Holger Reibold

DORA

für Nicht-Finanzunternehmen

Resilienz-Anforderungen verstehen und umsetzen

BRAIN-MEDIA.DE

Holger Reibold

DORA

für Nicht-Finanzexperten

Resilienz-Anforderungen verstehen und umsetzen

BRAIN-MEDIA.DE

ISBN: 978-3-95444-324-6

Cover: Freepik

Brain-Media.de
Dr. Holger Reibold – St. Johanner Str. 41-43 – 66111 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Vorwort: Warum dieses Buch wichtig ist

Die Verordnung über digitale operationale Resilienz im Finanzsektor (DORA) markiert einen tiefgreifenden Wendepunkt im europäischen Regulierungsumfeld. Was lange primär als internes Thema für Banken, Versicherungen und Wertpapierfirmen galt, wirkt heute weit über die Grenzen der Finanzbranche hinaus. Insbesondere Anbieter von SaaS-Lösungen, Managed Services, Cloud-Infrastrukturen und anderen IKT-Dienstleistungen geraten zunehmend in den Fokus regulatorischer Anforderungen — oft früher und intensiver, als sie selbst erwarten.

In der Praxis zeigt sich ein wiederkehrendes Muster: Viele Nicht-Finanzunternehmen gehen zunächst davon aus, dass DORA sie nicht betrifft. Die erste konkrete Berührung erfolgt dann nicht über die Aufsicht, sondern über den Kunden. Plötzlich trifft ein umfangreicher Fragebogen ein, Vertragsklauseln werden verschärft oder Audit-Rechte werden eingefordert. Spätestens an diesem Punkt wird klar, dass DORA faktisch entlang der digitalen Lieferkette wirkt.

Genau hier setzt dieses Buch an. Es richtet sich bewusst an Nicht-Finanzexperten — an Geschäftsführer, CTOs, CISOs, Compliance-Verantwortliche sowie an technische und organisatorische Entscheider in SaaS-, MSP-, Cloud- und IKT-Unternehmen. Das Ziel ist es nicht, die Verordnung juristisch zu kommentieren oder akademisch

zu interpretieren. Das Ziel ist es, die Logik hinter DORA verständlich zu machen und vor allem: umsetzbar.

Dabei verfolgt dieses Buch einen strikt pragmatischen Ansatz. Sie finden hier keine theoretischen Idealbilder, sondern erprobte Minimalansätze, typische Stolpersteine aus der Praxis und konkrete Hilfestellungen für die Umsetzung mit vertretbarem Aufwand. Besonders für kleine und mittlere Anbieter ist entscheidend, die Balance zu finden zwischen regulatorischer Erwartung, technischer Realität und wirtschaftlicher Vernunft.

Ein zentrales Missverständnis besteht darin, DORA ausschließlich als Compliance-Last zu betrachten. Richtig eingeordnet, bietet die Verordnung jedoch auch eine Chance: Unternehmen, die ihre operationale Resilienz strukturiert nachweisen können, gewinnen messbar an Vertrauen bei regulierten Kunden. In vielen Ausschreibungen entwickelt sich DORA-Readiness bereits heute zu einem Differenzierungsmerkmal.

Gleichzeitig ist wichtig zu verstehen: Dieses Buch ist eine Momentaufnahme in einem dynamischen regulatorischen Umfeld. Die technischen Regulierungsstandards (RTS/ITS) werden fortlaufend präzisiert, und auch die Aufsichtspraxis entwickelt sich weiter. Deshalb finden Sie an mehreren Stellen Hinweise, wie Sie regulatorische Updates systematisch beobachten und Ihre Umsetzung belastbar weiterentwickeln können.

Wenn Sie dieses Buch durcharbeiten, werden Sie drei Dinge gewinnen: ein klares Verständnis der tatsächlichen DORA-Erwartungen, eine realistische Einschätzung Ihrer eigenen Betroffenheit und einen pragmatischen Fahrplan für die nächsten Schritte.

Die digitale Resilienz wird in den kommenden Jahren zu einem zentralen Vertrauensfaktor in der Finanz-IT-Lieferkette. Je früher Sie strukturiert handeln, desto größer ist Ihr Handlungsspielraum.

Dieses Buch soll Ihnen dabei helfen.

Herzlichst

Holger Reibold

Für wen dieses Buch nicht ist

Dieses Buch richtet sich an Praktiker, die DORA verstehen und mit vertretbarem Aufwand umsetzen wollen. Es ist ausdrücklich nicht als juristischer Kommentar zur Verordnung konzipiert. Wenn Sie eine tiefgehende rechtliche Auslegung einzelner Artikel, eine wissenschaftliche Analyse oder eine vollständige regulatorische Kommentierung erwarten, wird dieses Buch Ihre Erwartungen nicht erfüllen.

Ebenso ist dieses Buch nicht für große Finanzinstitute gedacht, die bereits über ausgereifte Compliance-, Risk- und Legal-Abteilungen verfügen. Organisationen mit umfangreichen Second- und Third-Line-Strukturen benötigen in der Regel detailliertere, institutsindividuelle Umsetzungsprogramme.

Auch Unternehmen, die eine Checkbox-Compliance ohne tatsächliche organisatorische und technische Substanz anstreben, werden mit diesem Ansatz wenig anfangen können. DORA ist ausdrücklich auf nachweisbare operationale Resilienz ausgerichtet. Reine Dokumentationsfassaden halten einer Prüfung erfahrungsgemäß nicht stand.

Wie Sie dieses Buch effizient nutzen

Dieses Buch ist modular aufgebaut. Sie müssen es nicht zwingend von vorne bis hinten lesen. Wenn Sie zunächst klären wollen, ob und wie stark Ihr Unternehmen betroffen ist, beginnen Sie mit Kapitel 1 und dem 5-Minuten-Selbsttest. Für eine schnelle Standortbestimmung empfiehlt sich anschließend die Gap-Analyse in Kapitel 7.

Wenn Sie bereits konkrete Kundenanforderungen oder Fragebögen vorliegen haben, werden insbesondere Kapitel 2, 5 und 7 für Sie unmittelbar praxisrelevant sein. Technisch Verantwortliche finden den größten Mehrwert typischerweise in Kapitel 3 und Kapitel 8.

Arbeiten Sie mit Textmarkierungen, und nutzen Sie die bereitgestellten Checklisten und Templates konsequent. Der größte Nutzen entsteht erfahrungsgemäß nicht beim Lesen, sondern beim strukturierten Anwenden der Artefakte auf Ihre eigene Organisation.

Das Ziel dieses Buches ist nicht Vollständigkeit im theoretischen Sinn, sondern schnelle Handlungsfähigkeit in der Praxis. Nutzen Sie es entsprechend pragmatisch.

1 DORA in 30 Minuten

DORA wirkt auf den ersten Blick komplex und schwer zugänglich. Viele Verantwortliche sehen sich mit einer Vielzahl neuer Begriffe, Anforderungen und Querverweise konfrontiert — und verlieren dabei schnell den Blick für das Wesentliche. Genau hier setzt dieses Kapitel an.

Bevor Sie beginnen, einzelne Maßnahmen umzusetzen oder Dokumente zu erstellen, ist es entscheidend, die Grundlogik der Verordnung zu verstehen. DORA ist kein weiteres isoliertes Compliance-Regelwerk, sondern ein systematisch aufgebauter Rahmen zur Stärkung der digitalen operationalen Resilienz im Finanzökosystem. Wer diese Systematik einmal durchdrungen hat, erkennt schnell, dass viele Anforderungen weniger neu sind, als sie zunächst erscheinen.

Das Ziel dieses Kapitels ist daher bewusst ambitioniert: Sie sollen DORA in etwa 30 Minuten strukturell verstehen können. Nicht in allen juristischen Details, sondern in der Tiefe, die für fundierte Management- und Umsetzungsentscheidungen erforderlich ist. Dazu betrachten wir zunächst die Intention des Gesetzgebers, den tatsächlichen Anwendungsbereich und die Abgrenzung zu angrenzenden Regelwerken wie NIS-2 und ISO 27001.

Besonderes Augenmerk liegt auf typischen Fehlinterpretationen, die in der Praxis immer wieder auftreten — sowohl auf Seiten regulierter

Finanzunternehmen als auch bei deren IKT-Dienstleistern. Wer diese Denkfehler früh erkennt, spart später erheblichen Aufwand.

Am Ende dieses Kapitels sollten Sie drei Dinge klar beantworten können: ob Ihr Unternehmen direkt oder indirekt betroffen ist, welche Erwartungshaltung die Finanzaufsicht tatsächlich hat und wo die häufigsten Missverständnisse liegen. Mit diesem Fundament wird die weitere Umsetzung deutlich zielgerichteter und wirtschaftlicher möglich.

1.1 Ziel und Intention der Verordnung

Mit der Verordnung über digitale operationale Resilienz im Finanzsektor verfolgt der europäische Gesetzgeber ein klares strategisches Ziel: Die Widerstandsfähigkeit des Finanzsystems gegenüber IKT-Störungen und Cyberbedrohungen soll systematisch gestärkt und europaweit harmonisiert werden. Der Ausgangspunkt ist die Erkenntnis, dass digitale Risiken längst zu systemischen Risiken geworden sind.

In den vergangenen Jahren haben sich Finanzunternehmen in hohem Maß von komplexen IT-Landschaften, Cloud-Infrastrukturen und externen Dienstleistern abhängig gemacht. Gleichzeitig sind Cyberangriffe professioneller, Lieferketten verwundbarer und Ausfälle potenziell folgenreicher geworden. Einzelne Sicherheitsmaßnahmen reichen unter diesen Bedingungen nicht mehr aus. Genau hier setzt DORA an.

Die Verordnung verschiebt den Fokus weg von punktueller IT-Sicherheit hin zu nachweisbarer operationaler Resilienz. Entscheidend ist nicht mehr nur, ob Schutzmaßnahmen existieren, sondern ob ein Unternehmen Störungen antizipieren, verkraften, schnell wiederherstellen und daraus lernen kann. Diese End-to-End-Perspektive zieht sich durch alle Kapitel der Verordnung: vom ICT-Risikomanagement über Incident Reporting bis hin zum Third-Party Risk Management und zu Resilienztests.

Ein weiterer zentraler Zweck von DORA ist die Harmonisierung. Vor der Verordnung existierten in Europa zahlreiche nationale Aufsichtsanforderungen mit unterschiedlicher Tiefe und Schwerpunktsetzung. Für grenzüberschreitend tätige Finanzunternehmen und ihre Dienstleister führte dies zu erheblicher Komplexität. DORA schafft hier einen einheitlichen Referenzrahmen, der mittelfristig zu mehr Klarheit — aber auch zu höherer Erwartungstransparenz — führen wird.

Für IKT-Dienstleister ist besonders wichtig: DORA reguliert sie meist nicht direkt, aber faktisch sehr wirksam über die Finanzunternehmen. Die Verordnung zwingt Institute dazu, ihre digitale Lieferkette deutlich strenger zu steuern. Damit entsteht ein indirekter, aber sehr spürbarer regulatorischer Druck entlang der gesamten Wertschöpfungskette.

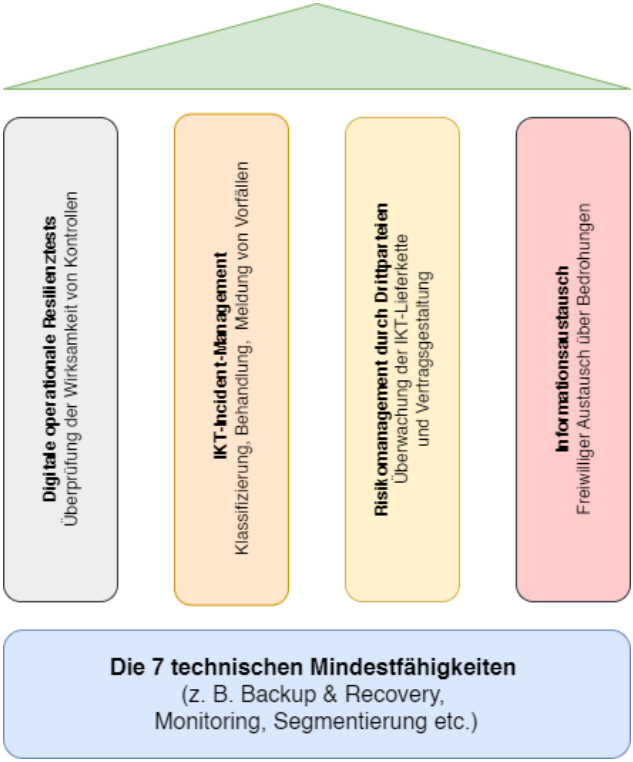
Um die Anforderungen von DORA praktisch greifbar zu machen, folgt dieses Buch einem durchgängigen Strukturmodell: dem DORA-Resilienz-Referenzmodell (DRRM). Es dient als Navigationshilfe, um die

Vielzahl einzelner Anforderungen in eine umsetzbare Gesamtlogik zu überführen.

Das DRRM bündelt die regulatorischen Erwartungen in klar abgegrenzte Fähigkeitsbereiche — von Governance und Risikosteuerung über Incident-Handling bis hin zu technischer Resilienz und Lieferkettenkontrolle. Ziel ist es, die Perspektive der Aufsicht mit der operativen Realität von SaaS-, MSP- und Cloud-Anbietern zu verbinden.

In den folgenden Kapiteln wird das DRRM schrittweise aufgebaut und mit konkreten Minimalanforderungen, Praxisbeispielen und Templates unterlegt. Sie müssen das Modell an dieser Stelle noch nicht im Detail verstehen. Wichtig ist zunächst nur: DORA ist kein Sammelsurium isolierter Pflichten, sondern folgt einer klaren Resilienzlogik — und genau diese Logik machen wir im weiteren Verlauf systematisch nutzbar.

Um DORA nicht als bloße Flut von Einzelvorschriften zu begreifen, nutzen wir in diesem Buch das DORA-Resilienz-Referenzmodell (DRRM). Wie nachstehende Abbildung zeigt, ruhen die regulatorischen Anforderungen auf einem stabilen Fundament technischer Mindeststandards. Die fünf Säulen repräsentieren die operativen Disziplinen, die ein IKT-Dienstleister beherrschen muss, während das Management-Dach sicherstellt, dass Resilienz keine IT-Inselaufgabe bleibt, sondern zur Chefsache wird.



Das DORA-Resilienz-Referenzmodell (DRRM). Die ganzheitliche Verknüpfung von technischer Basis, operativen Prozessen und strategischer Governance als Antwort auf die Anforderungen der EU-Verordnung.

1.2 Wen DORA direkt reguliert

DORA richtet sich in erster Linie an regulierte Finanzunternehmen innerhalb der Europäischen Union. Dazu zählen unter anderem Kreditinstitute, Zahlungsinstitute, E-Geld-Institute, Wertpapierfirmen, Versicherungsunternehmen sowie zentrale Marktinfrastrukturen. Für

Literatur- und Quellenverzeichnis

AMF (2024). The regulation on digital operational resilience in the financial sector (DORA). Autorité des marchés financiers.

BaFin (2024). DORA – Aufsichtliche Einordnung und Umsetzungshinweise. Bundesanstalt für Finanzdienstleistungsaufsicht.

Buttigieg, C. P., & Zimmermann, B. B. (2024). The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision. In ERA Forum (Vol. 25, No. 1, pp. 11-28). Berlin/Heidelberg: Springer Berlin Heidelberg.

Central Bank of Ireland (2024). Digital operational resilience act (DORA) – Supervisory overview.

Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). International Cybersecurity Law Review, 4(1), 79-90.

CSSF (2024). ICT and cyber risk for DORA entities. Commission de Surveillance du Secteur Financier.

European Banking Authority (2024). Digital operational resilience act (DORA) – Overview and supervisory materials.

European Central Bank (2023). TIBER-EU framework (updated version).

European Commission (2022). EU digital finance package – Digital operational resilience act.

European Parliament & Council of the European Union (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.

European Parliament & Council of the European Union (2022). Directive (EU) 2022/2555 (NIS2 Directive). Official Journal of the European Union.

European Parliament & Council of the European Union (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union.

European Supervisory Authorities (2024). First package of final RTS/ITS under DORA.

Kourmpetis, S. (2022). Management of ICT third party risk under the digital operational resilience act. In Digitalisation, Sustainability, and the Banking and Capital Markets Union: Thoughts on Current Issues of EU Financial Regulation (pp. 211-226). Cham: Springer International Publishing.

Kun, E. (2024). Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. Computer Law & Security Review, 52, 105931.

Neumannová, A., Bernroider, E. W., & Elshuber, C. (2022, December). The digital operational resilience act for financial services: A comparative gap analysis and literature review. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 570-585). Cham: Springer Nature Switzerland.

Pattison, A. (2023). A guide to the EU digital operational resilience act. Walter de Gruyter.

Scott, H. S. (2021). The EU's Digital Operational Resilience Act: Cloud Services & Financial Companies. Available at SSRN 3904113.

Tolin, G., Punia, G., & Emmanuel, J. (2025). Report: EU Digital Operational Resilience Regulation (DORA). Global Privacy Law Review, 6(1).

Stichwortverzeichnis

H

I

K

L

M

N

P

R

S

T

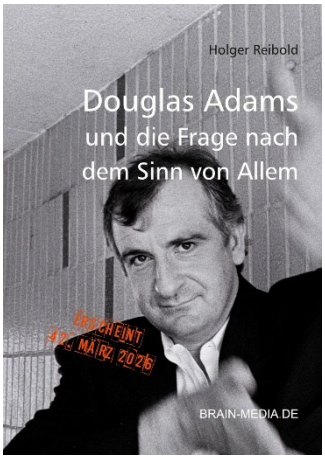
U

V

W

Z

Mehr von Brain-Media.de



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11 Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

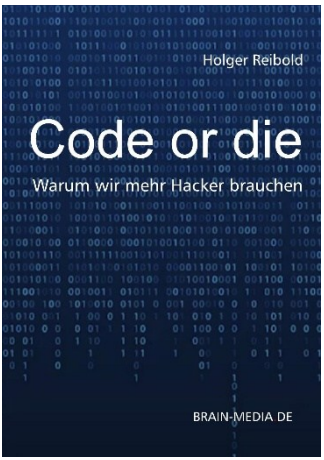
Preis: 14,99 EUR

Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

Preis: 14,99 EUR

Erscheint Frühjahr 2026

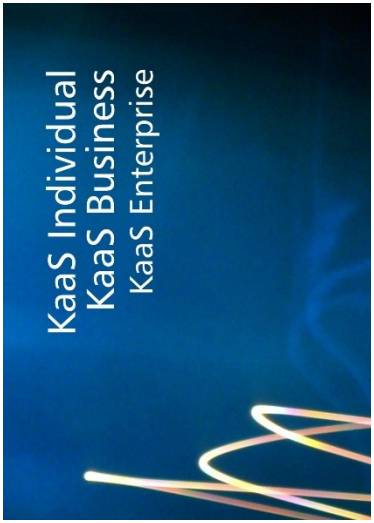
KI Incident Response – Wie man Sicherheitsvorfälle in KI-Systemen erkennt, eindämmt und verantwortet

Ziel- und punktgenaue Reaktionen für kritischen KI-Vorfälle.

Umfang: 140 Seiten

Preis: 16,99 EUR

Erscheint: Frühjahr 2026



Brain-Media KaaS

Individual

Business

Enterprise

– die E-Book-Flatrate –

Brain-Media.de ist ein **Pionier** in Sachen E-Book-Flatrates. Bereits 2014 wurden mit Plus+ E-Books als attraktives und preisgünstiges Abo angeboten. Im April 2026 erlebt Plus+ eine Renaissance.

Abonnementen erhalten **1 Jahr Zugriff auf alle E-Books**, die bereits erschienen sind, und auf alle Neuerscheinungen des Abozeitraums. Sie können über 30 verfügbare E-Books herunterladen – dazu editierbare Checklisten, Vorlagen, Beispiele etc. Sie können die E-Books ausdrucken und auf mehreren Lesegeräten verwenden. Die E-Books verwenden kein DRM!

Und das alles zum **unschlagbaren Sonderpreis**!

IT-Texter.one

100+ IT-Fachbücher

1500+ Fachartikel

30+ Erfahrung

KOMPLEXE INHALTE PUNKTGENAU AUFZUBEREITEN, IST EINE KUNST. ICH BEHERRSCHE SIE. BEI MIR ERHALTEN SIE FACHTEXTE, DIE KOMPLEXES VERSTÄNDLICH MACHEN.

Seit über 30 Jahren unterstütze ich Unternehmen aus der IT-, Software- und Digitalbranche dabei, ihre technischen Inhalte klar, präzise und zielgruppenorientiert zu kommunizieren. Als promovierter Informatiker und erfahrener IT-Journalist verbinde ich fundiertes Fachwissen mit journalistischem Storytelling. Als Key Account Manager eines IT-Dienstleisters verfüge ich obendrein über konkrete Erfahrungen mit allen gängigen Technologien.

WARUM SIE MIT MIR ARBEITEN SOLLTEN

35 Jahre Erfahrung mit Internet-, Netzwerk- und Webtechnologien

Kooperation mit führenden Akteuren der IT- und Medienbranche

Strategisches Denken: Texte, die nicht nur informieren, sondern auch verkaufen

THEMENSCHWERPUNKTE	WIE KANN ICH SIE UNTERSTÜTZEN?
Open-Source	Content Creation
Enterprise IT	Dokumentationen
IT-Consulting	Case Studies
SaaS	Suchmaschinenoptimierung
Künstliche Intelligenz	Tech-Marketing

MEIN VERSPRECHEN

Ich übernehme die inhaltliche und sprachliche Brücke zwischen Technologie und Anwendung. Selbst komplexe Sachverhalte kommen beim Publikum an – fachlich korrekt, prägnant und SEO-wirksam.

PREISMODELLE

Professionelle Leistungen, die ihresgleichen suchen, gibt es nicht umsonst. Sprechen Sie mit an. Gerne vereinbaren wir einen Fixpreis; das vereinfacht Ihre Kalkulation.

KONTAKT AUFNEHMEN

Sprechen wir über Ihr Projekt. Schreiben Sie mir eine Mail (info@it-texter.one). Oder besser noch: Rufen Sie mich an (+49 681 91005698).