

Inhaltsverzeichnis

	Seite
1. Vorwort	1
2. Thematische Einführung	3
3. Operationale Resilienz und der Weg zur DORA-Gesetzgebung	7
3.1 Operationale Resilienz und ihre wachsende Bedeutung	7
3.1.1 Resilienz in der VUCA-Welt	7
3.1.2 Treiber für operationale Resilienz in Versicherungs- unternehmen	8
3.2 Aktuelle Regulierung zu Resilienz im globalen Kontext	11
3.2.1 Officer of the Comptroller of the Currency (OCC) „Sound Practices to Strengthen Operational Resilience“ (USA)	11
3.2.2 Basel Committee on Banking Supervision – Prinzipien der operationalen Resilienz	13
3.2.3 Financial Conduct Authority (FCA) und Prudential Regulation Authority (PRA) – nationale Gesetzgebung zum Aufbau operativer Resilienz	14
3.3 DORA und seine Grundprinzipien	16
3.3.1 Strategische Rahmenvorgaben	17
3.3.2 IKT-Risikomanagementrahmen	18
3.3.3 IKT-Governance und Leitlinien	20
3.3.4 Dienstleister und Ausgliederungen	20
3.3.5 Business Continuity Management	21
3.3.6 IKT-Incidents	22
3.3.7 Szenarien und Testing	22
3.3.8 Meldepflichten	23
4. Die DORA-Themenbereiche und aktuelle Regulierungs- standards	25
4.0 Grundlagen und Anwendungsrahmen	25
4.1 Resilienz- und Dienstleisterstrategie	26
4.1.1 Dokumentation kritischer und wichtiger Geschäfts- funktionen	27
4.1.2 Resilienzstrategie („DOR-Strategie“) und	31
4.1.3 Strategie für IKT-Dienstleister-Risikomanagement (Dienstleister-Strategie)	31
4.1.4 Modellierter Aktualisierungsprozess inklusive Auslöser	34
4.1.5 Definition von KPIs zur Bewertung der Resilienz	34
4.2 IKT-Risikomanagementrahmen	35
4.3 IKT-Governance und Leitlinien	41

	Seite
4.4 Dienstleister und Ausgliederungen	54
4.4.1 Informationsregister	58
4.4.2 Mindestvertragsinhalte für IKT-Dienstleisterverträge	61
4.4.3 Leitlinie und Operationalisierung der regulären Überwachung der IKT-Dienstleister	63
4.4.4 Überarbeitete und aktualisierte Ausgliederungsrichtlinie	64
4.4.5 Konzept für Ausstiegsstrategien („Exit-Strategies“) für kritische und wichtige IKT-Dienstleister	65
4.4.6 Individuelle Ausstiegsstrategien („Exit-Strategies“) für kritische und wichtige IKT-Dienstleister	66
4.4.7 Nachweis der Kosten/Nutzen- und Konzentrationsanalysen für IKT-Dienstleisterbeziehung	67
4.4.8 Nachweis der Durchführung von IKT-Notfallplänen kritischer IKT-Dienstleister	69
4.4.9 Prozess und Meldepflicht bei neuer Aufnahme eines IKT-Dienstleisters	69
4.5 Business Continuity Management	70
4.5.1 Erstellung und Operationalisierung einer BCM- oder Geschäftsfortführungsrichtlinie	71
4.5.2 Erstellung oder Aktualisierung von IKT-Geschäftsfortführungsplänen	72
4.5.3 Erstellung oder Aktualisierung von spezifischen IKT-Reaktions- und Wiederherstellungsplänen	73
4.5.4 Kommunikationsstrategie und -pläne für schwerwiegende Störfälle	74
4.6 IKT-Incidents	75
4.6.1 Überprüfung, Durchführung und ggf. Erweiterung der BIA für schwerwiegende IKT-Vorfälle	80
4.6.2 Kommunikationsstrategie, Testverfahren und -pläne zur Kommunikationsdurchführung	80
4.6.3 Anforderungskatalog zu Kompetenz Krisenstabsfunktion	80
4.6.4 Prozesserstellung, -operationalisierung und -dokumentation für schwerwiegende IKT-Vorfälle	80
4.6.5 Kriterienkatalog und Leitfaden für schwerwiegende IKT-Vorfälle	81
4.6.6 Richtlinie und Umsetzung einer Angriffserkennung und Datenverlust-Sicherung (Intrusion Detection und Data Loss Prevention)	81
4.7 Szenarien und Testing	81
4.7.1 „Digitale Resilienz-Testrichtlinie“	83
4.7.2 Prozessdokumentation und Operationalisierung der Schwachstellenprüfung und Maßnahmenpriorisierung	84
4.7.3 Durchgeführte und protokollierte IKT-Tests	84

	Seite
4.7.4 Für BaFin benannte Unternehmen: Konzeption und Durchführung der TLPTs nach regulatorischer Vorgabe	85
4.8 Meldepflichten und Reporting	86
4.8.1 Prozess und Operationalisierung Meldung schwerwiegender IKT-Vorfälle,	87
4.8.2 Dokumentvorlage für Erstmeldung, Zwischenmeldung und Abschlussmeldung sowie	87
4.8.3 Dokumentvorlage für RCA & Abschlussbericht	87
4.8.4 Prozessdokumentation und Operationalisierung IKT-Vertragsregister-Meldung	90
5. DORA und Wechselwirkung zu bestehender Versicherungsregulierung	93
5.1 Einführung und Auswahl	93
5.2 Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen („MaGo“) – Mindestanforderungen an die Geschäftsorganisation von kleinen Versicherungsunternehmen („MaGo – kleine VU“)	94
5.3 Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter – aktualisiert als Aufsichtsmitteilung zur Auslagerungen an Cloud Anbieter (Regulatorische Zusammenfassung)	99
5.4 „Network and Information Security“-Richtlinie 2 („NIS-2“)	107
5.5 Versicherungsaufsichtliche Anforderungen an die IT (VAIT)	108
5.5.1 Höherer Anforderungsumfang & Detailgrad	111
5.5.2 Unterschiedliche Begriffsdefinitionen	111
5.5.3 Stärkere Verknüpfung der Themen	111
5.5.4 Konkretisierung durch technische Standards	111
5.5.5 IKT-Risikomanagement	111
5.5.5.1 Erkennung	112
5.5.5.2 Reaktion und Wiederherstellung	112
5.5.5.3 Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung	112
5.5.5.4 Lernprozesse und Weiterentwicklung	112
5.5.5.5 Kommunikation	112
5.5.6 Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle und Testen der digitalen operationalen Resilienz	113
5.5.6.1 Klassifizierung von IKT-bezogenen Vorfällen und Störfällen	113
5.5.6.2 Meldung schwerwiegende IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen	113
5.5.6.3 Harmonisierung von Inhalten und Vorlagen zu regulatorischen Meldungen	113

	Seite
5.5.6.4 Zentralisierung der Berichterstattung über schwerwiegende IKT-bezogene Vorfälle	113
5.5.6.5 Allgemeine Testanforderungen für digitale operationale Resilienz	114
5.5.6.6 Testen von IKT-Systemen und relevanten Tools	114
5.5.6.7 Anforderungen an Tester bezüglich der Durchführung von TLPTs	114
5.5.7 Management des IKT-Drittdienstleister- und Drittparteien-risikos	115
5.5.7.1 Allgemeine Prinzipien	115
5.5.7.2 Bewertung des IKT-Konzentrationsrisikos auf Ebene des individuellen Versicherungsunternehmens	115
5.5.7.3 Wesentliche Vertragsbestimmen für IKT-Dienstleister-verträge	116
5.6 Ergänzung des regulatorischen Ordnungsrahmens	117
6. Praktische Aspekte und Erfolgsfaktoren der DORA-Umsetzung	119
6.1 Aktueller Umgang mit RTS/ITS Regulierungsstandards	119
6.1.1 Art. 15 – RTS zum IKT-Risikomanagementrahmen/Art. 16 – RTS zum vereinfachten IKT-Risikomanagementrahmen (JCS 2023_86 IKT Risikomanagementrahmen)	120
6.1.2 Art. 29 Präzisierung der Leitlinie zur Nutzung von IKT-Dienstleistungen (JC 2023_85 ITS Informationsregister)	124
6.1.3 Art. 18 RTS über Kriterien zur Klassifizierung IKT-bezogener Vorfälle (JCS 2023_83 RTS Klassifizierung schwerwiegender Vorfälle und bedeutender Cyber-Bedrohungen)	129
6.1.4 Art. 29 RTS über Kriterien zur Klassifizierung IKT-bezogener Vorfälle (JCS 2023_84 RTS zur weiteren Spezifizierung der Richtlinie zur Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Geschäftsfunktionen)	130
6.2 DORA im Drei-Linien-Modell	131
6.2.1 Geschäftsleitung	132
6.2.2 1. Linie: Fachbereiche und operative Einheiten (First Line of Defense – FLOD)	134
6.2.3 2. Linie – Risikomanagement (Second Line of Defense – SLOD)	135
6.2.4 3. Linie – Revision (Third Line of Defense)	136
6.2.5 Die Rolle des Informationssicherheitsbeauftragten (ISB) in der DORA-Umsetzung	137
6.3 Mögliches Vorgehensmodell für eine DORA-Gap-Analyse	139
6.3.1 Ermittlung des DORA-Ist-Zustandes	141
6.3.2 Bestimmung des regulatorischen „DORA-Ambitionsniveaus“	145
6.3.3 Erarbeitung der Gap-Analyse und Ableitung von Handlungsempfehlungen	148

	Seite
6.4 Mögliches Vorgehensmodell für DORA-Umsetzung	150
6.4.1 Entscheidung für Organisationsform – Linien- versus Projektumsetzung der DORA-Anforderungen	150
6.4.2 DORA-spezifische Aspekte der Projektmanagementprozesse . .	155
6.5 DORA-Zielbetriebsmodell und Rollen, Aufgaben und Verant- wortlichkeiten	160
6.5.1 Kontinuierliche Berücksichtigung und Aktualisierung verbundener Information Assets	160
6.5.2 Starke, integrierte IT- und Cyber-Security Funktion mit Softwareunterstützung auf dem Stand der Technik	162
6.5.3 Konsistente strategische Abstimmung zwischen Versiche- rungsgruppe und Versicherungsunternehmen	163
6.5.4 Betriebliche Rollen, Aufgaben und Verantwortlichkeiten	165
6.6 DORA-Umsetzungsaspekte in ausgewählten VU-Konstellationen . . .	167
7. Ausblick und weitere Schritte	175
8. Danksagung	179
Stichwortverzeichnis	181