieren, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen. *(Vgl. Art. 5 (1) DORA)*	A-5.3

ISMS-6 – Planung

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
	Kein DORA-Mapping vorhanden	

ISMS-6.1 – Maßnahmen zum Umgang mit Risiken und Chancen

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
	Kein DORA-Mapping vorhanden	

ISMS-6.1.1 – Allgemeines

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
	Kein DORA-Mapping vorhanden	

...

Weitere Sollmaßnahmen in der Vollversion

A-5.3 – Aufgabentrennung

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
Funktionstrennung (Drei-Linien-Modell) | *Anforderung an die Operationalisierung*		
A-5.3.001	Das Finanzunternehmen soll eine angemessene Trennung und Unabhängigkeit zwischen der IKT-Risikomanagementfunktion (1. Verteidigungslinie), der IKT-Risikokontrollfunktion (2. Verteidigungslinie) und der internen Revisionsfunktion (3. Verteidigungslinie) gemäß dem Drei-Linien-Modell sicherstellen. *(Vgl. Art. 6 (4) DORA)*	
Aufgabentrennung bei der Berechtigungsvergabe | *Anforderung an die Operationalisierung*		
A-5.3.002	Das Finanzunternehmen soll sicherstellen, dass bei der Berechtigungsvergabe das Prinzip der Trennung der Aufgaben (Segregation of Duties) eingehalten wird und keine unzulässigen Berechtigungskombinationen umgesetzt werden. *(Vgl. Art. 21 (1b) RTS IKT-Risikomanagement)*	
Erkennung und Behebung von SoD-Konflikten | *Anforderung an die Operationalisierung*		
A-5.3.003	Das Finanzunternehmen soll sicherstellen, dass Kontrollen zur Erkennung und Behebung von SoD-Konflikten umgesetzt sind und dass Ausnahmen konform zu den internen Vorgaben gehandhabt werden. *(Vgl. Art. 21 (1b) RTS IKT-Risikomanagement)*	

A-5.4 – Verantwortlichkeiten der Leitung

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
Genehmigung und Überwachung des IKT-Risikomanagementrahmens | *Anforderung an die Operationalisierung*		
A-5.4.001	Das Leitungsorgan soll verantwortlich sein für die Definition, Genehmigung, Überwachung und Umsetzung des IKT-Risikomanagementrahmens. *(Vgl. Art. 5 (2) DORA)*	ISMS-5.1
Letztverantwortung für das IKT-Risikomanagement | *Anforderung an die Operationalisierung*		
A-5.4.002	Das Leitungsorgan soll die letztendliche Verantwortung für das Management der IKT-Risiken des Finanzunternehmens tragen. *(Vgl. Art. 5 (2a) DORA)*	ISMS-5.1
Festlegung von Leitlinien und IKT-Sicherheitsrichtlinien | *Anforderung an die Operationalisierung*		
A-5.4.003	Das Leitungsorgan soll geeignete Leitlinien und IKT-Sicherheitsrichtlinien festlegen, um hohe Standards für die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten sicherzustellen. *(Vgl. Art. 5 (2b) DORA)*	ISMS-5.1
Festlegung von Rollen und Koordination der IKT-Funktionen | *Anforderung an die Operationalisierung*		
A-5.4.004	Das Leitungsorgan soll sicherstellen, dass Rollen, Zuständigkeiten und Abstimmungswege zwischen allen IKT-bezogenen Funktionen klar geregelt sind, sodass Kommunikation, Zusammenarbeit und Koordination reibungslos erfolgen. *(Vgl. Art. 5 (2c) DORA)*	ISMS-5.1
Genehmigung der DOR-Strategie und Risikotoleranz | *Anforderung an die Operationalisierung*		
A-5.4.005	Das Leitungsorgan soll verantwortlich sein für die Festlegung und Genehmigung der DOR-Strategie einschließlich der Festlegung des IKT-Risikotoleranzniveaus. *(Vgl. Art. 5 (2d) DORA)*	ISMS-5.1
Genehmigung der IKT-Geschäftsfortführungspläne | *Anforderung an die Operationalisierung*		
A-5.4.006	Das Leitungsorgan soll die IKT-Geschäftsfortführungsleitlinie sowie die IKT-Reaktions- und Wiederherstellungspläne genehmigen, überwachen und regelmäßig überprüfen. *(Vgl. Art. 5 (2e) DORA)*	ISMS-5.1
Genehmigung der IKT-Auditpläne | *Anforderung an die Operationalisierung*		

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
A-5.4.007	Das Leitungsorgan soll die internen IKT-Revisionspläne, die Durchführung der IKT-Revision sowie wesentliche Änderungen daran genehmigen und regelmäßig überprüfen. *(Vgl. Art. 5 (2f) DORA)*	ISMS-5.1
Genehmigung der Leitlinien zur Nutzung von IKT-Dienstleistungen | *Anforderung an die Operationalisierung*		
A-5.4.008	Das Leitungsorgan soll die Leitlinien zur Nutzung von IKT-Dienstleistungen genehmigen und regelmäßig überprüfen. *(Vgl. Art. 5 (2h) DORA)*	ISMS-5.1
Berichtskanäle für IKT-Dienstleistungsvereinbarungen | *Anforderung an die Operationalisierung*		
A-5.4.009	Das Leitungsorgan soll geeignete Berichtskanäle einrichten, um informiert zu werden über • Vereinbarungen mit IKT-Dienstleistern, • geplante wesentliche Änderungen bei IKT-Dienstleistern, • die Auswirkungen und Risiken solcher Änderungen auf kwF, einschließlich einer Zusammenfassung von Ex-ante Risk Assessment und Due Diligence Prüfung, sowie • schwerwiegende IKT-bezogene Vorfälle und die ergriffenen Gegen-, Wiederherstellungs- und Korrekturmaßnahmen *(Vgl. Art. 5 (2i) DORA)*	ISMS-5.1
Jährliche IKT-Berichterstattung an das Leitungsorgan | *Anforderung an die Operationalisierung*		
A-5.4.010	Leitende IKT-Mitarbeiter sollen dem Leitungsorgan mindestens einmal jährlich über vorliegende Erkenntnisse und IKT-Risiken berichten. Der Bericht soll insbesondere Erkenntnisse und IKT-Risiken umfassen aus: • Tests zur digitalen operationalen Resilienz • IKT-bezogenen Vorfällen und Cyberangriffen • der Aktivierung von IKT-Geschäftsfortführungsplänen sowie von IKT-Reaktions- und Wiederherstellungsplänen • Informationen von Gegenparteien sowie aufsichtlichen Überprüfungen *(Vgl. Art. 13 (5) DORA)*	ISMS-5.1
Überprüfung der Risiken kritischer IKT-Verträge | *Anforderung an die Operationalisierung*		
A-5.4.011	Das Finanzunternehmen soll sicherstellen, dass das Leitungsorgan die Risiken im Zusammenhang mit kwF-relevanten IKT-Verträgen regelmäßig überprüft und dabei das Gesamtrisikoprofil sowie den Umfang und die Komplexität der Dienstleistungen berücksichtigt. *(Vgl. Art. 28 (2) DORA)*	ISMS-5.1

...

Weitere Sollmaßnahmen in der Vollversion

A-5.12 – Klassifizierung von Informationen

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
Verfahren zum IKT-Assetmanagement | *Anforderung an die Governance-Verfahren und -Methoden*		
A-5.12.001	Das Finanzunternehmen soll ein Verfahren zum IKT-Assetmanagement entwickeln, dokumentieren und implementieren, das die Vorgaben zur Ermittlung der Kritikalität von Assets enthält. *(Vgl. Art. 5 (1) RTS IKT-Risikomanagement)*	
A-5.12.002	Das Verfahren zum IKT-Assetmanagement soll festlegen, wie die Kritikalität von Informationsassets und IKT-Assets bewertet wird und welche Kriterien hierfür anzuwenden sind. In der Praxis wird hierfür häufig die Methodik der Schutzbedarfsanalyse verwendet. *(Vgl. Art. 5 (2) RTS IKT-Risikomanagement)*	
A-5.12.003	Das Finanzunternehmen soll eine Methodik zur Ermittlung der kritischen oder wichtigen Funktionen (kwF) definieren und dokumentieren. Sofern diese Methodik nicht an anderer Stelle geregelt ist, bietet es sich an, sie im Verfahren zum IKT-Assetmanagement festzulegen. Das Verfahren soll außerdem festlegen, dass neue kritische oder wichtige Funktionen (kwF) der zuständigen Aufsichtsbehörde zu melden sind. *(Vgl. Art. 8 (1) DORA, Art. 28 (3) DORA)*	
Klassifizierung von IKT-Assets nach Kritikalität | *Anforderung an die Operationalisierung*		
A-5.12.004	Das Finanzunternehmen soll alle Informationsassets und IKT-Assets identifizieren und diese hinsichtlich ihrer Kritikalität (Schutzbedarf) klassifizieren. *(Vgl. Art. 8 (1) DORA)*	
Regelmäßige Überprüfung der Schutzbedarfsklassifizierung | *Anforderung an die Operationalisierung*		
A-5.12.005	Die Schutzbedarfsklassifizierung der Informationsassets und IKT-Assets sowie die zugehörige Dokumentation sollen regelmäßig überprüft und bei Bedarf aktualisiert werden, mindestens jedoch einmal jährlich. *(Vgl. Art. 8 (1) DORA)*	
Berücksichtigung des IKT-Risikos bei der Schutzbedarfsklassifizierung | *Anforderung an die Operationalisierung*		
A-5.12.006	Bei der Schutzbedarfsklassifizierung von Informationsassets und IKT-Assets sollen das mit den unterstützten Geschäftsprozessen verbundene IKT-Risiko sowie die Abhängigkeiten dieser Geschäftsprozesse von den Informationsassets und IKT-Assets berücksichtigt werden. *(Vgl. Art. 5 (2a) RTS IKT-Risikomanagement)*	
Klassifizierung der Schutzbedarfe nach Schutzzielen | *Anforderung an die Operationalisierung*		
A-5.12.007	Bei der Schutzbedarfsklassifizierung von Informationsassets und IKT-Assets sollen die möglichen Auswirkungen eines Verlusts der Vertraulichkeit, Integrität und Verfügbarkeit dieser Assets auf die unterstützten Geschäftsprozesse und -tätigkeiten berücksichtigt werden. *(Vgl. Art. 5 (2b) RTS IKT-Risikomanagement)*	
Klassifizierung von Geschäftsprozessen als kwF | *Anforderung an die Operationalisierung*		
A-5.12.008	Das Finanzunternehmen soll alle IKT-unterstützten Geschäftsprozesse identifizieren und diese systematisch als kritische oder wichtige Funktionen (kwF) oder als nicht kritische bzw. nicht wichtige Funktionen klassifizieren. *(Vgl. Art. 8 (1) DORA)*	
Überprüfung der Einstufung von kwF | *Anforderung an die Operationalisierung*		
A-5.12.009	Die Klassifizierung der IKT-unterstützten Geschäftsprozesse als kritische oder wichtige Funktionen (kwF) oder als nicht kritische bzw. nicht wichtige Funktionen soll regelmäßig überprüft und bei Bedarf aktualisiert werden, mindestens jedoch einmal jährlich. *(Vgl. Art. 8 (1) DORA)*	

...

Weitere Sollmaßnahmen in der Vollversion

A-5.35 – Unabhängige Überprüfung der Informationssicherheit

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
Verfahren zur Nachverfolgung von IKT-Mängeln | *Anforderung an die Governance-Verfahren und -Methoden*		
A-5.35.001	Das Finanzunternehmen soll ein formelles Follow-up-Verfahren einrichten, das Regeln für die zeitnahe Überprüfung und Nachverfolgung kritischer Feststellungen der IKT-Revision festlegt. *(Vgl. Art. 6 (7) DORA)*	
(IKT-) Revisionspläne | *Anforderung an die Pläne*		
A-5.35.002	Das Finanzunternehmen soll (IKT-)Revisionspläne erstellen, dokumentieren und implementieren, um sicherzustellen, dass der IKT-Risikomanagementrahmen regelmäßig durch die interne Revision geprüft wird. Umfang und Frequenz der Prüfungen sollen den IKT-Risiken des Finanzunternehmens entsprechen. *(Vgl. Art. 6 (6) DORA)*	
A-5.35.003	Das Finanzunternehmen soll (IKT-)Revisionspläne erstellen, dokumentieren und implementieren, die sicherstellen, dass die IKT-Reaktions- und Wiederherstellungspläne regelmäßig und unabhängig durch die interne Revision überprüft werden. *(Vgl. Art. 11 (3) DORA)*	
A-5.35.004	Das Finanzunternehmen soll (IKT-)Revisionspläne erstellen, dokumentieren und implementieren, die sicherstellen, dass kwF-relevante IKT-Dienstleistungen regelmäßig einer unabhängigen Überprüfung unterzogen werden. *(Vgl. Art. 3 (7) RTS IKT-Drittparteien)*	A-5.22
Nachweise der internen Revision zur DL-Überwachung | *Anforderung an die Operationalisierung*		
A-5.35.005	Die interne Revision kann bei der Überprüfung und Überwachung von IKT-Dienstleistern auf unterschiedliche Nachweise zurückgreifen. Hierzu zählen insbesondere: • eigene Audits oder Bewertungen • unabhängige Prüfberichte des IKT-Dienstleisters • interne Prüfberichte des IKT-Dienstleisters • geeignete Zertifizierungen Dritter • weitere relevante vom IKT-Dienstleister bereitgestellte Informationen *(Vgl. Art. 6 (3, a - e) RTS IKT-Drittparteien)*	A-5.22
Prüf- und Kontrollmaßnahmen zur DL-Überwachung | *Anforderung an die Operationalisierung*		
A-5.35.006	Das Finanzunternehmen soll zur Überwachung von IKT-Dienstleistern geeignete Prüf- und Kontrollmaßnahmen nutzen, z. B. interne oder externe Audits, gemeinsame Audits und IKT-Tests mit anderen Nutzern sowie Zertifizierungen und Auditberichte Dritter. *(Vgl. Art. 8 (2, a-d) RTS IKT-Drittparteien)*	A-5.22
Prüfung von IKT-Systemen | *Anforderung an die Operationalisierung*		
A-5.35.007	Das Finanzunternehmen soll sicherstellen, dass Prüfungen der internen Revision sowie sonstige Testaktivitäten an IKT-Systemen so geplant und durchgeführt werden, dass sie nicht zu unangemessenen Störungen des laufenden Geschäftsbetriebs führen. *(Vgl. Art. 8 (2b, iv) RTS IKT-Risikomanagement)*	A-8.34
Prüfung des IKT-Risikomanagementrahmens | *Anforderung an die Operationalisierung*		
A-5.35.008	Das Finanzunternehmen soll sicherstellen, dass relevante Inhalte der Berichte der internen Revision in den Bericht zur Überprüfung des IKT-Risikomanagementrahmens einfließen. *(Vgl. Art. 27 (2k) RTS IKT-Risikomanagement)*	

...

Weitere Sollmaßnahmen in der Vollversion

A-8.17 – Uhrensynchronisation

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
Uhrensynchronisation | *Anforderung an die Operationalisierung*		
A-8.17.001	Das Finanzunternehmen soll die Systemuhren aller IKT-Systeme auf Grundlage einer dokumentierten, zuverlässigen Referenzzeitquelle (z. B. NTP-Server) synchronisieren, um eine konsistente und korrelierbare Zeitstempelung sicherzustellen. *(Vgl. Art. 12 (2f) RTS IKT-Risikomanagement)*	

A-8.18 – Gebrauch von Hilfsprogrammen mit privilegierten Rechten

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
	Kein DORA-Mapping vorhanden	

A-8.19 – Installation von Software auf Systemen im Betrieb

DORA-ID	DORA-Sollmaßnahmen	Weitere ISO-Mappings
Verfahren zur Daten- und Systemsicherheit: Softwarefreigabe | *Anforderung an die Governance-Verfahren und -Methoden*		
A-8.19.001	Das Verfahren zur Daten- und Systemsicherheit soll Maßnahmen festlegen, die sicherstellen, dass ausschließlich zugelassene und freigegebene Software auf IKT-Systemen und Endgeräten installiert wird, beispielsweise durch Application-Whitelisting, zentrale Softwareverteilung oder Freigabeprozesse. *(Vgl. Art. 11(2c) RTS IKT-Risikomanagement)*	A-5.1
Installation von Software auf Systemen im Betrieb | *Anforderung an die Operationalisierung*		
A-8.19.002	Das Finanzunternehmen soll die erforderlichen technischen und organisatorischen Maßnahmen umsetzen, um sicherzustellen, dass auf IKT-Systemen und Endgeräten ausschließlich zugelassene und freigegebene Software installiert und betrieben wird, z. B. durch Application-Whitelisting, zentrale Softwareverteilung sowie definierte Freigabe- und Ausnahmeprozesse. *(Vgl. Art. 11(2c) RTS IKT-Risikomanagement)*	

Vorschau-Version

Dies ist eine Vorschau des DORA-Sollmaßnahmenkatalogs.
Der vollständige Katalog mit allen 1.039 Sollmaßnahmen ist ab sofort verfügbar.

Weitere Informationen finden Sie unter
www.marlen-hofmann.de/digitale-produkte/