

A close-up photograph of a single yellow dandelion flower with a green stem and leaves, growing out of a deep crack in a grey asphalt surface. The flower is in full bloom, and the background is a blurred view of the surrounding pavement.

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

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Verlags ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopien oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt auch für das Recht der öffentlichen Wiedergabe. Der Verlag macht darauf aufmerksam, dass die genannten Firmen- und Markennamen sowie Produktbezeichnungen in der Regel marken-, patent- oder warenrechtlichem Schutz unterliegen.

Verlag und Autor übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren und Standards.

© 2026 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	1
Für wen dieses Buch nicht ist.....	4
Wie Sie dieses Buch effizient nutzen	5
1 DORA in 30 Minuten	7
1.1 Ziel und Intention der Verordnung.....	8
1.2 Wen DORA direkt reguliert.....	11
1.3 Abgrenzung zu NIS-2 und ISO 27001	13
1.4 DORA vs. ISO 27001 vs. NIS-2	16
1.5 DORA-Zeitlinie und Übergangsfristen	18
1.6 Die Logik der Finanzaufsicht.....	20
1.7 Typische Fehlannahmen in der Praxis.....	21
1.8 Was DORA ausdrücklich nicht verlangt	22
1.9 Das Prinzip der Verhältnismäßigkeit.....	24
1.10 Dynamik der Regulierung: RTS/ITS im Blick.....	26
1.11 5-Minuten-Selbsttest: Bin ich betroffen?	28
1.12 Management Summary	30
2 Betroffenheit	33
2.1 IKT-Drittdienstleister im Fokus	34

2.2	Regulatorische Infektion.....	36
2.3	Wer jetzt konkret handeln muss	38
2.4	DORA-Compliance als Wettbewerbsvorteil.....	41
2.5	Management Summary	44
3	ICT Risk Management umsetzen	45
3.1	Was DORA tatsächlich fordert	46
3.2	Was Prüfer wirklich sehen wollen	48
3.3	Minimalansatz für KMU.....	49
3.4	Typische Umsetzungslücken	51
3.5	Dokumentation mit vertretbarem Aufwand	53
3.6	Governance und Verantwortlichkeiten	55
3.7	Rolle des (Top-)Managements	57
3.8	Security Awareness als Resilienzfaktor	59
3.9	Management Summary	61
4	Incident Management.....	63
4.1	Was als DORA-relevanter Vorfall gilt	64
4.2	Klassifizierung von Incidents	66
4.3	Meldefähigkeit organisatorisch herstellen	69
4.4	Eskalations- und Kommunikationsplan	71
4.5	Was nach einer Meldung passiert.....	74
4.6	Information Sharing Arrangements nutzen	76

4.7	Typische Fehler in Incident-Prozessen.....	78
4.8	Management Summary	80
5	Third-Party Risk Management	81
5.1	Warum Lieferanten zum Risiko werden.....	82
5.2	Mindestanforderungen an Dienstleister	83
5.3	Vertragsanforderungen unter DORA	85
5.4	Musterklauseln für ICT-Verträge	88
5.5	Realitätscheck.....	90
5.6	Sub-Sub-Dienstleister wirksam steuern	91
5.7	Exit-Strategien realistisch planen.....	94
5.8	Typische Prüfungsfeststellungen	96
5.9	Das Informationsregister: Wer liefert.....	97
5.10	Management Summary	99
6	Resilienztests sinnvoll planen	101
6.1	Ziel und Logik der DORA-Tests.....	101
6.2	Testarten im Überblick	103
6.3	Für wen TLPT wirklich relevant ist	106
6.4	Pragmatische Teststrategie für KMU	107
6.5	Management Summary	109
7	DORA-Gap-Analyse.....	111
7.1	Reifegrad bestimmen	112

7.2	Prioritäten richtig setzen	114
7.3	Quick Wins identifizieren.....	115
7.4	Typische rote Flaggen in Audits	117
7.5	Kundenfragebögen effizient beantworten	119
7.6	Mini-Fallbeispiel: SaaS-Provider	121
7.7	Management Summary	122
8	Zielbild für technische Resilienz	123
8.1	DORA-Resilienz-Referenzmodell	124
8.2	Die 7 technischen Mindestfähigkeiten	126
8.3	Mindestarchitektur für resiliente Systeme	128
8.4	Backup- und Recovery	130
8.5	Monitoring und Telemetrie	131
8.6	Segmentierung und Schadensbegrenzung	133
8.7	Management Summary	135
9	Der 12-Monats-Umsetzungsplan	137
9.1	Phase 1: Stabilisieren	138
9.2	Phase 2: Strukturieren	140
9.3	Phase 3: Nachweisfähig werden	142
9.4	Aufwand und Ressourcen realistisch planen	144
9.5	Typische Stolpersteine	145
9.6	Prüfungssichere Dokumentation	147

9.7	Die ersten 10 Schritte	149
9.8	Management Summary	151
10	Der DORA-Werkzeugkasten.....	153
10.1	Übersicht aller Checklisten	154
10.2	Übersicht aller Templates.....	156
10.3	Empfohlene Mindestartefakte	157
10.4	Reifegrad-Selbstbewertung	159
10.5	Management Summary	162
	Zum Schluss – Einladung zur Umsetzung	163
	Anhang.....	167
	DORA-Schnellreferenz für IKT-Dienstleister	167
	Artefakt-Landkarte	169
	Typische DORA-Kundenfragen	171
	Glossar	173
	Literatur- und Quellenverzeichnis	179
	Stichwortverzeichnis	181
	Mehr von Brain-Media.de	185
	IT-Texter.one	188

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 strukturieren 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 Aufsichts-anforderungen 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.

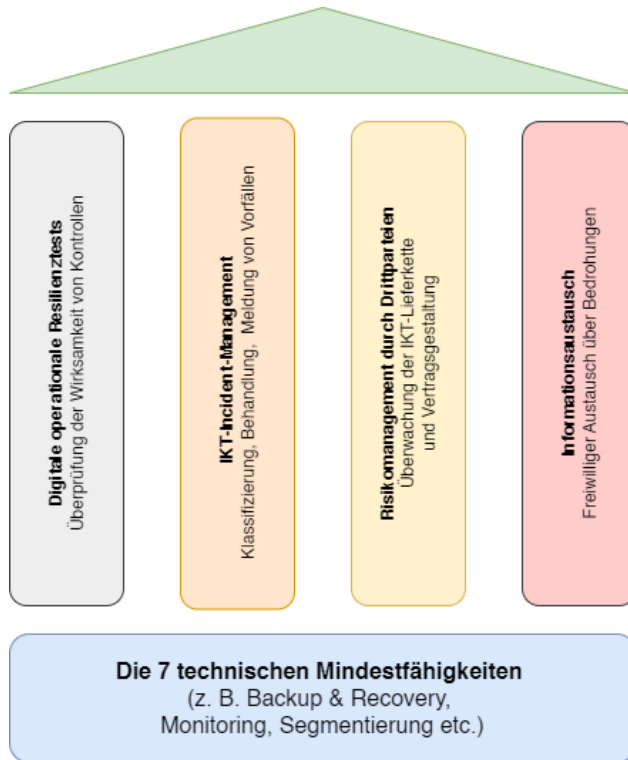
Um die Anforderungen von DORA praktisch greifbar zu machen, folgt dieses Buch einem durchgängigen Strukturmodell: dem DORA-Resilienz-Referenzmodell (DRRM). Es dient als Navigationshilfe, um die

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

B

Backup	50, 126
Betroffenheit	33
Bewertungsmodell	160
Big-Bang-Ansatz	137

C

Change-Management	50
Checkliste	154
Cloud	1
Compliance	41
Cyberangriff	8

D

Deployment	128
Dokumentation	47, 53
DORA	1
DORA-Gap-Analyse	111
DORA-Questionnaire	119
DORA-Readiness	2
DORA-Resilienz-Referenzmodell ...9, 124	
DORA-Roadmap	113

DORA-Test	101
Drei-Säulen-Modell	108
DRRM	9, 125
Due-Diligence	77

E

EBA	27
EIOPA	27
Eskalationsplan	72
ESMA	27
Evidence-Kette	142
Exit-Strategie	94

F

Fehlannahme	21
Finanzaufsicht	20
Finanzkunde	35
Finanzsystem	8
Finanzunternehmen	8, 11
Fragebogen	121
Frühindikator	40

G

Gesetzgeber	7
-------------------	---

Governance.....	46
-----------------	----

H

Handlungsbedarf.....	39
Handlungsdruck.....	38
Hyperscaler.....	92

I

ICT Risk Management	45
ICT-Risk-Policy	54
IKT.....	1
Implementing Technical Standard	26
Incident Management	63
Incident-Management	50
Informationsregister	97
Informationssicherheits-	
Managementsystem	14
Inkrafttreten	18
ISMS.....	14
ISO 27001.....	7, 13, 125
ITS.....	2, 26
IT-Sicherheit.....	9

K

Klassifizierung.....	66
KMU	85
Kommunikationsplan	71

L

Lieferant	82
Lieferkette.....	8

M

Managed Services	1
Management	57
Meldefähigkeit	69
Meldung.....	74
Migration.....	95
Mindestarchitektur.....	128
Mindestartefakt.....	157
Minimalansatz.....	49
Monitoring.....	27, 131

N

NIS-2.....	7, 13
------------	-------

P

Patch-Management.....	84
Penetrationstest	103
Priorität.....	39

R

Realitätscheck	90
Recovery	50, 126

Red Teaming.....	109
Regulatorik.....	36
Regulatory Technical Standard	26
Regulierungsstandard	2
Reifegrad.....	23, 112
Reifegrad-Selbstbewertung	159
Resilienz.....	47, 123
Resilienzlogik	10
Resilienztest.....	9, 49, 101, 103
Ressource	144
Risikomanagementverfahren	46
Risikomodell	50
Risikoorientierung	114
Risikoverantwortung.....	56
Rollenarchitektur.....	55
RTS	2, 26
Runbook.....	127

S

SaaS.....	1
Schadensbegrenzung	133
Security.....	23
Security Awareness	59
Segmentierung	133
Selbsttest.....	28
Stabilisierung	138, 140
Sub-Dienstleister	84
Sub-Sub-Dienstleister	91

T

Tabletop-Exercise	104
Technologieanbieter.....	12
Telemetrie.....	131
Template.....	156
Testarten.....	103
Teststrategie	107
Third-Party Risk Management	81
Threat-Led Penetration Testing ...	106
Three Lines Model	56
TLPT	106

U

Umsetzung.....	19
Umsetzungslücke	51
Umsetzungsplan	137

V

Verhältnismäßigkeit	24
Vertragsanforderung	85
Vollzertifizierung	23
Vulnerability.....	84
Vulnerability Scan	103

W

Warnsignal.....	117
Werkzeugkasten.....	153

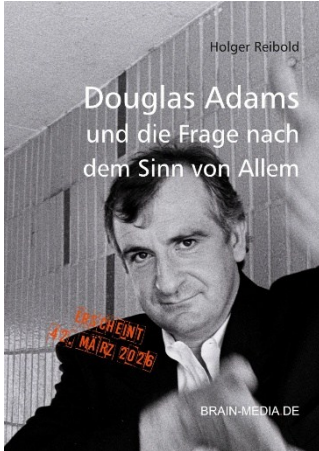
Widerstandsfähigkeit.....8

Wiederverwendbarkeit.....51

Z

Zeitlinie 18

Zugriffskontrolle..... 126



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

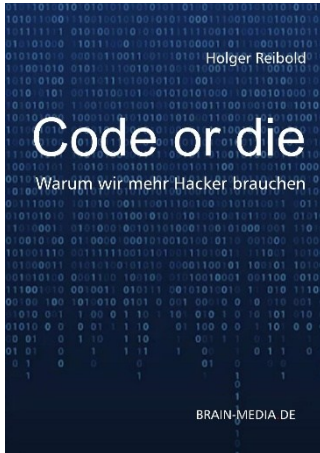
Erscheint: 42. März 2026



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.

Abonnenten 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 FACH-
TEXTE, 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).