DataNavigator

EUROGROUP CONSULTING

DataNavigator #20

November 2023 ISSN 2702-1904

Digital Operational Resilience Act (DORA): Wie hoch wird die nächste Welle der Regulierung?

Stefan Bauer

Die Regulierung im Finanzsektor nimmt – insbesondere seit der globalen Finanzkrise im Jahr 2008 – kontinuierlich zu. Ein wesentlicher Grund sind die weiterhin immensen Schäden durch Cyberkriminalität (148 Mrd. Euro jährlich allein in Deutschland)[1].

Mit der EU-Verordnung „DORA" (Digital Operational Resilience Act), die am 16.01.2023 in Kraft gesetzt wurde, rollt die nächste Regulierungswelle auf Finanzunternehmen zu. DORA soll bestehende nationale Regelungen zum Risikomanagement für IKT (Informations- und Kommunikationstechnologien) im Finanzsektor innerhalb der EU vereinheitlichen, um den Finanzmarkt gegen Cyberrisiken und IKT-Störungen widerstandsfähiger zu machen. Die Regelung soll ab 17.01.2025 angewendet werden.

Für Finanzunternehmen bedeutet das: DORA wird die Anforderungen aus MaRisk/BAIT bzw. VAIT noch einmal deutlich verschärfen. Hinzu kommt eine Detaillierung der Anforderungen in Form von verpflichtenden technischen Regulierungsstandards (RTS) und technischen Durchführungsstandards (ITS) durch die European Supervisory Authorities (EBA, EIOPA, ESMA) bis Mitte 2024.

Im Folgenden geben wir einen Überblick über wesentliche Aufwandstreiber für die Umsetzung der regulatorischen Anforderungen aus DORA.

Wesentliche Aufwandstreiber in der Umsetzung von DORA

Wir haben im Rahmen eines detaillierten Abgleichs von DORA gegenüber MaRisk/BAIT bzw. VAIT insbesondere die in Abbildung 1 genannten Anforderungen als Aufwandstreiber für die Umsetzung identifiziert.

[1] Vgl. Bitkom Presseinformation vom 01.09.2023

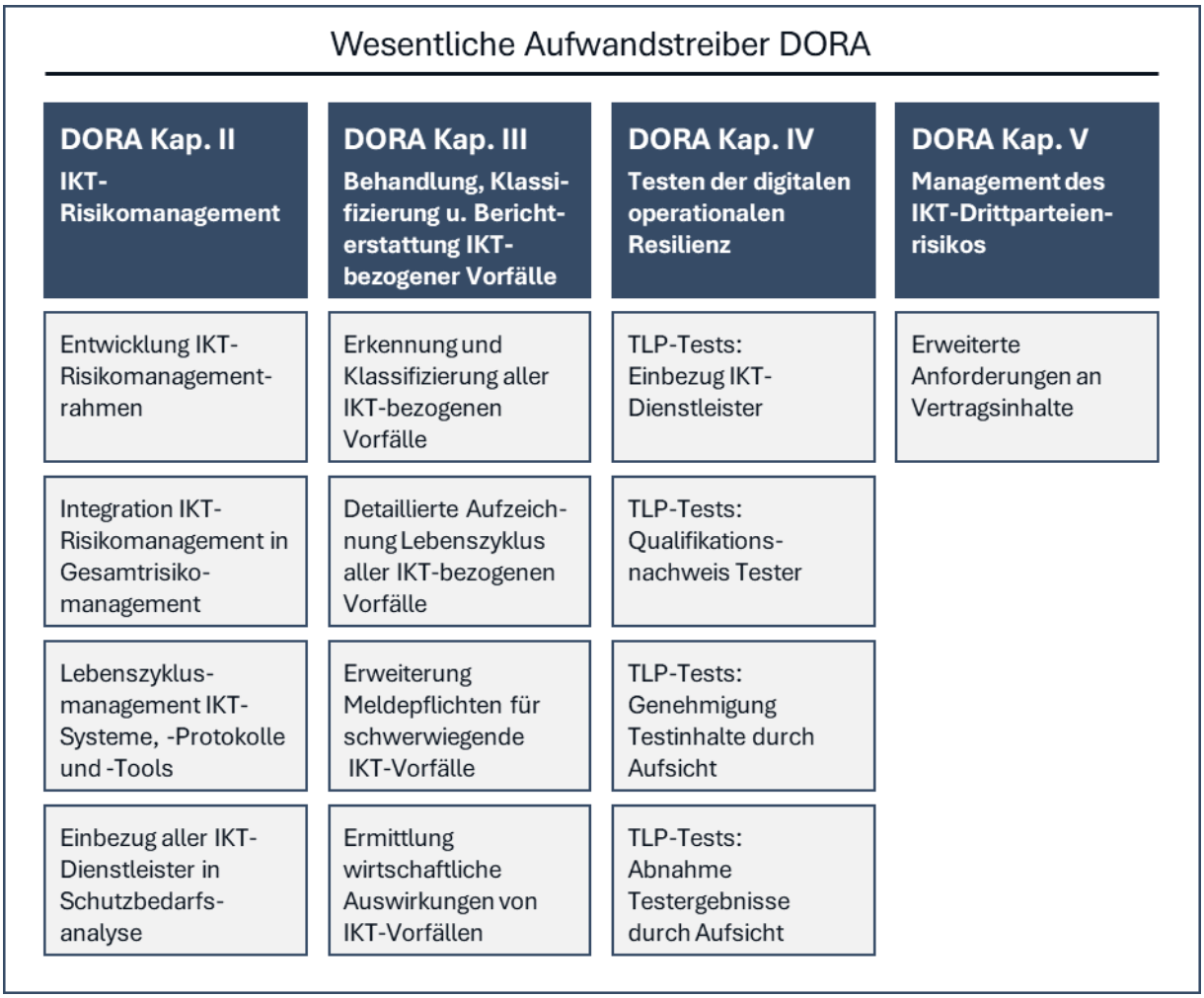

Abbildung 1 - Wesentliche Aufwandstreiber von DORA

Betrachten wir nun diese Aufwandstreiber in den folgenden Abschnitten etwas näher.

IKT-Risikomanagement (DORA Kap. II)

Neben der Erstellung eines umfassenden IKT-Risikomanagementrahmens (u.a. Strategie zur digitalen operationalen Resilienz, Leit- und Richtlinien, Verfahren sowie IKT-Protokollen und -Tools) wird insbesondere die geforderte Integration des IKT-Risikomanagements in das Gesamtrisikomanagement hohe Aufwände bei den Beteiligten in Risikomanagement, Compliance und Revision (für die geforderte Prüfung durch unabhängige Dritte) erzeugen.

Die Anforderung, stets auf dem neuesten Stand zu haltende IKT-Systeme, -Protokolle und -Tools einzusetzen, wird nur mit einem entsprechenden Lebenszyklusmanagement umzusetzen sein. Gut aufgestellte Finanzdienstleister setzen dies bereits seit Jahren als Erweiterung ihres IT-Assetmanagements ein. Wer jetzt erst damit startet, sollte daran denken, dass der Hauptaufwand nicht in der Einführung eines Tools, sondern in der initialen Datenerhebung und nachfolgend in der Fortschreibung nach einem zu definierenden Aktualisierungsprozess liegt.

Die Konkretisierung der Schutzbedarfsanalyse für IKT-Risiken verlangt, dass Prozesse über die Grenze zu IKT-Dienstleistern hinweg betrachtet werden. DORA unterscheidet dabei nicht zwischen "IT-Auslagerung" und "sonstigem Fremdbezug von IT-Dienstleistungen“, wodurch die Anzahl einzubeziehender IKT-Dienstleister und damit der Aufwand nicht unbeträchtlich steigen dürfte.

Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (DORA Kap. III)

Die geforderte umgehende Erkennung und Klassifizierung aller IKT-bezogenen Vorfälle erfordert das Aufsetzen eines entsprechenden Prozesses mit Einbezug des Security Operations Centers (Erkennung) und IKT-Risikomanagements (Klassifizierung).

Die verlangte detaillierte Aufzeichnung aller Tätigkeiten vor und während eines IKT-bezogenen Vorfalls wird – neben der Definition eines entsprechenden Prozesses – eine toolgestützte und automatisierte Umsetzung erfordern. Der Aufwand für die technische Implementierung hängt u.a. vom Reifegrad des eingesetzten SIEM (Security Information and Event Management) und den vorhandenen Möglichkeiten zur Erfassung und revisionssicheren Protokollierung aller Tätigkeiten ab.

Die Meldepflichten werden erweitert um die Meldung der geschätzten aggregierten jährlichen Kosten und Verluste, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden. Bei schwerwiegenden IKT-Vorfällen ist ein detailliertes Reporting an die Aufsichtsbehörde sowie Information der betroffenen Kunden gefordert. Neben den entsprechenden Prozessen müssen die Rollen und Verantwortlichkeiten definiert werden.

Im Rahmen der Klassifizierung sind auch die wirtschaftlichen Auswirkungen (namentlich direkte und indirekte Kosten und Verluste) des jeweiligen IKT-bezogenen Vorfalls zu ermitteln.

Testen der digitalen operationalen Resilienz (DORA Kap. IV)

DORA unterscheidet zwischen Tests von IKT-Tools und -Systemen und erweiterten Tests auf Basis von Threat Led Penetration Testing (TLPT).

Bei Ersteren ist erwähnenswert, dass diese u.a. auch Schwachstellenscans, Open-Source-Analysen und Quellcodeprüfungen sowie Penetrationstests enthalten sollen. Das sollte bereits heute gängige Praxis sein, bspw. Schwachstellenanalysen durch Level-3-Analysten des Security Operations Centers und Pentests durch unabhängige Dritte.

Bei den neu hinzukommenden erweiterten Tests (TLPT) aller kritischen oder wichtigen Funktionen sind die jeweiligen IKT-Dienstleister einzubeziehen, was ein übergreifendes Testmanagement erfordert. Es versteht sich von selbst, dass bedrohungsorientierte Penetrationstests gegen das Produktivsystem auszuführen sind. Die Testinhalte sind von der Aufsichtsbehörde zu genehmigen und die Testergebnisse zum Erhalt einer Bescheinigung vorzulegen. Entsprechend aufwändig sind die Planung, Durchführung und revisionssichere Dokumentation dieser alle drei Jahre geforderten Tests.

Threat Led Penetration Tests können auch durch interne Tester durchgeführt werden, jeder dritte TLP-Test muss jedoch durch externe Tester erfolgen. Tester müssen dafür spezifisches

Fachwissen nachweisen (bspw. Bedrohungsanalyse, Penetrationstests und Red-Team-Tests) und über eine Berufshaftpflichtversicherung verfügen. Der Einsatz interner Tester muss zudem durch die Aufsichtsbehörde genehmigt werden. Neben den Aufwänden für die (Teil-) Auslagerung der Tests an externe Dienstleister sind dabei auch Qualifizierungsmaßnahmen für interne Tester einzuplanen.

Management des IKT-Drittparteienrisikos (DORA Kap. V)

DORA stellt im Vergleich zu BAIT bzw. VAIT weitergehende Anforderungen an die Inhalte von IKT-Dienstleisterverträgen. So ist beim Bezug von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen neben einer Exit-Klausel bspw. auch eine Klausel darüber zu vereinbaren, dass Verträge nicht aufgrund einer Umstrukturierung gekündigt, ausgesetzt oder geändert werden können. Diese und weitere Detaillierungen erfordern eine Überprüfung und ggf. Anpassung aller betroffenen Verträge, was mit deutlichem Aufwand für die Rechtsabteilung einhergehen dürfte.

Detailregelungen RTS und ITS lassen weitere Aufwände erwarten

Die regulatorischen Anforderungen aus DORA werden derzeit noch in verpflichtenden technischen Regulierungsstandards (RTS) und technischen Durchführungsstandards (ITS) konkretisiert und bis 17.01.2024 bzw. 17.07.2024 finalisiert. Die Übersicht in Abbildung 2 zeigt die Themenfelder und deren Fertigstellungstermine.

	RTS (Regulatory Technical Standards)	ITS (Implementing Technical Standards)
Finalisierung bis 17.01.2024	RTS (Art. 15+16) IKT-Risikomanagementrahmen und vereinfachter Risikomanagementrahmen	
	RTS (Art. 18.3) Klassifizierung IKT-bezogener schwerwiegender Vorfälle	
	RTS (Art. 28.10) Leitlinie bzgl. IKT-Dienstleistungen zur Unterstützung kritischer und wichtiger Funktionen	ITS (Art. 28.9) Informationsregister bzgl. IKT-Dienstleistungen von IKT-Drittparteien
Finalisierung bis 17.07.2024	RTS (Art. 20a) Meldung IKT-bezogener schwerwiegender Vorfälle	ITS (Art. 20b) Details zur Meldung IKT-bezogener schwerwiegender Vorfälle
	RTS (Art. 26.11) Tests von IKT-Tools, Systemen und Prozessen	
	RTS (Art. 30.5) Unterverlagerung / Weiterverlagerung kritischer Funktionen	
	RTS (Art. 41) Details der Information über die Überwachungstätigkeiten	

Abbildung 2 - Technische Regulierungsstandards (RTS) und technische Durchführungsstandards (ITS)

Die RTS und ITS enthalten u.a. Detaillierungen

- zu erweiterten Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT (Threat Led Penetration Testing),
- zum Management des IKT-Drittparteienrisikos, wie Vorgaben für ein Register inkl. dessen Befüllung, zu internen Richtlinien sowie zur Unterauslagerung von kritischen oder wichtigen Funktionen,
- zur Klassifizierung von IKT-bezogenen Vorfällen (bspw. Schwellenwerte zur Bestimmung schwerwiegender IKT-Vorfälle und Cyberbedrohungen) und

– zur Berichtspflicht, Meldeterminen, einheitlichen Meldeformaten für schwerwiegende IKT-Vorfälle sowie Mitteilung wesentlicher Cyberbedrohungen,

die von Finanzunternehmen in der Umsetzung zu berücksichtigen sind.

Vor der Veröffentlichung der RTS und ITS kann noch nicht abgeschätzt werden, welche Aufwände für die Umsetzung aus diesen Detaillierungen resultieren werden, insbesondere für TLPT dürften diese jedoch aufgrund der Komplexität und des Umfangs mit vielen einzubeziehenden Beteiligten (inkl. IKT-Dienstleister) nicht gering ausfallen.

Fazit

Die aufgezeigten Aufwandstreiber und die schiere Anzahl an Verschärfungen und Detaillierungen der aufsichtsrechtlichen Anforderungen aus DORA sind es, die Finanzunternehmen vor allem vor kapazitative Herausforderungen in der Umsetzung stellen werden. Davon sind neben der IT vor allem Risikomanagement, Compliance, Revision sowie die Rechtsabteilung betroffen.

Wie hoch die Welle der neuen Anforderungen aus DORA für das jeweilige Institut wird, hängt insbesondere auch vom bisher erreichten Reifegrad der Umsetzung MaRisk/BAIT bzw. VAIT und der Ausstattung mit den erforderlichen Ressourcen für die Umsetzung ab.

Daher ist ein vorbereitender Schritt, der sofort angegangen werden sollte, eine Standortbestimmung (Gap-Analyse) der Umsetzung BAIT bzw. VAIT, um die „Absprungbasis“ für die Umsetzung von DORA zu kennen. Parallel dazu sollten in Arbeit befindliche Umsetzungen regulatorischer Vorgaben hinsichtlich der Überschneidung mit DORA geprüft werden, um Doppelarbeiten zu vermeiden.

Auf Basis dieser Vorarbeiten kann unmittelbar mit der Umsetzungsplanung für DORA begonnen und eine Ressourcenplanung für die IT und die genannten Fachabteilungen durchgeführt werden, um sicherzustellen, dass die Umsetzung von DORA nicht zu einem Anforderungsstau bei der Umsetzung wichtiger Vorhaben führt.

Stefan Bauer ist Manager bei Eurogroup Consulting und Experte für IT-Architektur und IT-Management. Seine Projektexpertise umfasst u.a. die Durchführung von IT-Assessments, IT-Architekturanalysen und Neuaufstellung von Anwendungslandschaften, IT-Strategie, IT-Security, IT-Prozessmanagement sowie die Neuausrichtung von IT-Organisationen. Seit 26 Jahren unterstützt er Kunden aus dem Banken- und Versicherungsumfeld bei der Konzeption und Umsetzung ihrer Vorhaben. Zuvor war er 6 Jahre als Diplom-Informatiker in der Softwareentwicklung tätig.

Über den DataNavigator

Unterschiedliche Autoren beleuchten in der Reihe DataNavigator die vielfältigen Facetten des Datenmanagements und zeigen Ihnen interessante Aspekte auf. Der DataNavigator wird von Eurogroup Consulting regelmäßig zweimonatlich herausgegeben und möchte Ihnen interessante Denkanstöße liefern. Wir freuen uns, Ihnen mit dem DataNavigator unsere Erfahrungen weiterzugeben und stehen Ihnen für die Diskussion gerne zur Verfügung! Sie erreichen Autoren und Herausgeber bei Anregungen und Feedback unter der E-Mail-Adresse datanavigator@eurogroupconsulting.de.

Bisher erschienen:

#1 Dr. Marco Weiß – *Welt und Wesen des Datenmanagements*; September 2020

#2 Mario Kubik – *„DLT" – Potenzial zur Zukunftstechnologie?*; November 2020

#3 Jonathan Misler – *Verwendung von Daten und Modellen in datengetriebenen Geschäftsmodellen*; Januar 2021

#4 Johannes Bänsch – *Data Analytics und die Cloud*; März 2021

#5 Kurt Tanneberger – *Ja, wo sind sie denn? – Daten im IT-Betrieb*; Mai 2021

#6 Thomas Tiebor – *Data Governance als Fundament guten Datenmanagements;* Juli 2021

#7 Dr. Marco Weiß – *Artificial Intelligence – Nature or Nurture?*; September 2021

#8 Binjamin Sancar, Hermann Sgardelli – *Vertriebschancen in einer Bank durch Nutzung ihrer Daten und ihres Ökosystems;* November 2021

#9 Abdalla El Kadi – *Datenvisualisierung – eine Geschichte in Bildern;* Januar 2022

#10 Carsten Kuhlmann – *Kundenfokussierung: Daten und Technik*; März 2022

#11 Luca Winters – *CIEM – Cloud Infrastructure Entitlements Management*; Mai 2022

#12 Kristian Buric – *Der Informationsverbund - Daten (nur) für die Aufsicht?*; Juli 2022

#13 Stefan Bauer – *Aufbau eines SOC (Security Operations Center) als Kommandozentrale zur Cyberabwehr*; September 2022

#14 Thomas Tiebor – *Der Charme von IT-Datenarchitekturmustern;* November 2022

#15 Dr. Marco Weiß – *Citius, Altius, Fortius – Daten im Sport*; Januar 2023

#16 Simon Wilmerding – *Daten statt (nur) Bauchgefühl – Mit Datenanalysen den War for Talent gewinnen*; März 2023

#17 Kay Helbig – *ESG-Berichterstattung bei Versicherungen*; Mai 2023

#18 Dr. Marco Weiß – *Daten und Modelle in der 7. MaRisk-Novelle*; Juli 2023

#19 Fabio Giacomo Müller – *Softwareeinführungsprojekte im internationalen Kontext*; September 2023

#20 Stefan Bauer – *Digital Operational Resilience Act (DORA): Wie hoch wird die nächste Welle der Regulierung?*; November 2023