DORA-Puzzle Kompakt

Ein Anforderungskatalog zur Umsetzung der
Verordnung (EU) 2022/2554 (DORA)

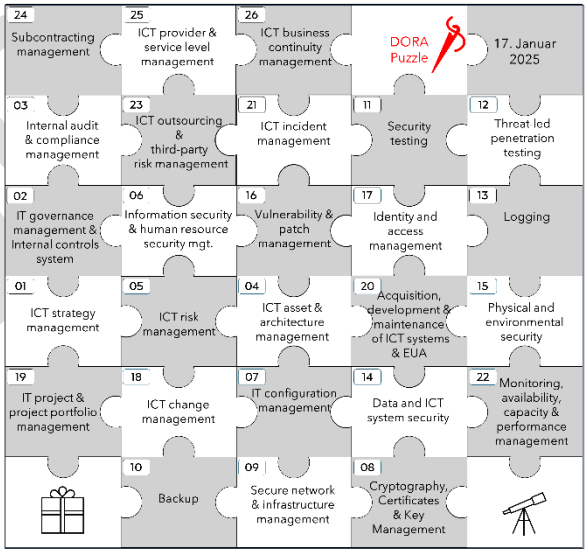
Version 1.0

Dr. Marlen Hofmann

Leseprobe

Vorwort

DORA Puzzle



Die rasante Digitalisierung hat den Finanzsektor in den letzten Jahren tiefgreifend verändert. Finanzinstitute stützen sich zunehmend auf Informations- und Kommunikationstechnologien (IKT), um ihre Kernprozesse zu optimieren und ihre Dienstleistungen effizient sowie sicher zu erbringen. Diese Entwicklung bringt jedoch auch erhebliche Herausforderungen mit sich: Cyberangriffe, IKT-Ausfälle und technische Störungen stellen nicht nur eine Bedrohung für einzelne Institute dar, sondern können auch die Stabilität des gesamten Finanzsystems gefährden.

Um diesen Risiken zu begegnen und die digitale Widerstandsfähigkeit der Finanzinstitute zu stärken, hat die Europäische Union die Verordnung (EU) 2022/2554, bekannt als DORA (Digital Operational Resilience Act), eingeführt. Diese Verordnung legt klare Anforderungen an das IKT-Risikomanagement, die Sicherheitsstrukturen und die Zusammenarbeit mit externen IKT-Dienstleistern fest.

Der vorliegende Anforderungskatalog fasst die DORA-Vorgaben in 26 fachliche Domänen zusammen, die das sogenannte DORA-Puzzle bilden. Das Puzzle entstand durch eine strukturierte Analyse der Verordnung sowie der dazugehörigen technischen Regulierungsstandards (RTS), Implementierungsstandards (ITS) und Guidelines. Ziel dieser Analyse war es, zentrale Ergebnistypen zu identifizieren, die im Rahmen von DORA-Projekten erstellt oder überprüft werden müssen. Die Analyse führte zur Erstellung eines ersten Katalogs von rund 500 Anforderungen (DORA Deep Dive V1.0), die später durch eine Detailanalyse auf ca. 1.500 Einzelanforderungen erweitert wurden (DORA Deep Dive V2.0). Um die Anwendbarkeit des Katalogs zu erleichtern, wurden diese Anforderungen in 26 Domänen gegliedert, die alle wichtigen Bereiche der DORA-Umsetzung adressieren – von der strategischen Steuerung der IKT-Risiken bis hin zu spezifischen Vorgaben für die Zusammenarbeit mit externen IKT-Dienstleistern.

Domain 01 ICT strategy management
Domain 02 IT governance management & Internal controls system
Domain 03 Internal audit and compliance management
Domain 04 ICT asset & architecture management
Domain 05 ICT risk management
Domain 06 Information security & human resource (security) management
Domain 07 IT configuration management
Domain 08 Cryptography, Certificates & Key Management
Domain 09 Secure network & infrastructure management
Domain 10 Backup
Domain 11 Security testing
Domain 12 Threat-led penetration testing
Domain 13 Logging
Domain 14 Data and ICT system security
Domain 15 Physical and environmental security
Domain 16 Vulnerability & patch management
Domain 17 Identity and access management
Domain 18 ICT change management
Domain 19 IT project & project portfolio management
Domain 20 Acquisition, development & maintenance of ICT systems & EUA
Domain 21 ICT incident management
Domain 22 Monitoring, Availability, Capacity & Performance Management
Domain 23 ICT outsourcing & third-party risk management
Domain 24 Subcontracting management
Domain 25 ICT provider & service level management
Domain 26 ICT business continuity management

Das vorliegende Dokument beinhaltet eine kompakte und zusammengefasste Übersicht über die zentralen Anforderungen aus dem DORA Deep Dive 2.0 und enthält konkrete Referenzen auf die DORA-Verordnung sowie Checkfragen, die für die Überprüfung der DORA-Compliance herangezogen werden können.

Leseprobe

Quellen: Folgende Quellen bilden die Grundlage für den Anforderungskatalog:

- **REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022** on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
- **2024/1774 COMMISSION DELEGATED REGULATION (EU) 2024/1774 of 13 March 2024:** supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework
- **2024/1772 COMMISSION DELEGATED REGULATION (EU) 2024/1772 of 13 March 2024:** supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents
- **2024/1773 COMMISSION DELEGATED REGULATION (EU) 2024/1773 of 13 March 2024:** supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers
- **Final Report:** Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat
- **Final report:** on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554
- **Final Report**: Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554
- **Final Report:** On Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554

Compliance-Hinweise:

(1) Dieser Anforderungskatalog 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. Die Inhalte stellen keine offizielle Stellungnahme ihres Arbeitgebers dar und sollten nicht als solche interpretiert werden.

(2) Alle Anforderungen basieren auf einer detaillierten Auseinandersetzung mit der DORA-Verordnung sowie den relevanten Regulierungsstandards. Es wird ausdrücklich darauf hingewiesen, dass dieser Anforderungskatalog lediglich als Orientierungshilfe für die Umsetzung der DORA-Verordnung dient. Er erhebt keinen Anspruch auf Vollständigkeit oder rechtliche Verbindlichkeit. Die Verwendung dieses Dokuments ersetzt keine rechtliche Beratung. Die Autorin übernimmt keine Haftung für Schäden oder Verluste, die durch die Anwendung oder Interpretation dieses Anforderungskatalogs entstehen.

(3) Da regulatorische Anforderungen und technische Standards fortlaufend weiterentwickelt werden und insbesondere die Final Reports bisher nicht offiziell von der Europäischen Kommission veröffentlicht wurden, kann eine Aktualisierung des Anforderungskatalogs erforderlich sein. Es obliegt den Nutzern, sich eigenständig über Änderungen der relevanten Rechtsvorschriften und Standards zu informieren und diese bei der Umsetzung entsprechend zu berücksichtigen.

(4) Alle Inhalte, insbesondere Texte und Grafiken sind urheberrechtlich geschützt. Alle Rechte, einschließlich der Vervielfältigung, Veröffentlichung, Bearbeitung und Übersetzung, bleiben vorbehalten.

Leseprobe

Leseprobe

ID/ Thema	Anforderung (Kompakt)	Checkfrage	Referenz
	Domain 01 ICT strategy management		
sStrat_01: Definition and documentation of the DOR strategy:	Ihre Organisation muss eine Strategie zur digitalen Resilienz (DOR-Strategie) dokumentieren, die Methoden zur Bewältigung von IKT-Risiken, klare Sicherheitsziele und das Risikotoleranzniveau festlegt. Die Strategie muss die Unterstützung der Geschäftsziele durch den IKT-Risikomanagementrahmen erläutern, die IKT-Referenzarchitektur beschreiben und Mechanismen zur Erkennung, Vermeidung und Bewältigung von IKT-Vorfällen enthalten. Zudem müssen präventive Maßnahmen und Resilienztests dokumentiert, die aktuelle Risikosituation analysiert und eine Kommunikationsstrategie für Vorfälle definiert werden.	Beinhaltet die DOR-Strategie Methoden zur Risikobewältigung, Sicherheitsziele, das Risikotoleranzniveau, Vorfallserkennung, Resilienztests, präventive Maßnahmen und eine Kommunikationsstrategie?	Art. 6 (8) DORA
sStrat_02: Multi-vendor strategy	Falls erforderlich, sollte eine ganzheitliche IKT-Mehrlieferantenstrategie entwickelt werden, die innerhalb der DOR-Strategie die Abhängigkeiten von IKT-Drittanbietern und die Gründe für die Auswahl und Mischung der Anbieter detailliert beschreibt.	Wurde eine IKT-Mehrlieferantenstrategie definiert, die die Abhängigkeiten von IKT-Drittanbietern und die Beschaffungsgründe innerhalb der DOR-Strategie berücksichtigt?	Art. 6 (9) DORA
sStrat_03: Monitoring and adaptation of the DOR strategy:	Überwachen Sie die Umsetzung der DOR-Strategie und prüfen Sie regelmäßig deren Wirksamkeit. Behalten Sie technologische Entwicklungen im Blick und bewerten Sie kontinuierlich deren Auswirkungen auf die IKT-Sicherheitsanforderungen und die digitale Resilienz.	Wird die Wirksamkeit der DOR-Strategie überwacht und werden technologische Entwicklungen regelmäßig auf potenzielle Auswirkungen auf die IKT-Sicherheitsanforderungen und digitale Resilienz bewertet?	Art. 13 (4, 7) DORA
	Domain 02 IT governance management & Internal controls system		
sGov_01: Proportionality principle	Bei der Entwicklung und Implementierung von IKT-Sicherheitsrichtlinien und der Anwendung der DORA-Anforderungen muss das Prinzip der Verhältnismäßigkeit beachtet werden. Dabei sind die Größe, das Risikoprofil sowie die Art, der Umfang und die Komplexität der Dienstleistungen und Geschäftstätigkeiten des Unternehmens zu berücksichtigen.	Wird bei der Entwicklung und Implementierung von IKT-Sicherheitsrichtlinien und der Anwendung der DORA-Anforderungen das Prinzip der Verhältnismäßigkeit unter Berücksichtigung der Größe, des Risikoprofils sowie der Art, des Umfangs und der Komplexität der Unternehmensaktivitäten beachtet?	Art. 4 (1 & 2) DORA Art. 1 RTS risk mgt.
sGov_02: ICT Security Policies	Finanzunternehmen müssen IKT-Sicherheitsrichtlinien entwickeln, die mit den Informationssicherheitszielen ihrer DOR-Strategie übereinstimmen und Aspekte wie Verschlüsselung, IKT-Betrieb, Netzwerksicherheit sowie Projekt- und Änderungsmanagement abdecken. Diese Richtlinien müssen Risiken für Vertraulichkeit, Integrität und Verfügbarkeit von Daten adressieren und Störungen der Geschäftskontinuität berücksichtigen. Sie sollen formale Genehmigungen, Überwachungsmaßnahmen, Dokumentation von Ausnahmen, Verantwortlichkeiten, Sanktionen bei Nichteinhaltung und regelmäßige Überprüfungen umfassen und mindestens jährlich sowie nach wichtigen Vorfällen aktualisiert werden.	Decken die IKT-Sicherheitsrichtlinien alle relevanten Themen wie Verschlüsselung, IKT-Betrieb und Netzwerksicherheit ab, berücksichtigen sie IKT-Risiken für Daten, formale Genehmigungen, Sanktionen und Überprüfungen und werden sie mindestens jährlich sowie nach wesentlichen Ereignissen aktualisiert?	Art. 1, 2 RTS risk mgt.

Leseprobe

ID/ Thema	Anforderung (Kompakt)	Checkfrage	Referenz
sGov_03: Requirements for ICT risk mgt. policies	Finanzunternehmen müssen IKT-Risikomanagement-Richtlinien und -Verfahren entwickeln, dokumentieren und implementieren, die das genehmigte IKT-Risiko-Toleranzniveau beinhalten.	Sind IKT-Risikomanagement-Richtlinien und -Verfahren dokumentiert und implementiert und wird das genehmigte IKT-Risiko-Toleranzniveau eindeutig angeben?	Art. 3 (a) RTS risk mgt.
sGov_04: Governance and Control Framework:	Finanzunternehmen müssen ein Governance- und Kontrollrahmenwerk etablieren, um ein wirksames IKT-Risikomanagement und hohe digitale Resilienz sicherzustellen. Die Geschäftsleitung trägt die Verantwortung für die Definition, Genehmigung und Überwachung aller IKT-Sicherheits- und -Risikomanagementrichtlinien, einschließlich der Festlegung klarer Rollen, Bereitstellung von Budgets und Implementierung der DOR-Strategie. Die Richtlinien müssen regelmäßig überprüft werden. Zudem sind Berichterstattungskanäle einzurichten, und die Geschäftsleitung muss ihre IKT-Kenntnisse regelmäßig aktualisieren.	Gewährleistet das Governance-Rahmenwerk ein effektives IKT-Risikomanagement mit klaren Rollen, Budgetzuteilungen, regelmäßigen Überprüfungen, Berichterstattungskanälen und regelmäßigen Schulungen der Geschäftsleitung?	Art. 5 (1, 2, 4) DORA Art. 13 (5) DORA
sGov_05: Information sharing	Finanzinstitute können Informationen zu Cyberbedrohungen in vertrauenswürdigen Gemeinschaften austauschen, um ihre digitale Resilienz zu stärken. Dieser Austausch muss durch Regelungen geschützt sein, die Vertraulichkeit, Datenschutz und die Einhaltung von Wettbewerbsrichtlinien sicherstellen. Die Teilnahmebedingungen sowie die Einbindung von Behörden und IKT-Drittanbietern müssen klar definiert werden. Finanzunternehmen müssen die zuständigen Behörden über ihre Teilnahme informieren.	Erfolgt der Informationsaustausch zu Cyberbedrohungen unter Einhaltung von Vertraulichkeit, Datenschutz und Wettbewerbsrichtlinien, und sind Teilnahmebedingungen sowie die Einbindung von Behörden und Drittanbietern klar geregelt?	Art. 45 (1 - 3) DORA
	Domain 03 Internal audit and compliance management		
sIA_01: Proportionality principle	Die DORA-Anforderungen sollten entsprechend der Größe, dem Risikoprofil sowie der Art, dem Umfang und der Komplexität der Dienstleistungen, Aktivitäten und Geschäftstätigkeiten des Finanzunternehmens umgesetzt werden. Dabei müssen die relevanten Bestimmungen der DORA-Verordnung beachtet werden.	Werden die DORA-Anforderungen unter Berücksichtigung der Größe, des Risikoprofils sowie der Art, des Umfangs und der Komplexität der Dienstleistungen und Aktivitäten des Unternehmens verhältnismäßig umgesetzt und entsprechen sie den relevanten DORA-Bestimmungen?	Art. 4 (1, 2) DORA
sIA_02: Roles & Responsibilities of the Management Body	Die Geschäftsleitung muss interne IKT-Auditpläne, durchgeführte Audits und wesentliche Änderungen daran genehmigen und regelmäßig überprüfen.	Genehmigt und überprüft die Geschäftsleitung regelmäßig die internen IKT-Auditpläne, die durchgeführten Audits und alle wesentlichen Änderungen daran?	Art. 5 (2f) DORA
sIA_03: ICT Risk Control Function	Die Verantwortung für das Management und die Überwachung von IKT-Risiken muss einer unabhängigen Kontrollfunktion zugewiesen werden, um Interessenkonflikte zu vermeiden. Dabei ist eine klare Trennung der IKT-Risikomanagementfunktion (1. Verteidigungslinie), der IKT-Risikomanagement-Kontrollfunktion (2. Verteidigungslinie) und der internen Auditfunktion (3. Verteidigungslinie) gemäß dem Modell der drei Verteidigungslinien sicherzustellen.	Ist die Verantwortung für das Management und die Überwachung von IKT-Risiken einer unabhängigen Kontrollfunktion zugewiesen, und wird eine klare Trennung der drei Verteidigungslinien entsprechend dem Modell zur Vermeidung von Interessenkonflikten gewährleistet?	Art. 6 (4) DORA

Leseprobe

ID/ Thema	Anforderung (Kompakt)	Checkfrage	Referenz
sIA_04: ICT contract control function	Eine Rolle oder ein Mitglied der Geschäftsleitung sollte benannt werden, um die Überwachung von IKT-Verträgen und die Kontrolle der IKT-Drittanbieterrisiken sicherzustellen.	Wurde eine Rolle oder ein Mitglied der Geschäftsleitung benannt, um die Überwachung von IKT-Verträgen und die Kontrolle der IKT-Drittanbieterrisiken zu gewährleisten?	Art. 5 (3) DORA
sIA_05: Crisis management function	Eine Krisenmanagementfunktion sollte eingerichtet werden, um klare Verfahren für die interne und externe Kommunikation während der Aktivierung von IKT-Geschäftskontinuitäts- sowie Reaktions- und Wiederherstellungsplänen sicherzustellen.	Wurde eine Krisenmanagementfunktion eingerichtet, um klare Verfahren für die interne und externe Kommunikation während der Aktivierung von IKT-Geschäftskontinuitäts-, Reaktions- und Wiederherstellungsplänen festzulegen?	Art. 11 (7) DORA
sIA_06: Outsourcing of assurance	Die Überprüfung der Einhaltung der IKT-Risikomanagementanforderungen kann an gruppeninterne oder externe Stellen ausgelagert werden, solange das Finanzunternehmen die volle Verantwortung für die Einhaltung trägt.	Wird die Überprüfung der Einhaltung der IKT-Risikomanagementanforderungen optional an gruppeninterne oder externe Stellen ausgelagert, und stellt das Unternehmen sicher, dass es die volle Verantwortung für die Einhaltung trägt?	Art. 6 (10) DORA
sIA_07: Audit Requirements:	Das IKT-Risikomanagement-Rahmenwerk sollte regelmäßig von unabhängigen, qualifizierten Prüfern überprüft werden. Die Häufigkeit und Schwerpunkte der Audits müssen den aktuellen IKT-Risiken entsprechen, und es muss ein Verfahren vorhanden sein, um kritische Feststellungen schnell zu beheben. Für die Überwachung von IKT-Drittanbietern sind Inspektionen, interne oder externe Audits, gemeinsame Prüfungen und Zertifizierungen notwendig. Audits sollten die Geschäftstätigkeit so wenig wie möglich stören. Alle Ergebnisse aus internen Audits, Compliance-Bewertungen und Resilienztests müssen in den IKT-Risikomanagement-Bericht aufgenommen werden.	Werden regelmäßige Audits durch unabhängige, qualifizierte Prüfer durchgeführt, wobei die Häufigkeit und Schwerpunkte auf die IKT-Risiken abgestimmt sind, und sind die Verfahren zur Überprüfung kritischer Feststellungen sowie die Ergebnisse der Audits und Tests vollständig im IKT-Risikomanagement-Bericht dokumentiert?	Art. 6 (6 - 7), 11 (3) DORA Art. 6 (3), 8 (2) RTS "3P-policy" Art. 27 (2k) RTS risk mgt.
	Domain 04 ICT asset & architecture management		
sAsset_01: ICT Asset Management Policy:	Finanzunternehmen müssen eine Richtlinie zum Management von IKT-Assets entwickeln, dokumentieren und implementieren, die den gesamten Lebenszyklus der IKT-Assets überwacht. Diese muss Aufzeichnungen zu eindeutigen Kennungen, Standorten, Klassifikation, Eigentümern, unterstützten Prozessen, Kontinuitätsanforderungen, Netzwerkanbindungen, Verbindungen und Abhängigkeiten sowie Support-Enddaten enthalten. Für größere Unternehmen sind zudem Informationen zur Risikobewertung veralteter IKT-Systeme erforderlich. Kritische IKT-Assets und ihre Konfigurationen müssen vollständig identifiziert und abgebildet werden.	Deckt die Richtlinie alle erforderlichen Informationen zu IKT-Assets ab, einschließlich Lebenszyklusüberwachung, kritischer Assets, detaillierter Aufzeichnungen und Risikobewertungen veralteter Systeme?	Art. 4 (1, 2) RTS risk mgt. Art. 8 (4) DORA
…	…	…	…

Lernhilfe