

Inhaltsverzeichnis

Vorwort 5

Abbildungsverzeichnis 15

Tabellenverzeichnis 17

Abkürzungsverzeichnis 19

Bearbeiterverzeichnis 25

1 Einführung und Kurzüberblick 27

1.1 Einführung 27

1.1.1 Adressaten des Buchs 27

1.1.2 Gliederung des Textes 28

1.1.3 Die Erfolgsgeschichte der BAIT 29

1.1.4 Aufbau der BAIT 33

1.2 Kurzüberblick zu den Neuerungen der BAIT 2.0 35

1.2.1 BaFin-Veröffentlichungen vom 16.08.2021 35

1.2.2 Inhaltlicher Geltungskreis im Teil I BAIT 36

1.2.3 Stärkung der Anforderungen an den Informationsverbund (BAIT-Kapitel II.3.) 38

1.2.4 Anpassungen im BAIT-Kapitel II.4. zur Informationssicherheitsleitlinie
und zum Schulungsprogramm 40

1.2.5 Neues BAIT-Kapitel II.5. Operative IT-Sicherheit 41

1.2.6 Anpassungen in den BAIT-Kapiteln II.6., II.7. und II.8. 42

1.2.7 Neues BAIT-Kapitel II.10. IT-Notfallmanagement 43

1.2.8 Schnittstellen zu den MaRisk-Novellen 44

1.3 Übergang von BAIT zu DORA 45

1.4 Vorgaben in CRR/CRD und im Kreditwesengesetz 47

1.5 Aktivitäten von EZB und EBA inklusive DORA-Umsetzung 54

1.6 Baseler Ausschuss und weitere internationale Gremien 64

1.6.1 Baseler Ausschuss 64

1.6.2 G7 und Financial Stability Board 65

1.7 BSI, KRITIS, IT-Sicherheitsgesetz 2.0 und weitere Neuerungen 67

1.7.1 BSI und ENISA 67

1.7.2 BSI-Gesetz und KRITIS 69

1.7.3 Lieferkettengesetzgebung und CSRD 73

2 Kommentierung zur BAIT-Fassung vom 16.08.2021 77

2.1 Teil I Vorbemerkung und BAIT-Gliederung 77

2.2 BAIT II.1. IT-Strategie 81

2.2.1 Einführung in das Kapitel IT-Strategie 81

2.2.2 Ziele und Maßnahmen der IT-Strategie (Tz. II.1.1. BAIT) 82

2.2.3	Mindestinhalte der IT-Strategie (Tz. II.1.2. BAIT)	84
2.2.4	Zur Bedeutung der IT-Strategie	91
2.3	BAIT II.2. IT-Governance	93
2.3.1	Einführung in das Kapitel IT-Governance	93
2.3.2	Anforderungen an die IT-Governance in BAIT-Kapitel 2	95
2.4	BAIT II.3. Informationsrisikomanagement	98
2.4.1	Einführung in das Kapitel Informationsrisikomanagement	98
2.4.2	Grundlegende Anforderungen an das Informationsrisikomanagement (Tz. II.3.1. BAIT)	98
2.4.3	Governance zum Informationsrisikomanagement (Tz. II.3.2. BAIT)	100
2.4.4	Bestandteile des Informationsverbundes (Tz. II.3.3. BAIT)	101
2.4.5	Schutzbedarfsanalyse (Tz. II.3.4. BAIT)	103
2.4.6	Zuständigkeit für die Überprüfung der Schutzbedarfsfeststellung (Tz. II.3.5. BAIT)	103
2.4.7	Sollmaßnahmen (Tz. II.3.6. BAIT)	104
2.4.8	Risikoanalyse und Soll-Ist-Vergleich (Tz. II.3.7. BAIT)	105
2.4.9	Sonstige risikoreduzierende Maßnahmen (Tz. II.3.8. BAIT)	106
2.4.10	Integration in den OpRisk-Managementprozess (Tz. II.3.9. BAIT)	106
2.4.11	Bedrohungs- und Schwachstellenanalyse (Tz. II.3.10. BAIT)	107
2.4.12	Interne Berichtspflichten (Tz. II.3.11. BAIT)	108
2.5	BAIT II.4. Informationssicherheitsmanagement	109
2.5.1	Aufgaben des Informationssicherheitsmanagements (Tz. II.4.1. BAIT)	110
2.5.2	Informationssicherheitsleitlinie (Tz. II.4.2. BAIT)	111
2.5.3	Informationssicherheitsrichtlinien und -prozesse (Tz. II.4.3. BAIT)	113
2.5.4	Funktion des Informationssicherheitsbeauftragten (Tz. II.4.4. BAIT)	113
2.5.5	Unabhängigkeit des Informationssicherheitsbeauftragten (Tz. II.4.5. BAIT)	115
2.5.6	Beschränkte Auslagerungsmöglichkeit (Tz. II.4.6. BAIT)	117
2.5.7	Analysen nach Informationssicherheitsvorfällen (Tz. II.4.7. BAIT)	120
2.5.8	Richtlinie zum Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit (Tz. II.4.8. BAIT)	122
2.5.9	Schulungs- und Sensibilisierungsprogramm (Tz. II.4.9. BAIT)	123
2.5.10	Berichterstattung zur Informationssicherheit (Tz. II.4.10. BAIT)	124
2.6	BAIT II.5. Operative Informationssicherheit	125
2.6.1	Einführung in das Kapitel Operative Informationssicherheit	125
2.6.2	Aufgaben der operativen IT-Sicherheit (Tz. II.5.1. BAIT)	125
2.6.3	Operative Informationssicherheitsmaßnahmen und -prozesse (Tz. II.5.2. BAIT) ..	127
2.6.4	Gefährdungsanalyse (Tz. II.5.3. BAIT)	130
2.6.5	Identifizierung sicherheitsrelevanter Ereignisse (Tz. II.5.4. BAIT)	131
2.6.6	Reaktion auf sicherheitsrelevante Ereignisse (Tz. II.5.5. BAIT)	132
2.6.7	Überprüfung der Sicherheit der IT-Systeme (Tz. II.5.6. BAIT)	134
2.6.8	Zusammenfassung und Ausblick auf DORA	135

2.7	BAIT II.6. Identitäts- und Rechtemanagement	136
2.7.1	Einführung in das Kapitel Identitäts- und Rechtemanagement	136
2.7.2	Zielsetzung (Tz. II.6.1. BAIT)	139
2.7.3	Anforderungen an Berechtigungskonzepte, Zuordenbarkeit von Zugriffen und Vergabe von Berechtigungen (Tz. II.6.2. BAIT bis Tz. II.6.4. BAIT)	140
2.7.4	Anforderungen an die Rezertifizierung von Berechtigungen (Tz. II.6.5. BAIT und Tz. II.6.6. BAIT)	145
2.7.5	Anforderungen an privilegierte Berechtigungen (Tz. II.6.7. BAIT)	146
2.7.6	Anforderungen an technisch-organisatorische Maßnahmen (Tz. II.6.8. BAIT)	148
2.7.7	Zusammenfassendes Fazit und Ausblick zu DORA	148
2.8	BAIT II.7. IT-Projekte und Anwendungsentwicklung	153
2.8.1	Einführung in das Kapitel IT-Projekte und Anwendungsentwicklung	153
2.8.2	Zielsetzung der Regelungen zu IT-Projekten und Anwendungsentwicklung (Tz. II.7.1. BAIT)	155
2.8.3	Regelungen zu IT-Projekten (Tz. II.7.2. BAIT bis Tz. II.7.5. BAIT)	156
2.8.4	Regelungen zur Anwendungsentwicklung (Tz. II.7.6. BAIT bis Tz. II.7.12. BAIT) ...	159
2.8.5	Regelungen zur individuellen Datenverarbeitung (Tz. II.7.13. BAIT und Tz. II.7.14. BAIT)	166
2.8.6	Zusammenfassendes Fazit und Ausblick zu DORA	169
2.9	BAIT II.8. IT-Betrieb	170
2.9.1	Einführung in das Kapitel IT-Betrieb	170
2.9.2	Allgemeine Vorgaben zum IT-Betrieb (Tz. II.8.1. BAIT)	172
2.9.3	Angaben zu Komponenten der IT-Systeme (Tz. II.8.2. BAIT)	173
2.9.4	Steuerung und Aktualisierung von IT-Systemen (Tz. II.8.3. BAIT)	174
2.9.5	Änderung von IT-Systemen (Tz. II.8.4. BAIT und Tz. II.8.5. BAIT)	176
2.9.6	Umgang mit ungeplanten Abweichungen vom Regelbetrieb (Tz. II.8.6. BAIT)	178
2.9.7	Verfahren zur Datensicherung und Datensicherungskonzepte (Tz. II.8.7. BAIT) ..	180
2.9.8	Leistungs- und Kapazitätsbedarf (Tz. II.8.8. BAIT)	181
2.9.9	Zusammenfassendes Fazit und Ausblick zu DORA	182
2.10	BAIT II.9. Auslagerungen/IT-Fremdbezug	185
2.10.1	Einführung in das Kapitel Auslagerungen und sonstiger Fremdbezug von IT- Dienstleistungen	185
2.10.2	Auslagerungen vs. sonstiger Fremdbezug von IT-Dienstleistungen (Tz. II.9.1. BAIT)	195
2.10.3	Risikobewertungen für sonstigen IT-Fremdbezug (Tz. II.9.2. BAIT)	198
2.10.4	Steuerung und Überwachung des sonstigen IT-Fremdbezugs (Tz. II.9.3. BAIT) ...	199
2.10.5	Verbindung der Risikobewertung mit Vertragsgestaltung und OpRisk- Management (Tz. II.9.4. BAIT)	201
2.10.6	Überprüfung der Risikobewertungen (Tz. II.9.5. BAIT)	202

2.11	BAIT II.10. IT-Notfallmanagement	203
2.11.1	Einführung in das Kapitel IT-Notfallmanagement	203
2.11.2	Ziele zum Notfallmanagement (Tz. II.10.1. BAIT)	207
2.11.3	Ziele und Rahmenbedingungen (Tz. II.10.2. BAIT)	212
2.11.4	IT-Notfallpläne (Tz. II.10.3. BAIT)	213
2.11.5	IT-Notfalltests (Tz. II.10.4. BAIT)	214
2.11.6	Notfallplanung für Rechenzentren (Tz. II.10.5. BAIT)	216
2.11.7	Fortentwicklung der Anforderungen und der Prüfungspraxis zur Notfallplanung .	217
2.12	BAIT II.11. Kundenbeziehungen mit Zahlungsdienstnutzern	219
2.13	BAIT II.12. Kritische Infrastrukturen	228
2.13.1	Einführung in das Kapitel Kritische Infrastrukturen	228
2.13.2	Einzelanforderungen in Kapitel 12 (Tz. II.12.1. bis Tz. II.12.5. BAIT)	231
3	Kommentierung zu DORA	237
3.1	DORA-Rechtstexte und Auslegungen im Überblick	237
3.1.1	DORA-Verordnung, DORA-Richtlinie und FinmadiG	237
3.1.2	Delegierte Rechtsakte zu DORA	243
3.1.3	Auslegungen der Aufsicht zu DORA	249
3.1.4	Vorgaben in Kapitel I DORA-VO zum Anwendungskreis und zur Proportionalität .	252
3.2	IKT-Risikomanagement	254
3.2.1	Vorgaben in Kapitel II DORA-VO und Delegierte Verordnung 2024/1774	254
3.2.2	Vorgaben zu Leitungsorgan, Governance und Schulungen	258
3.2.3	IKT-Risikomanagementrahmen und dessen Überprüfung sowie DOR-Strategie ..	263
3.2.4	Geschäftskontinuitätsplanung	273
3.2.5	Vereinfachter IKT-Risikomanagementrahmen	277
3.3	Incident Management und Incident Reporting	281
3.3.1	Anforderungen gemäß DORA-Verordnung und Relevanz von schwerwiegenden Vorfällen	281
3.3.2	Vorgaben in den Delegierten Rechtsakten	285
3.3.3	Meldeprozess an die BaFin	292
3.4	Testen der digitalen operationalen Resilienz	294
3.5	Management des IKT-Drittparteienrisikos	302
3.5.1	Anforderungen gemäß DORA-Verordnung im Überblick	302
3.5.2	Anforderungen gemäß DelVO 2024/1773 zur Leitlinie zur Nutzung von IKT- Dienstleistungen von Dritten	309
3.5.3	Anforderungen an das Informationsregister	312
3.6	Überwachung kritischer IKT-Drittdienstleister	319
3.6.1	Vorgaben gemäß DORA-VO	319
3.6.2	Delegierte Rechtsakte zu kritischen IKT-Drittdienstleistern	322
3.7	Gesamtbewertung des DORA-Regelwerks	326

- 4 Weitere Entwicklungen 331**
- 4.1 Finanzaufsichtliche Entwicklungen im engeren Sinne 331
 - 4.1.1 Weiterentwicklung im Fachgremium IT und auf EU-Ebene 331
 - 4.1.2 Vorgaben an Cloud-Computing-Provider 335
 - 4.1.3 Threat-led-Penetration Test/TIBER-DE 338
- 4.2 Weitere wesentliche rechtliche Entwicklungen mit IT-Bezug 339
 - 4.2.1 Fintechs und Digital Markets Act 339
 - 4.2.2 KI und AI Act 342

- 5 Schlusswort 345**

- Rechtstexte 349
- Literatur 353
- Stichwortverzeichnis 369
- Autorenteam 377