

# Inhaltsverzeichnis

	Seite
<b>1 Vorwort zur 2. Auflage</b> .....	1
<b>2 Thematische Einführung</b> .....	5
<b>3 Operationale Resilienz und der Weg zur DORA-Gesetzgebung</b> .....	11
3.1 Operationale Resilienz und ihre wachsende Bedeutung .....	11
3.1.1 Resilienz in der VUCA-Welt .....	11
3.1.2 Treiber für operationale Resilienz in Versicherungsunternehmen .....	12
3.2 Aktuelle Regulierung zu Resilienz im globalen Kontext .....	16
3.2.1 Officer of the Comptroller of the Currency (OCC) „Sound Practices to Strengthen Operational Resilience“ (USA) .....	16
3.2.2 Basel Committee on Banking Supervision – Prinzipien der operationalen Resilienz .....	17
3.2.3 Financial Conduct Authority (FCA) und Prudential Regulation Authority (PRA) – nationale Gesetzgebung zum Aufbau operationaler Resilienz .....	18
3.2.4 Australian Prudential Regulation Authority – Prudential Standard CPS 230 .....	20
3.3 DORA und seine Grundprinzipien .....	22
3.3.1 Strategische Rahmenvorgaben .....	23
3.3.2 IKT-Risikomanagementrahmen .....	25
3.3.3 IKT-Governance .....	26
3.3.4 Dienstleister und Ausgliederungen .....	27
3.3.5 Business Continuity Management .....	28
3.3.6 IKT-Incidents .....	28
3.3.7 Szenarien und Testing .....	29
3.3.8 Meldepflichten .....	30
<b>4 Die DORA-Themenbereiche und aktuelle Regulierungsstandards</b> .....	33
4.0 Grundlagen und Anwendungsrahmen .....	33
4.1 Resilienz- und Strategiedokumente .....	35
4.1.1 Dokumentation kritischer und wichtiger Geschäftsfunktionen .....	37
4.1.2 Resilienzstrategie („DOR-Strategie“) und Strategie für IKT-Dienstleister-Risikomanagement (Dienstleister-Strategie) .....	41
4.1.3 Aktualisierung/Abnahme Kommunikationsprozess inkl. Auslöser für anlassbezogene Änderungen .....	45
4.1.4 Definition und Übersichtsdarstellung von KPIs zur Bewertung der Resilienz .....	45
4.1.5 Kommunikationsstrategie für IKT-bezogene Vorfälle .....	46

	Seite
4.1.6    Management- und Mitarbeiterschulung zur digitalen operationalen Resilienz .....	47
4.1.7    Programme zur Sensibilisierung für IKT-Sicherheit .....	47
4.2    IKT-Risikomanagementrahmen .....	48
4.3    IKT-Governance .....	56
4.3.1    Informationssicherheitsleitlinie .....	58
4.3.2    Richtlinien und Verfahren für das Management von IKT-Assets .....	59
4.3.3    Einrichtung eines Inventars von IKT-Funktionen, Rollen und Verantwortlichkeiten, Assets und Dienstleistern („IKT-Asset-Management“) .....	59
4.3.4    Inventar alle IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten .....	61
4.3.5    Dokumentation IKT-Governance-Regelungen und Budgetzuweisung hierzu .....	62
4.3.6    Einrichtung eines zentralen IKT-Melderegisters und Meldeprozesses an die Geschäftsleitung des Versicherungsunternehmens .....	63
4.3.7    Richtlinie für Verschlüsselung und kryptografische Kontrollen .....	64
4.3.8    Register aller Zertifikate und Zertifikatsspeicher für IKT-Assets, die kritische wichtige Funktionen unterstützen .....	68
4.3.9    Richtlinie und Verfahren für das Management der IKT-Vorgänge (Betrieb) .....	69
4.3.10    Verfahren für das Kapazitäts- und Leistungsmanagement (inkl. Überwachung) .....	71
4.3.11    Verfahren für das Schwachstellenmanagement .....	71
4.3.12    Richtlinie für Patches und Updates und Verfahren für das Patchmanagement .....	72
4.3.13    Verfahren für die Daten- und Systemsicherheit .....	73
4.3.14    Einrichtung von Richtlinien und Verfahren zur Datensicherung .....	75
4.3.15    Richtlinie für das Management der Netzwerksicherheit sowie Verfahren, Protokolle und Tools für das Management der Netzwerksicherheit .....	76
4.3.16    Richtlinie für das IKT-Projektmanagement .....	77
4.3.17    Richtlinie und Verfahren für die Beschaffung, Wartung und Entwicklung von IKT-Systemen .....	78
4.3.18    Richtlinien, Verfahren und Kontrollen für das IKT-Änderungsmanagement .....	79
4.3.19    Richtlinien für die physische Sicherheit und die Sicherheit von Umweltereignissen .....	79
4.3.20    Verfahren, Protokolle und Tools für die Datenaufzeichnung (Logging) .....	80

	Seite
4.3.21 Dokumentation eines vollständigen Risikokataloges inkl. Auslöser für Änderungen .....	81
4.3.22 Kommunikationsleitlinien und Kommunikationspläne in Bezug auf den IKT-Risikomanagementrahmen .....	82
4.3.23 Durchführung eines regelmäßigen Schulungsprogramms für die Geschäftsleitung zur Steuerung von IKT-Risiken .....	82
4.3.24 Dokumentation eines vollständigen Risikokataloges inkl. Auslöser für Änderungen .....	82
4.3.25 Anpassung der Personalrichtlinie zu IKT-Sicherheitsrahmen ..	83
4.4 IKT-Dienstleister und Ausgliederungen .....	83
4.4.1 Vollständig befülltes IKT-Informationsregister .....	88
4.4.2 Leitlinie für die Nutzung von IKT-Dienstleistungen für kritische und wichtige Funktionen .....	93
4.4.3 Überarbeitete und aktualisierte Ausgliederungsrichtlinie – Leitlinie für IKT-Dienstleistungen .....	93
4.4.4 Durchgeführte Anpassungen aller IKT-Dienstleistungsverträge .....	95
4.4.5 Durchgeführte Anpassungen aller IKT-Dienstleistungsverträge, die kritische und wichtige Funktionen unterstützen ..	96
4.4.6 Ausstiegspläne („Exit-Strategies“) für IKT-Dienstleister in kritischen wichtigen Funktionen .....	97
4.4.7 Prozess und Operationalisierung der Meldepflicht bei Aufnahme einer neuen wesentlichen IKT-Dienstleistung .....	100
4.4.8 Inventar aller Prozesse die von IKT-Drittienstleistern abhängen .....	101
4.4.9 Nachweis der Kosten/Nutzen- und Konzentrationsanalysen für IKT-Dienstleisterbeziehung .....	101
4.5 Business Continuity Management .....	103
4.5.1 Allgemeine Geschäftsfortführungsleitlinie inkl. Business-Impact-Analyse (BIA) .....	104
4.5.2 IKT-Geschäftsfortführungsleitlinie .....	107
4.5.3 IKT-Geschäftsfortführungspläne (IKT-GFP) .....	109
4.5.4 IKT-Reaktions- und Wiederherstellungspläne .....	110
4.5.5 Aufzeichnung über Tätigkeiten vor und während Störungen ..	112
4.5.6 Richtlinie und Verfahren für die Datensicherung (Backup) ..	112
4.5.7 Wiedergewinnungs- und Wiederherstellungsverfahren .....	112
4.6 IKT-Incidents und Meldepflichten .....	113
4.6.1 Richtlinie für die Behandlung IKT-bezogener Vorfälle .....	118
4.6.2 Kommunikationsstrategie, Testverfahren und -pläne zur Kommunikationsdurchführung und Anforderungskatalog zu Kompetenz Krisenstabsfunktion .....	119
4.6.3 Prozesserstellung, -operationalisierung und -dokumentation zur Erkennung und Behandlung sowie Meldung schwerwiegender IKT-Vorfälle .....	119

	Seite
4.6.4 Kriterienkatalog und Erkennungsmechanismus für anomale Aktivitäten und Klassifizierung schwerwiegender IKT-Vorfälle .	121
4.6.5 Dokumentation IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen . . . . .	122
4.6.6 Dokumentvorlage für Erst-, Abschluss- und Zwischenmeldung und für Root-Cause-Analyse . . . . .	122
4.6.7 Prozessdokumentation und Operationalisierung IKT-Vertragsregister-Meldung . . . . .	125
4.7 Szenarien und Testing . . . . .	126
4.7.1 Programm für die Tests der digitalen operationalen Resilienz . . . . .	128
4.7.2 Leitlinien und Verfahren zur Priorisierung, Klassifizierung und Behebung im Test identifizierter Probleme . . . . .	129
4.7.3 Validierungsmethoden . . . . .	130
4.7.4 Für BaFin benannte Unternehmen: Konzeption und Durchführung der TLPTs nach regulatorischer Vorgabe . . . . .	131
4.7.5 Prozessdokumentation und Operationalisierung IKT-Vertragsregister-Meldung . . . . .	132
4.8 Personalpolitik und Zutrittskontrolle . . . . .	133
<b>5 DORA und Wechselwirkung zu bestehender Versicherungsregulierung . . . . .</b>	<b>137</b>
5.1 Einführung und Auswahl . . . . .	137
5.2 Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen („MaGo“) – Mindestanforderungen an die Geschäftsorganisation von kleinen Versicherungsunternehmen („MaGo – kleine VU“) . . . . .	138
5.3 Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter – aktualisiert als Aufsichtsmitteilung zu Auslagerungen an Cloud Anbieter (Regulatorische Zusammenfassung) . . . . .	142
5.4 Aufsichtsmitteilung – Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteienrisikomanagement . . . . .	150
5.5 „Network and Information Security“-Richtlinie 2 („NIS-2“) . . . . .	156
5.6 Versicherungsaufsichtliche Anforderungen an die IT (VAIT) . . . . .	157
5.7 Ergänzung des regulatorischen Ordnungsrahmens . . . . .	160
<b>6 Praktische Aspekte und Erfolgsfaktoren der DORA-Umsetzung . . . . .</b>	<b>163</b>
6.1 Aktueller Umgang mit RTS/ITS Regulierungsstandards . . . . .	163
6.1.1 RTS zum IKT-Risikomanagementrahmen/RTS zum vereinfachten IKT-Risikomanagementrahmen . . . . .	163
6.1.2 Art. 29 Präzisierung der Leitlinie zur Nutzung von IKT-Dienstleistungen . . . . .	167

	Seite
6.1.3 RTS zu Kriterien zur Klassifizierung IKT-bezogener Vorfälle und Klassifizierung schwerwiegender Vorfälle und bedeuter Cyber-Bedrohungen .....	171
6.1.4 Art. 29 RTS über Kriterien zur Klassifizierung IKT-bezogener Vorfälle zur weiteren Spezifizierung der Richtlinie zur Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Geschäftsfunktionen) .....	172
6.2 DORA im Drei-Linien-Modell .....	173
6.2.1 Geschäftsleitung .....	175
6.2.2 1. Linie: Fachbereiche und operative Einheiten (First Line of Defense – FLOD) .....	177
6.2.3 2. Linie – Risikomanagement (Second Line of Defense – SLOD) .....	178
6.2.4 3. Linie – Revision (Third Line of Defense) .....	179
6.2.5 Die Rolle des Informationssicherheitsbeauftragten (ISB) in der DORA-Umsetzung .....	180
6.2.6 IKT-Risikokontrollfunktion .....	182
6.2.7 Überwachungsfunktion für IKT-Dienstleister .....	183
6.3 Mögliches Vorgehensmodell für eine DORA-Gap-Analyse .....	184
6.3.1 Ermittlung des DORA-Ist-Zustandes .....	185
6.3.2 Bestimmung des regulatorischen „DORA-Ambitionsniveaus“ ..	190
6.3.3 Erarbeitung der Gap-Analyse und Ableitung von Handlungsempfehlungen .....	192
6.4 Mögliches Vorgehensmodell für DORA-Umsetzung .....	195
6.4.1 Entscheidung für Organisationsform – Linien- versus Projektumsetzung der DORA-Anforderungen .....	195
6.4.2 DORA-spezifische Aspekte der Projektmanagementprozesse ..	200
6.5 DORA-Zielbetriebsmodell und Rollen, Aufgaben und Verantwortlichkeiten .....	205
6.5.1 Kontinuierliche Berücksichtigung und Aktualisierung verbundener Information Assets .....	205
6.5.2 Starke, integrierte IT- und Cyber-Security Funktion mit Softwareunterstützung auf dem Stand der Technik .....	207
6.5.3 Konsistente strategische Abstimmung zwischen Versicherungsgruppe und Versicherungsunternehmen .....	208
6.5.4 Betriebliche Rollen, Aufgaben und Verantwortlichkeiten ..	210
6.6 DORA-Umsetzungsaspekte in ausgewählten VU-Konstellationen ..	212
<b>7 Ausblick und weitere Schritte .....</b>	<b>219</b>
<b>8 Danksagung .....</b>	<b>223</b>