

# Inhaltsverzeichnis

Vorwort	5
Inhaltsverzeichnis	7
Symbol- und Abkürzungsverzeichnis	11
Abbildungsverzeichnis	19
Tabellenverzeichnis	21
Verzeichnis der Anlagen im Anhang	23
1. Einleitung	25
1.1. Problemstellung und Zielsetzung des Buches	25
1.2. Aufbau des Buches	29
2. Definition und Systematisierung der IT-Risiken	31
2.1. Grundlagen der bankbetrieblichen Risiken	31
2.1.1. Definition des Begriffs „Risiko“ und Kategorisierung bankbetrieblicher Risiken	31
2.1.2. Unterteilung der operationellen Risiken	33
2.1.3. Einordnung von IT-bezogenen Vorfällen in die Systematisierung der operationellen Risiken	37
2.2. Definition des Begriffs „IT-Risiko“	42
2.3. Schutzziele in Bezug auf IT(-Systeme), Daten bzw. Informationen	46
3. Bestehende regulatorische Anforderungen an das IT- Risikomanagement	49
3.1. Überblick über die zu einem IT-Risikomanagement verpflichtenden Normen	49

3.2.	Sektorübergreifende regulatorische Anforderungen an das IT-Risikomanagement	51
3.2.1.	Aktienrechtliche Anforderungen	51
3.2.2.	Datenschutzrechtliche Anforderungen	53
3.3.	Bankenspezifische Anforderungen an das IT-Risikomanagement durch den Baseler Ausschuss	55
3.4.	Bankenspezifische europäische Anforderungen an das IT-Risikomanagement	57
3.4.1.	Aufsichtsrechtliches Rahmenwerk durch CRR und CRD	57
3.4.2.	Die EBA-Leitlinien	58
3.5.	Bankenspezifische nationale Anforderungen an das IT-Risikomanagement	59
3.5.1.	Anforderungen gemäß § 25a KWG	59
3.5.2.	Anforderungen gemäß MaRisk	60
3.5.2.1.	Anwendungsbereich der MaRisk	60
3.5.2.2.	Aufbau und Veröffentlichungsstand der MaRisk	62
3.5.2.3.	AT 7.2 MaRisk: Anforderungen an die technisch-organisatorische Ausstattung	64
3.5.2.4.	BTR 4 MaRisk: Operationelle Risiken	67
3.5.3.	Analyse der bankaufsichtlichen Anforderungen an die IT (BAIT)	68
3.5.3.1.	Anwendungsbereich und Aufbau der BAIT	68
3.5.3.2.	Kapitel 1 BAIT: IT-Strategie	70
3.5.3.3.	Kapitel 2 BAIT: IT-Governance	74
3.5.3.4.	Kapitel 3 BAIT: Informationsrisikomanagement	76
3.5.3.5.	Kapitel 4 BAIT: Informationssicherheitsmanagement	79
3.5.3.6.	Kapitel 5 BAIT: Operative Informationssicherheit	85
3.5.3.7.	Kapitel 6 BAIT: Identitäts- und Rechtmanagement	87
3.5.3.8.	Kapitel 7 BAIT: IT-Projekte und Anwendungsentwicklung	91
3.5.3.9.	Kapitel 8 BAIT: IT-Betrieb	97
3.5.3.10.	Kapitel 9 BAIT: Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen	102

3.5.3.10.1.	Abgrenzung der Begriffe Auslagerung und sonstiger Fremdbezug	102
3.5.3.10.2.	AT 9 MaRisk: Anforderungen an Auslagerungen von IT-Dienstleistungen	106
3.5.3.10.3.	Kapitel 9 BAIT: Anforderungen an den sonstigen Fremdbezug von IT-Dienstleistungen	108
3.5.3.11.	Kapitel 10 BAIT: IT-Notfall- management	109
3.5.3.12.	Kapitel 11 BAIT: Management der Beziehungen mit Zahlungsdienstnutzern	113
3.5.3.13.	Kapitel 12 BAIT: Kritische Infrastrukturen	114
4.	Zukünftige regulatorische Anforderungen an das IT- Risikomanagement	119
4.1.	Anforderungen gemäß der überarbeiteten Richtlinie für Netzwerk- und Informationssicherheit (NIS-2-RL)	119
4.2.	Regulatorische Anforderungen des Digital Operational Resilience Act (DORA)	121
4.2.1.	Ziele und Aufbau des DORA	121
4.2.2.	Anwendungsbereich des DORA	123
4.2.3.	Kapitel II DORA: IKT-Risikomanagement	126
4.2.3.1.	Art. 5 DORA: Governance und Organisation	126
4.2.3.2.	Art. 6 DORA: IKT- Risikomanagementrahmen	128
4.2.3.3.	Art. 7 DORA: IKT-Systeme, -Protokolle und -Tools	132
4.2.3.4.	Art. 8 DORA: Identifizierung	133
4.2.3.5.	Art. 9 DORA: Schutz und Prävention	135
4.2.3.6.	Art. 10 DORA: Erkennung	137
4.2.3.7.	Art. 11 DORA: Reaktion und Wiederherstellung	138
4.2.3.8.	Art. 12 DORA: Richtlinien und Verfahren zum Backup sowie Verfahren	

	und Methoden zur Wiedergewinnung und Wiederherstellung	143
4.2.3.9.	Art. 13 DORA: Lernprozesse und Weiterentwicklung	145
4.2.3.10.	Art. 14 DORA: Kommunikation	147
4.2.3.11.	Art. 16 DORA: Vereinfachter IKT- Risikomanagementrahmen	148
4.2.4.	Kapitel III DORA: Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle	149
4.2.5.	Kapitel IV DORA: Testen der digitalen operationellen Resilienz	151
4.2.6.	Kapitel V DORA: Management des IKT- Drittparteienrisikos	153
4.3.	Anforderungen an das Risikomanagement von Hochrisiko-KI gemäß der geplanten KI-Verordnung	155
5.	Fazit	159
	Anhang	165
	Literaturverzeichnis	167
	Verzeichnis der Rechtsquellen	191