

Inhaltsverzeichnis

Vorwort	V
Verzeichnis der Autorinnen und Autoren	VII
Abkürzungsverzeichnis	XXVII
1. Grundlagen & Entwicklung der IKT-Sicherheit	1
1.1. Historischer Abriss der Entwicklung der Finanzindustrie	1
1.2. Die Entwicklung der Digitalisierung	3
1.3. Die IKT-Risikokategorien	5
1.4. Das IKT-Risiko in der Aufsicht	8
1.5. Genese des Digital Operational Resilience Act	19
2. Im Überblick: Regelungsinhalte & Ziele des Digital Operational Resilience Act	22
2.1. Kapitel 1: Allgemeine Bestimmungen (Art 1 bis 4)	22
2.2. Kapitel 2: IKT-Risikomanagement (Art 5 bis 16)	24
2.3. Kapitel 3: Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Art 17 bis 23)	26
2.4. Kapitel 4: Testen der digitalen operationalen Resilienz (Art 24 bis 27)	27
2.5. Kapitel 5: Management des IKT-Drittparteienrisikos (Art 28 bis 44)	28
2.6. Kapitel 6 bis 9: Vereinbarungen über den Austausch von Informationen (Art 45), zuständige Behörden (Art 46 bis 56), delegierte Rechtsakte (Art 57) sowie Übergangs- und Schlussbestimmungen (Art 58 bis 64)	31
2.7. Innerstaatliche Begleitgesetzgebung zum Digital Operational Resilience Act	35
2.7.1. Legistischer Prozess	35
2.7.2. Das DORA-Vollzugsgesetz (DORA-VG)	36
3. IT-Risikomanagement in der Praxis und Auswirkungen von DORA	38
3.1. Einleitung	38
3.2. IT-Risikomanagement in Finanzunternehmen mit besonderem Fokus auf Banken	39
3.2.1. Rahmenbedingungen und Definitionen	40
3.2.1.1. Verfügbarkeit	43
3.2.1.2. Vertraulichkeit	44
3.2.1.3. Integrität und Authentizität	45
3.2.1.4. Kritische Anwendung	45

Inhaltsverzeichnis

3.2.1.5.	Tourliche Überprüfung	45
3.2.2.	Business-Impact-Analyse (BIA)	45
3.2.3.	Risikoanalysen	46
3.2.4.	Risikosteuerung	48
3.2.5.	Auswirkungen des Digital Operational Resilience Act (DORA) auf das Unternehmen	49
3.2.5.1.	IKT-Risikomanagement Framework	49
3.2.5.2.	IT-Risiken als Chancen und Treiber	50
3.2.5.2.1.	Cyberbedrohungen	51
3.2.5.2.2.	IKT-Vorfallmanagement	52
3.2.5.2.3.	BCM	52
3.2.5.2.4.	IKT-Dienstleistersteuerung und IT-Risiko- management	52
3.2.5.2.5.	Überwachung zentraler IKT-Dienstleister	52
3.2.6.	Fazit	53
3.3.	IT-Risikomanagement bei Versicherungsunternehmen	54
3.3.1.	Aktuelle Entwicklungen in der IT und deren mögliche Auswirkungen auf die Zielgröße „Resilienz“ in Bezug auf DORA	54
3.3.1.1.	Ausgliederung der internen IT in eine eigene Gesellschaft	55
3.3.1.2.	Aufbau eines IT-Risk-Managements	56
3.3.1.3.	Wechsel von On-Prem-Lösungen hin zur Cloud	59
3.3.2.	Ausgewählte Werkzeuge zur Mitigation von IT-Risiken	60
3.3.2.1.	Vorschlag zur Erweiterung der Risk-Management- basierten Ansätze um den „Black-Swan/ White-Swan“-Ansatz	60
3.3.2.2.	Ausgewählte Werkzeuge zur Mitigation von IT-Risiken unter besonderer Berücksichtigung von „Black-Swan“-Risiken	61
3.3.2.2.1.	Attention buys you time, and time buys you options	62
3.3.2.2.2.	Luck is not a strategy	62
3.3.2.2.3.	Belt and Suspenders	63
3.3.2.2.4.	Steering Committees	63
3.3.2.2.5.	Security Deputies/IS-Champions	64
3.3.2.2.6.	Silent Security Audits	65
3.3.2.2.7.	Satellite Companies	65
3.3.2.2.8.	Firefighting Processes	66
3.3.2.2.9.	Prevention Paradox	67
3.3.2.2.10.	Bug Bounty Program	68
3.3.2.2.11.	Toxic-Components und Burndown Chart	69

3.3.2.3.	Mögliche Re-Evaluierung von On-Prem vs Cloud ...	70
3.3.3.	Summary	72
4.	Finanzmarkt-Bedrohungslage	73
4.1.	Begriffsbestimmungen	73
4.2.	Motivation, Ziele und Angriffstechniken	74
4.2.1.	Motivation	74
4.2.2.	Die Ziele von Cyberangriffen	75
4.2.3.	Die wesentlichsten Angriffstechniken	75
4.2.3.1.	Denial of Service	75
4.2.3.2.	Social Engineering	76
4.2.3.3.	Typosquatting	78
4.2.3.4.	DNS Spoofing	79
4.2.3.5.	Waterholing	80
4.2.3.6.	Bösartige Software (Malware)	80
4.2.3.6.1.	Viren, Würmer, Trojaner und Spyware	80
4.2.3.6.2.	Ransomware	81
4.2.3.7.	Fehlerhafte Software und Konfiguration	83
4.2.3.7.1.	Session Hijacking	83
4.2.3.7.2.	Cross-Site-Scripting	84
4.2.3.7.3.	Drive-by attacks	84
4.2.3.7.4.	Code Injection	85
4.2.3.7.5.	Unsichere Kryptografie	85
4.2.3.8.	Veränderung von Daten	86
4.2.3.8.1.	Defacement	86
4.2.3.8.2.	Datenbankenmanipulation	86
4.2.3.8.3.	Datentransfer und „Adversary in the Middle“ (AitM)	87
4.2.4.	Systematische Einordnung der Angriffsarten	87
4.2.4.1.	Lockheed Martin „Cyber Kill Chain“	87
4.2.4.2.	Tactics, Techniques, and Procedures	88
4.2.4.3.	MITRE ATT&CK	88
4.2.4.4.	Pyramid of Pain	89
4.2.5.	Kategorisierung von Angreifern	91
4.2.5.1.	Organisierte Kriminalität	91
4.2.5.2.	Hacker	92
4.2.5.3.	Insidertäter	92
4.2.5.4.	Nation States	92
4.2.5.5.	Hacktivismus	93
4.3.	Die Herausforderungen bei der Abwehr von Cyberbedrohungen	94
4.3.1.	Technologische Komplexität und Dynamik	94
4.3.2.	Vulnerabilitäten	95

Inhaltsverzeichnis

4.3.3.	Schwachstellenmärkte	96
4.3.4.	Der menschliche Faktor	96
4.4.	Die wesentlichsten Cyberangriffsarten im Finanzsektor	97
4.4.1.	Trojanische Apps	97
4.4.2.	Cryptocurrency Theft	98
4.4.3.	Data Breach	99
4.4.4.	DDoS	99
4.4.5.	Ransomware	100
4.4.6.	Malware	100
4.4.7.	Phishing	101
4.4.8.	Zwei-Faktor/Multifaktor-Authentifizierungs-Bypass	101
4.5.	Auswirkung von DORA auf Cyberangriffsarten	102
4.5.1.	Prüfung von Drittienstleistern	103
4.5.2.	Prüfung von Software	103
4.5.3.	Erkennung von Data Breaches	104
4.5.4.	Threat-Led Penetration Testing	104
4.5.5.	Identifizierung aller Assets und IKT-Ressourcen	105
4.5.6.	Verpflichtende Verschlüsselung	105
4.5.7.	Identity Management & Access Control	106
4.5.8.	Vulnerability & Patch Management	106
4.6.	Auswirkung von Artificial Intelligence auf Cyberangriffe	107
4.7.	Trends und Ausblick	108
5.	Meldung von Vorfällen und Bedrohungen	111
5.1.	Einleitung	111
5.2.	Begriffsdefinitionen	111
5.2.1.	Vorfall (Incident)	112
5.2.2.	IKT-bezogener Vorfall	112
5.2.3.	Schwerwiegender IKT-bezogener Vorfall	113
5.2.4.	Zahlungsbezogener Betriebs- oder Sicherheitsvorfall	113
5.2.5.	Schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfall	113
5.2.6.	Cyberbedrohung	114
5.2.7.	Erhebliche Cyberbedrohung	114
5.2.8.	Schwachstelle	115
5.3.	Klassifizierung von Vorfällen und Cyberbedrohungen	116
5.4.	Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen	119
5.4.1.	Bedeutung für Finanzunternehmen und die Finanzmarktaufsicht	120
5.4.2.	Der Meldeprozess	121

5.4.2.1.	Inhalte der Erstmeldung auf einen Blick	121
5.4.2.2.	Meldefristen	122
5.4.2.3.	Kommunikation mit der Finanzmarktaufsicht	123
5.4.3.	Datenqualität	124
5.4.4.	Innerbehördlicher Informationsfluss	124
5.4.5.	Meldeverpflichtungen für Finanzunternehmen nach NIS-2	125
5.4.6.	Strafen bei Meldeversäumnissen	126
5.5.	Fazit	126
6.	Threat-Led Penetration Testing in der Praxis: Die Umsetzung von TIBER in Österreich	127
6.1.	Testen der Cyber-Resilienz von Finanzunternehmen in der EU	127
6.1.1.	Ursprung von TIBER	127
6.1.2.	Das einheitliche Rahmenwerk auf EU-Ebene: TIBER-EU	128
6.2.	Die österreichische Umsetzung von TIBER-EU	130
6.2.1.	Ein Überblick über TIBER-AT	130
6.2.2.	Akteure bei einem TIBER-AT-Test	130
6.2.3.	Phasen eines TIBER-AT-Tests	134
6.2.4.	„Tricks of the Trade“: die Details entscheiden	136
6.3.	Neuerungen bei TLPT gemäß TIBER unter DORA	137
6.3.1.	Einleitung	137
6.3.2.	Ausgewählte Elemente des RTS on TLPT	137
6.3.3.	Weitere aktuelle Entwicklungen und Ausblick	140
6.4.	Exkurs: Erkenntnisse in Deutschland aus fünf Jahren TIBER-DE	141
6.4.1.	Einführung	141
6.4.2.	Grundlagen und Besonderheiten von TIBER-DE	141
6.4.3.	Kooperation und Informationsaustausch	142
6.4.4.	Erkenntnisse, Implikationen und Auswirkungen	143
6.4.5.	Fazit aus fünf Jahren TIBER-DE	149
7.	Das Management des Drittparteienrisikos und der neue Überwachungsrahmen für kritische IKT-Drittdienstleister	151
7.1.	Einleitung	151
7.1.1.	Vorteile und Chancen durch Nutzung von IKT-Drittdienstleistern	151
7.1.2.	Risiken bei der Nutzung von IKT-Drittdienstleistern	151
7.1.3.	Die Bedeutung der Lieferkette beim Management von IKT-Risiken	152

Inhaltsverzeichnis

7.2. Regulatorische Vorgaben im Bereich IKT-Auslagerungsmanagement	154
7.2.1. IKT-Drittparteienrisiko als integraler Bestandteil des IKT-Risikos	154
7.2.2. Definition des IKT-Drittparteienrisikos	155
7.2.2.1. Kritikalitätseinstufung	156
7.2.3. Strategie zu IKT-Drittparteienrisiko	157
7.2.4. Vorvertragliche Pflichten	159
7.2.4.1. Due Diligence	159
7.2.4.2. Risikobewertung	160
7.2.4.3. Ausstiegsplanung	161
7.2.5. Vertragliche Bestimmungen bei einer Inanspruchnahme eines IKT-Drittdienstleisters	163
7.2.6. Laufende Überwachung von IKT-Drittdienstleistern durch das Finanzunternehmen	164
7.2.7. Informationsregister und Meldepflichten	165
7.3. Der Überwachungsrahmen für kritische IKT-Drittdienstleister	168
7.3.1. Hintergrund	168
7.3.2. Überwachungsmechanismus	169
7.3.2.1. Institutionen des Überwachungsmechanismus und ihre Rollen	170
7.3.2.2. Einstufungskriterien und Einstufungsmodalitäten für kritische IKT-Drittdienstleister	173
7.3.2.3. Vorgaben für kritische IKT-Drittdienstleister	175
7.3.3. Maßnahmen und Rechtsdurchsetzung	176
7.3.3.1. Jährlicher Überwachungsplan	176
7.3.3.2. Befugnisse der federführenden Überwachungsbehörde	177
7.3.4. Kritische IKT-Drittdienstleister in Drittstaaten	180
7.4. Praktische Lösungsansätze für das Drittparteien-Risikomanagement	181
7.4.1. Kritikalitätseinstufung und Kategorisierung	181
7.4.2. Risikomanagementmaßnahmen	185
7.4.2.1. Basissicherheit	186
7.4.2.2. Risikobasierte Sicherheitsstandards	189
7.4.3. Überwachung und Steuerung der Dienstleistungsgüte	190
8. IKT-Risiko-Beaufsichtigung im Bankensektor	193
8.1. Aufbau der österreichischen Bankenaufsicht	193
8.1.1. Organisatorischer Aufbau der österreichischen Bankenaufsicht	193

8.1.1.1.	Die Finanzmarktaufsichtsbehörde in der Bankenaufsicht	194
8.1.1.2.	IKT-Risiko-Aufsicht im Bereich Bankenaufsicht in der FMA	194
8.1.1.3.	Die Oesterreichische Nationalbank in der Bankenaufsicht	195
8.1.1.4.	IKT-Risiko-Aufsicht in der OeNB	195
8.1.2.	Rechtliche Grundlagen bis zur DORA	195
8.1.3.	Einbindung der Bankenaufsicht in den DORA-Hub der FMA	197
8.2.	Vor-Ort-Prüfungen	198
8.2.1.	Prüfinhalte und -schwerpunkte bei IKT-Risiko-Prüfungen	198
8.2.2.	Exkurs: Prüfplanung	200
8.2.2.1.	Nationale Prüfplanung	200
8.2.2.2.	Prüfplanung auf europäischer Ebene	201
8.2.3.	Ablauf einer Vor-Ort-Prüfung	202
8.2.3.1.	Prüfungsvorbereitung	202
8.2.3.2.	Prüfungsdurchführung	203
8.2.3.3.	Prüfergebnis und Prüfbericht	204
8.2.4.	Änderungen durch DORA	204
8.3.	Laufende behördliche Aufsicht	205
8.3.1.	Aufsichtlicher Überprüfungs- und Bewertungsprozess (SREP)	205
8.3.2.	Analysen/Sonderanalysen	207
8.3.3.	Der Mängelverfolgungsprozess bei Vor-Ort-Prüfungen	208
8.3.4.	Meldewesen von IKT-bezogenen Vorfällen im Bankensektor – Vergleich ZaDiG 2018 und DORA	209
8.3.4.1.	Meldeprozess	210
8.3.4.2.	Fristen	210
8.3.4.3.	Klassifizierung von Vorfällen	211
8.3.4.4.	Behördliche Behandlung von Vorfällen	213
8.3.4.5.	Abgrenzung zum SSM Cyber Incident Reporting	214
8.3.4.6.	Zusammenführung der Meldeverpflichtungen	214
8.3.4.7.	Zahlen zu Vorfällen im Überblick	214
8.3.5.	IKT-Auslagerungen	216
8.4.	Aufsichtsmaßnahmen/Verwaltungsstrafen	217
8.4.1.	Maßnahmenbescheid gemäß § 70 Abs 4 BWG	217
8.4.2.	SREP-Aufschlag für operationelle Risiken	218
8.4.3.	§ 98 Abs 5 Z 4 BWG und § 99d BWG sowie Strafen gemäß DORA bzw DORA-Vollzugsgesetz	219

Inhaltsverzeichnis

8.4.4.	Verstöße gegen Meldeverpflichtungen gemäß ZaDiG/NISG	221
8.5.	Weitere Aufsichtstätigkeiten	222
8.5.1.	IKT-Systembetreiberlandkarte/Austrian Digital Finance Landscape	222
8.5.2.	Digitalisierungsumfrage	223
8.5.3.	Planspiele und Stresstests	224
8.5.3.1.	Cybercoin 2019	224
8.5.3.2.	Cyber Dry Run 2023	225
8.5.3.3.	Cyberstresstest 2024	225
8.5.4.	IT-Governance Deep Dives	226
8.5.5.	Sonstige Maßnahmen	227
8.5.6.	Nationale und internationale Zusammenarbeit	228
8.5.7.	Exkurs: EU-SCICF	228
9.	IT-Risiko-Beaufsichtigung im Versicherungs- und Pensionskassensektor	229
9.1.	Spezifika des Versicherungs- und Pensionskassensektors	229
9.1.1.	Strukturentwicklung	229
9.1.2.	Geschäftsmodellbezogene Besonderheiten	230
9.1.3.	Spezifika in Bezug auf IT-Dienstleister	230
9.1.4.	IT-Systeme	231
9.1.5.	Bedrohungslage	233
9.1.6.	Vorfälle	234
9.2.	Gesetzliche Grundlagen	235
9.2.1.	Versicherungssektor	235
9.2.2.	Pensionskassensektor	238
9.3.	ICT Security Toolbox	239
9.3.1.	Cyber Maturity Level Assessment	240
9.3.2.	Cloud Maturity Level Assessment	244
9.3.3.	Blackout Maturity Level Assessment	246
9.3.4.	Cyber Exercise	248
9.3.5.	Assessment zu Mitigationsmaßnahmen	250
9.3.6.	Post-Covid-19-IKT-bezogene Risiken	253
9.3.7.	Incidents	253
9.3.8.	IKT-Systeme	254
9.3.9.	DORA-Gap-Analyse 2024	256
9.4.	Vor-Ort-Prüfungen	257
9.4.1.	Prüfansatz	258
9.4.2.	Rechtliche Beurteilung	259
9.4.3.	Einbezug von IT-Dienstleistern der Unternehmen in Vor-Ort-Prüfungen	259
9.4.4.	Prüfgebiete im Fokus	260

9.4.5.	Erfahrungen und Beurteilung der Situation aus Sicht der Prüfung	261
9.4.6.	Zukünftige Entwicklungen	261
9.5.	Ausblick	262
10.	IT-Risiko-Beaufsichtigung im Wertpapiersektor	263
10.1.	IT-Risiko-Beaufsichtigung bei Wertpapierfirmen	263
10.1.1.	Einleitung	263
10.1.2.	Geltungsbereich Wertpapierfirmen	265
10.1.3.	Vereinfachter IKT-Risikomanagementrahmen für Klasse 3 - Wertpapierfirmen	266
10.1.3.1.	Governance und Steuerung	266
10.1.3.2.	Informationssicherheitsleitlinien und -maßnahmen	267
10.1.3.3.	IKT-Risikomanagement und Klassifizierung von Informations- und IKT-Assets	268
10.1.3.4.	Physische Sicherheit und Zugangskontrolle	269
10.1.3.5.	IKT-Betriebssicherheit	270
10.1.3.6.	Daten-, System- und Netzsicherheit	271
10.1.3.7.	IKT-Sicherheitstests	271
10.1.3.8.	Beschaffung, Entwicklung und Wartung von IKT-Systemen	272
10.1.3.9.	IKT-Projekt- und Änderungsmanagement	272
10.1.3.10.	IKT-Business Continuity Management	273
10.1.3.11.	Testen von Plänen zur Fortführung des Geschäftsbetriebs	274
10.1.3.12.	Bericht über die Überprüfung des vereinfachten IKT-Risikomanagementrahmens	275
10.2.	IT-Risiko-Beaufsichtigung bei Verwaltungsgesellschaften	276
10.2.1.	Einleitung und Geltungsbereich	276
10.2.2.	(Immo-)Kapitalanlagegesellschaften, Alternative Investmentfondsmanager	277
10.2.2.1.	Besonderheiten im Hinblick auf die Konstruktion des Geschäftsmodells	279
10.2.3.	Betriebliche Vorsorgekassen	281
10.2.4.	Künftige DORA-Aufsichtstätigkeit bei Verwaltungsgesellschaften	282
10.3.	DORA & Finanzmarktinfrastrukturen in Österreich	283
10.3.1.	Finanzmarktinfrastrukturen in Österreich	284
10.3.1.1.	Handelsplatz: Wiener Börse AG (WBAG)	285
10.3.1.2.	Zentrale Gegenpartei: CCP Austria Abwicklungsstelle für Börsengeschäfte GmbH (CCP.A)	288

Inhaltsverzeichnis

10.3.1.3.	Zentralverwahrer: OeKB CSD GmbH (OeKB CSD)	290
10.3.2.	Auswirkungen von DORA auf Finanzmarktinfrastrukturen in Österreich	291
10.3.3.	Künftige DORA-Aufsichtstätigkeit bei Finanzmarktinfrastrukturen	293
11. Angrenzende Rechtsakte im Bereich der Cybersicherheit und Resilienz	296
11.1.	Einleitung	296
11.2.	NIS-2-Richtlinie	297
11.2.1.	Hintergrund	297
11.2.2.	Hauptfelder der NIS-2-Richtlinie	299
11.2.2.1.	Fähigkeiten der Mitgliedstaaten	299
11.2.2.2.	Kooperation und Informationsaustausch	301
11.2.2.3.	Cybersicherheitsrisikomanagement	302
11.2.3.	Gegenüberstellung NIS-2-Richtlinie zu DORA	310
11.2.3.1.	Unterschiedliche Grundkonzeption in DORA und NIS2	310
11.2.3.2.	Finanzunternehmen im Anwendungsbereich von DORA und NIS-2-Richtlinie	311
11.2.3.3.	Zusammenarbeit der nationalen Behörden unter DORA und der NIS-2-Richtlinie	315
11.2.3.4.	Sonderfall IKT-Drittienstleister	317
11.2.3.5.	Bestimmungen der NIS-2-Richtlinie mit Relevanz für den Finanzbereich	319
11.3.	Richtlinie über kritische Einrichtungen	322
11.3.1.	Hintergrund	322
11.3.2.	Kerninhalte der RKE-Richtlinie	324
11.3.2.1.	Anwendungsbereich	324
11.3.2.2.	Pflichten	327
11.3.2.3.	Aufgaben der Mitgliedstaaten	328
11.3.3.	Gegenüberstellung zu DORA	329
11.4.	Cyber Resilience Act	331
11.5.	EU-Zertifizierungsrahmen	333
11.6.	Schlusswort	334
12. Informationsaustausch und Zusammenarbeit aller Stakeholder bei Cyberbedrohungen	336
12.1.	Der Mehrwert im Austausch von Bedrohungsinformationen	336
12.2.	Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen nach DORA	338
12.3.	Status quo des Austauschs von Bedrohungsinformationen im Finanzsektor in Österreich	339

12.4. Zielbild einer strukturierten Zusammenarbeit durch eine zentrale Stelle	342
12.5. Skandinavien als Vorbild	344
12.6. Case Study: Informationsaustausch und Zusammenarbeit beim Ivanti Secure Connect VPN Zero-Day-Vorfall	345
13. Sanktionsregime	350
13.1. Einleitung	350
13.1.1. Zuständige Behörde für das Sanktionsregime	350
13.1.2. Verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen	351
13.1.3. Strafrechtliche Sanktionen	353
13.2. Adressaten der Verwaltungsstrafatbestände	353
13.2.1. Rechtsträger	353
13.2.2. Verantwortliche	354
13.3. Verfahrensrechtliche Bestimmungen	356
13.3.1. Subsidiarität	356
13.3.2. Verjährung	357
13.3.3. Opportunität	358
13.3.4. Verfahrensbeendigung gemäß § 22 Abs 2b FMABG ...	359
13.3.5. Gesamtstrafe – Absorptionsprinzip	359
13.4. Die einzelnen Strafnormen	361
13.4.1. Verstoß gegen Anforderungen an das IKT-Risikomanagement	361
13.4.2. Verstoß gegen Anforderungen an das vereinfachte IKT-Risikomanagement	361
13.4.3. Fehlverhalten in Bezug auf IKT-bezogene Vorfälle und Cyberbedrohungen	362
13.4.4. Fehlverhalten in Bezug auf Testung der digitalen operationalen Resilienz	362
13.4.5. Keine erweiterten Tests als ermitteltes Unternehmen	362
13.4.6. Fehlverhalten in Bezug auf das Drittspielenrisiko oder vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen	363
13.4.7. Fehlverhalten betreffend einen IKT-Drittspieler mit Sitz in einem Drittland	364
13.4.8. Verstoß gegen Anordnungen der FMA	365
13.4.9. Pflichtverletzung bei Austausch von Informationen	365
13.4.10. Sonstige Pflichtverletzungen mit Konnex zur DORA	366

13.5. Strafbestimmungen betreffend juristische Personen	366
13.5.1. Allgemeines	366
13.5.2. Die Zurechnung	368
13.5.2.1. Allgemeines	368
13.5.2.2. Führungskräftetat	369
13.5.2.3. Tätigentat	371
13.5.2.4. Relation zwischen Führungskräftetat und Tätigentat	372
13.5.3. Der Strafrahmen	373
13.6. Strafbemessung	375
13.6.1. Ausgangslage	375
13.6.2. Bemessungskriterien nach DORA-VG	376
13.7. Öffentliche Bekanntmachung verwaltungsrechtlicher Sanktionen	377
13.7.1. Allgemeines	377
13.7.2. Zeitpunkt und Ort der Veröffentlichung	379
13.7.3. Zweck der Veröffentlichung	380
13.7.4. Umfang der Veröffentlichung	381
13.7.5. Prüfmaßstab	382
13.7.5.1. Allgemeine Verhältnismäßigkeitsprüfung	382
13.7.5.2. Gefährdung der Stabilität der Finanzmärkte	384
13.7.5.3. Gefährdung der Durchführung laufender strafrechtlicher Ermittlungen	385
13.7.5.4. Unverhältnismäßig hoher Schaden	385
13.7.6. Aufschub der (personenbezogenen) Veröffentlichung	386
13.7.7. Aktualisierung der Veröffentlichung und Veröffentlichungsdauer	386
13.7.8. Lauf des Veröffentlichungsverfahrens und Überprüfungsverfahren	387
14. Typische Herausforderungen bei der Implementierung einer zeitgemäßen Informations- und IT-Sicherheitsarchitektur unter DORA	388
14.1. Warum braucht es neue Ansätze wie DORA?	388
14.2. Umsetzung einer zeitgemäßen Informations- und IT-Sicherheitsarchitektur	389
14.2.1. Aufwand und Komplexität bei der Umsetzung der Anforderungen	390
14.2.1.1. Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle	391
14.2.1.2. Testen der digitalen operationalen Resilienz	394
14.2.1.3. IKT-Risikomanagement	396

Inhaltsverzeichnis

14.2.1.4.	Management des IKT-Drittparteienrisikos	419
14.2.2.	Herausforderungen in der praktischen Umsetzung	422
14.2.2.1.	Komplexität der Implementierung	423
14.2.2.2.	Definition „kritischer oder wichtiger“ Funktionen	425
14.2.2.3.	DORA und Cybersecurity	429
14.2.2.4.	Relevante Richtlinien in Ergänzung zu DORA	432
14.3.	Von der Idee zur Umsetzung – Wie funktioniert die Implementierung in der Praxis?	434
	Stichwortverzeichnis	439