

# **NEUE BAIT – Neuerungen aufsichtskonform umsetzen**

**Erhebliche Änderungen in den Prozessen mit  
IT-Bezug erkennen und BAIT-konform anpassen**

Zitiervorschlag:

*Autor*, NEUE BAIT – Neuerungen aufsichtskonform umsetzen, 2022,  
RdNr. XX.

Hinweis: Zur besseren Lesbarkeit und Unterstützung des Leseflusses wurde im nachfolgenden Buch auf die Verwendung des generischen Maskulinums zurückgegriffen. Selbstverständlich schließen jedoch alle Formulierungen und Personenbezeichnungen alle Geschlechter gleichermaßen ein.

ISBN: 978-3-95725-988-2  
© 2022 Finanz Colloquium Heidelberg GmbH  
Im Bosseldorn 30, 69126 Heidelberg  
www.FCH-Gruppe.de  
info@FCH-Gruppe.de  
Satz: Finanz Colloquium Heidelberg GmbH  
Druck: VDS-VERLAGSDRUCKEREI SCHMIDT,  
Neustadt an der Aisch

# **NEUE BAIT – Neuerungen aufsichtskonform umsetzen**

**Erhebliche Änderungen in den Prozessen mit  
IT-Bezug erkennen und BAIT-konform anpassen**

**Thomas Arnsberg**

Vorstand  
movisco AG

**Joachim Astel**

CRO  
noris network AG

**Stefan Bachinger**

Vorstand  
movisco AG

**Dustin Dehez**

Geschäftsführung  
secori advisors GmbH

**Alfred Glocker**

Informationssicherheitsbeauftragter  
Infrastruktur Zentrale Dienstleistungen  
SÜDWESTBANK - BAWAG AG Niederlassung Deutschland

**Nora Haberkorn**

Berater Information Security  
ADVISORI FTC GmbH

**Kirsten Klosin**  
Vorstand  
EFDIS AG Bankensoftware

**Uwe Naujoks**  
Partner, Geschäftsbereichsleiter Risikomanagement  
WG-DATA GmbH

**Michael Pöhlsen**  
Geschäftsführer  
Vasgard GmbH

**Louis Renner**  
Berater Information Security  
ADVISORI FTC GmbH

**Sarah Richter**  
Bereichsleiterin Information Security  
ADVISORI FTC GmbH

**Sebastian Troch**  
Managing Director  
secori advisors GmbH

**Christian Wust**  
Vorstand  
EFDIS AG Bankensoftware

## Inhaltsübersicht

<b>A. Die neuen »Bankaufsichtlichen Anforderungen« an die IT</b> <i>(Haberhorn/Renner/Richter)</i>	<b>1</b>
<b>B. Umsetzung der (neuen) BAIT zu IT-Compliance und Cyber Threat Intelligence</b> <i>(Pöhlson)</i>	<b>91</b>
<b>C. BAIT-Implementierung bei einem 3rd-Party- Dienstleister – Erfahrungen und Lessons Learned</b> <i>(Klosin/Wust)</i>	<b>113</b>
<b>D. Anwendungsentwicklung und IT-Projektmanagement nach der BAIT-Novelle 2021</b> <i>(Arnsberg/Bachinger)</i>	<b>133</b>
<b>E. BAIT/MaRisk-IT aus Sicht des Informations- sicherheitsbeauftragten</b> <i>(Glocker)</i>	<b>157</b>
<b>F. Die neue Rolle der Informationssicherheit im Modell der 3LoD</b> <i>(Debez/Troch)</i>	<b>219</b>
<b>G. Als IT-Dienstleister in der Regulatorik Benchmarks setzen</b> <i>(Astel)</i>	<b>243</b>
<b>H. Business Continuity Management (BCM) – aufsichts- konform umsetzen</b> <i>(Naujoks)</i>	<b>253</b>
<b>Anhang</b>	<b>273</b>



## Inhaltsverzeichnis

<b>A. Die neuen »Bankaufsichtlichen Anforderungen« an die IT</b>	<b>1</b>
I.    Historie und Einleitung	3
II.   Vorbemerkung	7
III.  IT-Strategie	10
1.  Leitaussagen zur Entwicklung der IT-Aufbau- und Ablauforganisation sowie dem Einsatz von externen Dienstleistungen	11
2.  Festlegung zur Umsetzung gängiger Standards in der IT	13
3.  Festlegung der Bedeutung der Informations- sicherheit sowie grundlegender Verantwortlichkeiten in einem Institut	14
4.  Anforderungen an die Weiterentwicklung der IT-Infrastruktur	16
5.  Rolle des Notfallmanagements	17
6.  Umgang mit selbstbetriebenen IT-Systemen und individueller Datenverarbeitung (IDV) in den Fachbereichen	17
7.  Fazit	19
IV.  IT-Governance	20
1.  Standards für die IT-Governance	20
a)    ITIL 4	21
b)    COBIT 2019	21
c)    Vorteile der Anwendung von Standards für IT-Governance	21
2.  IT-Aufbau- und Ablauforganisation (IT-Organisation)	22
3.  Informationsrisikomanagement (IRM)	23
4.  Informationssicherheitsmanagement (ISM)	24
5.  Angemessene Personalausstattung (quantitativ und qualitativ)	25
a)    Umfang und Qualität der technisch- organisatorischen Ausstattung	26

b)	Verantwortlichkeiten und Rollen für die Pflege der Dokumentation der IT-Governance	27
6.	Fazit	27
V.	Informationsrisikomanagement (IRM)	28
1.	Rolle eines IRM in Instituten	28
2.	Der Informationsverbund	30
3.	Strategien zur Behandlung von Informationsrisiken	31
4.	Änderungen zur Vorversion	33
5.	Fazit	35
VI.	Informationssicherheitsmanagement (ISM)	35
1.	Informationssicherheit im Allgemeinen	35
2.	Informationssicherheitsbeauftragter (ISB)	38
3.	Ausgestaltung der Dokumentenhierarchie	39
4.	Identifikation und Behandlung von Sicherheitsvorfällen	42
5.	Regelmäßige Überprüfung und Testen von Maßnahmen der Informationssicherheit	43
6.	Schulungen und Sensibilisierungsmaßnahmen von Mitarbeitern des Instituts	44
7.	Fazit	45
VII.	Operative Informationssicherheit	45
1.	Konkrete Anforderungen an die operative Informationssicherheit	46
2.	Security Incident and Event Management (SIEM)	47
3.	Security Operation Center (SOC)	48
4.	Gründe für die Formalisierung des Kapitels »Operative Informationssicherheit«	49
a)	Stellung des ISB	49
b)	Klare Verantwortlichkeiten	50
c)	Regelmäßige Überprüfung von IT-Systemen	51
d)	Proaktive Identifikation von Gefährdungen	51
5.	Fazit	52
VIII.	Identitäts- und Rechtemanagement	53

1.	Identitäts- und Rechtemanagement im Allgemeinen	53
2.	Änderungen durch die neue Novelle	54
3.	Anwendung	55
4.	Fazit	56
IX.	IT-Projekte und Anwendungsentwicklung	57
1.	IT-Projekte und Anwendungsentwicklung im Allgemeinen	57
2.	Auswirkungsanalyse	58
3.	Anforderungen an den Umgang mit Projektrisiken	58
4.	Wichtige Parameter für die Projektdurchführung und Anwendungsentwicklung	59
5.	IT-Service Management (ITSM) und gängige Rahmenwerke	61
6.	Fazit	61
X.	IT-Betrieb	62
1.	Dokumentation der Bestandssysteme und IT-Komponenten	62
2.	IT-Lebenszyklus-Management	63
a)	Wartung als essenzieller Bestandteil bei der Sicherstellung von IT-Systemen	63
b)	Änderungen und Außerbetriebnahme von IT-Systemen	64
3.	Incident- und Problem-Management	65
4.	Datensicherungskonzept	66
5.	Änderungen zur Vorversion	67
XI.	Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen	68
1.	Durchführung von Risikoanalysen	70
2.	Anforderungen an die Vertragsgestaltung	70
3.	Kontinuierliche Überwachung von Dienstleistern	72
4.	Auslagerungsregister	72
5.	Fazit	74

XII. IT-Notfallmanagement	74
1. IT-Notfallmanagement nach Best Practice	75
2. Kernelemente eines funktionalen Notfallmanagements	76
3. Abhängigkeit zu externen Dienstleistern im Rahmen von Auslagerungen	78
4. Durchführung von regelmäßigen Tests und Übungen	78
5. Fazit	79
XIII. Management der Beziehungen mit Zahlungsdienstnutzern	79
1. Allgemeines zum Hintergrund	79
2. Aufgaben des Instituts gegenüber den Zahlungsdienstnutzern	81
a) Sensibilisierung der Nutzer gegenüber den Risiken bei Verwendung der Zahlungsdienste	81
b) Einrichtung angemessener Kommunikationskanäle für die Nutzer, die auch angemessen ausgewiesen sind	81
c) Zahlungsdienstleister sollen dem Zahlungsdienstnutzer die Möglichkeit anbieten, einzelne Zahlungsfunktionalitäten zu deaktivieren	82
d) Der Zahlungsdienstnutzer soll die Möglichkeit haben, Betragsobergrenzen anzupassen und nach den eigenen Anforderungen zu gestalten	83
e) Zahlungsdienstleister sollen dem Zahlungsdienstnutzer die Möglichkeit anbieten, Benachrichtigungen über getätigte und fehlgeschlagene Transaktionen zu erhalten	83
3. Fazit	83
XIV. Kritische Infrastrukturen	84
1. Schwellwerte zur Klassifizierung einer kritischen Infrastruktur	86
2. Inventarisierung von Komponenten der kritischen Infrastruktur	86

3.	Hochverfügbarkeitskonzept (Sicherstellung des KRITIS-Schutzziels Versorgungssicherheit)	87
4.	Nachweis der Konformität	88
5.	Fazit	89
XV.	Zusammenfassung	89
 <b>B. Umsetzung der (neuen) BAIT zu IT-Compliance und Cyber Threat Intelligence</b>		 <b>91</b>
I.	Einleitung	93
1.	Situation	93
2.	Anforderungen aus Sicht der BAIT	93
3.	Herausforderungen im Kontext der operativen Informationssicherheit (IS)	95
a)	Informationssilos und fehlende Transparenz	95
b)	Heterogene IT-Security-Architektur	96
4.	In drei Schritten zur operativen IS	96
II.	Lösungsbausteine	99
1.	Informationsverbund	101
2.	Strukturanalyse und Schutzbedarfsfeststellung	104
3.	Operative IS in der Praxis	105
4.	Schwachstellenmanagement (VAS)	107
a)	Einführung	107
b)	Erfolgsfaktoren	107
5.	Security Information and Event Management (SIEM)	108
a)	Einführung	108
b)	SIEM Use Case	108
c)	Identifizierung von Anforderungen für das Security Monitoring	109
d)	Implementierung des SIEM-Systems	109
e)	Anbindung der Logquellen	109
f)	Implementierung und Test der SIEM Use Cases	110
g)	Vorbereitung des Regelbetriebes	110
6.	Security Operation Center (SOC)	110

7.	Security Compliance Operations Center (SCOC)	111
8.	Fazit	111
<b>C.</b>	<b>BAIT-Implementierung bei einem 3rd-Party-Dienstleister – Erfahrungen und Lessons Learned</b>	<b>113</b>
I.	Einleitung	115
II.	BAIT-Implementierung bei EFDIS	116
1.	Planung	116
2.	Methodenhandbuch	116
3.	Kooperation mit den Mandanten	117
4.	Partnerschaften	118
III.	Umsetzung	118
1.	Anforderungen	118
2.	Konzeption	119
3.	BAIT-Bereiche	119
a)	IT-Strategie	119
b)	IT-Governance	120
c)	Informationsrisiko-Management	120
d)	Informationssicherheits-Management	121
e)	Benutzerberechtigungsmanagement	121
f)	IT-Projekte und Anwendungsentwicklung	122
g)	IT-Betrieb	122
h)	Auslagerung und sonstiger Fremdbezug	123
i)	Notfallmanagement	124
4.	Ergebnistypen	124
5.	Prozessmanagement	125
6.	»Internes Kontrollsystem« (IKS)	126
7.	IDW PS 951	126
IV.	Lessons Learned	127
1.	Partnerschaftlich zum Erfolg	127
2.	Freiheitsgrade im Regelkorsett	127
3.	Praktische Relevanz des »Internen Kontrollsystems«	128

4.	Risikomanagement statt Risikoverwaltung	128
5.	BAIT-konforme Neuordnung der Verträge	129
V.	Anforderungen aus den neuen BAIT	129
1.	Operative Informationssicherheit	129
2.	Notfallmanagement	130
3.	Fazit zum Status neue BAIT	130
<b>D. Anwendungsentwicklung und IT-Projektmanagement nach der BAIT-Novelle 2021</b>		<b>133</b>
I.	Anforderungen an die Anwendungsentwicklung in Banken	137
1.	Individuelle Datenverarbeitung (IDV) in der Anwendungsentwicklung	137
2.	Prozesse zur Anwendungsentwicklung	139
3.	Anforderungserhebung und ihre Dokumentation	140
4.	Softwaretests sind notwendig	141
5.	Sicherstellung der Integrität und Qualitätssicherung	142
6.	Dokumentation der Entwicklung	144
II.	Anforderung an das Projektmanagement	145
1.	Definition eines Projekts und organisatorische Grundlagen	145
2.	Die Steuerung von Projekten	148
3.	Das Management eines Projektportfolios	151
4.	Verpflichtende Berichtserstattung an die Geschäftsleitung	154
III.	Umsetzung der BAIT ist auch eine Frage des Mindsets	155
<b>E. BAIT/MaRisk-IT aus Sicht des Informationssicherheitsbeauftragten</b>		<b>157</b>
I.	Einleitung	159
II.	IT-Strategie	159
III.	IT-Governance	164
IV.	Informationsrisikomanagement	166

V.	Informationssicherheitsmanagement	172
VI.	Operative Informationssicherheit	181
VII.	Identitäts- und Rechtemanagement	185
VIII.	IT-Projekte, Anwendungsentwicklung	191
IX.	IT-Betrieb	198
X.	Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen	204
XI.	IT-Notfallmanagement	207
XII.	Management der Beziehungen mit Zahlungsdienst- nutzern	211
XIII.	Kritische Infrastrukturen	214
<b>F.</b>	<b>Die neue Rolle der Informationssicherheit im Modell der 3LoD</b>	<b>219</b>
I.	Einleitung	221
1.	Einordnung der Informationssicherheit in das Modell der drei Verteidigungslinien	223
2.	Schnittstellen des Informationsrisikomanagements zum Management der operationellen Risiken	229
3.	Systematischer Aufbau eines Informationssicherheitsmanagements	233
4.	Ausblick: Informationssicherheitsmanagement in stürmischen Zeiten	239
II.	Literatur	240
<b>G.</b>	<b>Als IT-Dienstleister in der Regulatorik Benchmarks setzen</b>	<b>243</b>
I.	IT-Auslagerung: Voraussetzungen für die Governance	245
II.	Risk Management und Auslagerungsmanagement: Integrales Risikomanagementsystem braucht Branchenexpertise	247
III.	Business Continuity Management: IT-Grundschatz und Notfallplanung	248
IV.	Security Operation Center: Operative Informationssicherheit per Security Incident und Event Management	250

<b>H. Business Continuity Management (BCM) – aufsichtskonform umsetzen</b>	<b>253</b>
I. BCM – Ausweitung der regulatorischen Rahmenvorgaben	255
II. Neue Anforderungen der BAIT an Dokumentation und echte BCM-Tests	257
1. Definition der Zielsetzung zum Notfallmanagement (NFM)	258
2. Konkretisierung des NFM-Konzeptes	258
3. IT-Notfallpläne	258
4. IT-Testkonzept	258
III. Projektbericht zur Umsetzung	259
1. Programm Management	260
a) Zielsetzung	261
b) Geltungsbereich	261
c) Rollen und Verantwortlichkeiten	261
2. Analysephase	261
a) Business Impact Analyse (BIA)	262
b) Risikoanalyse (RIA)	263
3. BCM Strategie	265
a) Personalstrategie	265
b) Gebäude- und Arbeitsplatz-Strategie	266
c) IT- und ITSCM-Strategie	266
d) Dienstleisterstrategie	266
4. Exkurs ITSCM	266
5. Business Continuity-Planung	267
6. Tests und Übungen (Validierung)	268
a) Zielsetzung	268
b) Ablauf	268
7. Monitoring	269
a) Zielsetzung	269
b) Ergebnis	270
8. Awareness und Trainings	270
9. Dienstleistersteuerung (DLS)	270

## INHALTSVERZEICHNIS

---

a)	Aufgabe der DLS	270
b)	Ablauf der DLS	271
IV.	Fazit	271
<b>Anhang</b>		<b>273</b>

**A.**

**Die neuen »Bankaufsichtlichen Anforderungen«  
an die IT**



## A. Die neuen »Bankaufsichtlichen Anforderungen« an die IT

### I. Historie und Einleitung

Die »Bankaufsichtlichen Anforderungen an die IT« (BAIT) sind eine Ansammlung regulatorischer Vorgaben, die in Form eines Rundschreibens der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) veröffentlicht werden, um den Anforderungen einer globalisierten Finanzwelt gerecht zu werden. Die Globalisierung betrifft die Finanzwelt durch weltweite Geldtransfers, digitale Bezahlungsmöglichkeiten (Zahlungsdienste) und Online-Geldanlagen. Auch durch den Paradigmenwechsel vom klassischen Kundengeschäft zu einem umfangreicheren Angebot digitaler Dienstleistungen hat sich die Risikoexposition von Instituten verändert. Der Fokus der Institute liegt auf dem Kerngeschäft, daher werden Optionen wie Auslagerungen, Nearshoring und Offshoring häufig präferiert. Hierbei müssen die Gefahren durch eine eventuelle Verminderung der Kontrolle auf die Ausführung der Leistungen berücksichtigt werden. Dementsprechend überwacht die BaFin neben der Liquidität und dem Kapital auch die Informationstechnologie (IT) in der Finanzindustrie. Ein übergreifendes Risikomanagement und die damit verbundene Absicherung der IT ist essenziell, um erfolgreich am Markt zu bestehen, wettbewerbsfähig zu bleiben und teilweise die eigene Existenz zu sichern. Ein Wettbewerbsvorteil kann sich für das Institut ergeben, in dem es ein besonderes Augenmerk auf die Einhaltung regulatorischer Anforderungen legt und diese für sich besonders streng auslegt. Das können u. a. erweiterte Sicherheitsmaßnahmen zum Schutz der Kundendaten sein. Dem Kunden wird ein gutes Gefühl gegeben und der Vertrauensvorschuss bei Vertragsabschluss im Umgang mit seinen Daten bestmöglich sichergestellt.

Die BAIT-Veröffentlichung der BaFin aus dem Jahr 2017 dient dazu, den Instituten einen Leitfaden bei der IT-Governance hinsichtlich der Ausgestaltung der IT-Systeme und den Prozessen zur Verfügung zu stellen. Die gesetzliche Basis bilden die Anforderungen aus dem Kreditwesengesetz (KWG) des § 25a Abs. 1 Satz 3 Nr. 4 und 5<sup>1</sup>. Die BAIT betreffen Institute im Sinne des KWG, d. h. Kreditinstitute und Finanzdienstleistungsinstitute, und hat das Ziel, einen flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausstattung der

<sup>1</sup> Vgl. *BaFin, BAIT*: BaFin veröffentlicht Anforderungen an die IT von Banken, 2017, abrufbar über [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung\\_171106\\_BAIT.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171106_BAIT.html)

Institute vorzugeben. In der Novelle wird das Verständnis der BaFin einer angemessenen technisch-organisatorischen Ausstattung von IT-Systemen und Prozessen definiert, wobei im Besonderen die Anforderungen an Informationssicherheit sowie das Notfallmanagement Berücksichtigung finden.

- 3 Die BAIT legen die Anforderungen der MaRisk zugrunde und konkretisieren diese für die IT. Die MaRisk und BAIT unterliegen einem kontinuierlichen Überarbeitungsprozess und werden somit regelmäßig überarbeitet. Am 14.09.2018 wurde das Kapitel *Kritische Infrastrukturen* veröffentlicht<sup>2</sup>. Hierunter fallen Anforderungen für Institute, die gemäß BSI-Kritisverordnung (BSI-KritisV) Betreiber kritischer Infrastrukturen sind. Zwei Jahre später, am 26.10.2020, wurde ein öffentliches Konsultationsverfahren für die Entwürfe der BAIT und MaRisk eingeführt<sup>3</sup>. In dem Konsultationsverfahren wurden eingegangene Stellungnahmen zum Entwurf des BAIT-Rundschreibens geprüft, konsolidiert und dem Fachgremium IT der BaFin vorgestellt. Die Überarbeitung war abgeschlossen und die Novellierungen wurden am 16.08.2021 veröffentlicht.

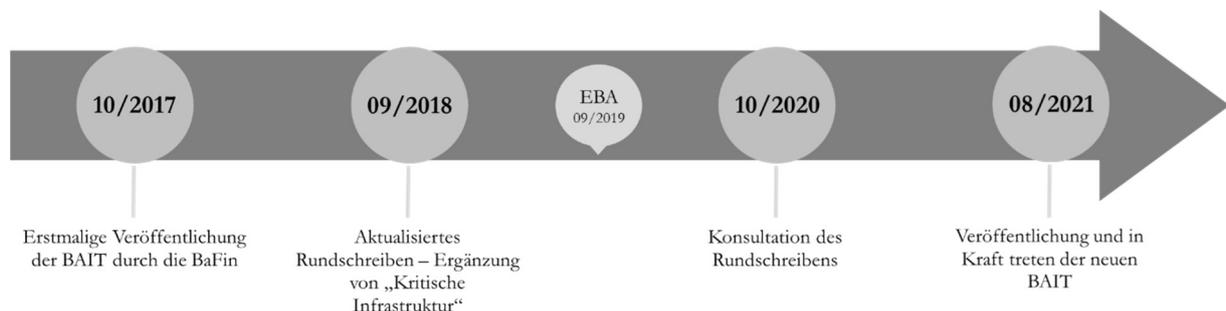


Abbildung A.-1: Zeitstrahl der BAIT

- 4 Da die Grundlage der Inhalte der BAIT die MaRisk-Novelle ist, wurde diese gleichzeitig angepasst und veröffentlicht. Die Umsetzung der MaRisk ist essenziell, bspw. AT 4.2 in Bezug auf die IT-Strategie. Der Hintergrund der Überarbeitung war u. a. die Veröffentlichung der Leitlinien der Bankenaufsichtsbehörde European Banking Authority (EBA) im November 2019. EBA/GL/2019/04 zum Management von Informations- und Kommunikationstechnik sowie Sicherheitsrisiken wurde erneuert und konkretisiert. In dieser

2 Vgl. *BaFin*, Kritische Infrastrukturen: BaFin ergänzt BAIT um KRITIS-Modul, 2018, abrufbar über [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung\\_180914\\_Ueberarbeitung\\_BAIT.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung_180914_Ueberarbeitung_BAIT.html)

3 Vgl. *BaFin*, Konsultation 14/2020 – Mindestanforderungen an das Risikomanagement, 2020, abrufbar über [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Konsultation/2020/kon\\_14\\_20\\_Konsultation\\_MaRisk.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Konsultation/2020/kon_14_20_Konsultation_MaRisk.html)

Leitlinie wurde ein Rahmen für die nationalen Aufsichtsbehörden wie die BaFin beschrieben. Hieraus erfolgte eine Überprüfung der BAIT durch die BaFin in Zusammenarbeit mit dem Fachgremium IT sowie Fachverbänden und Institutionen<sup>4</sup>.

In der BAIT-Novellierung von 2021 konkretisiert die BaFin ihre Erwartungen an die IT und die Informationssicherheit von Instituten. 5

Auf Basis der alten Darstellung aller BAIT-Module und deren Zuordnung zu den verschiedenen Organisationsebenen eines Instituts wurde eine Aktualisierung erarbeitet. Die folgenden 12 Module werden in der Abbildung A.-2 unterteilt in die Ebenen Governance (Leitung), Management (Verwaltung) und Operativ (Umsetzung): 6

- IT-Strategie
- IT-Governance
- Informationsrisikomanagement (IRM)
- Informationssicherheitsmanagement (ISM)
- Operative Informationssicherheit
- Identitäts- und Rechtemanagement
- IT-Projekte und Anwendungsentwicklung
- IT-Betrieb
- Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
- Notfallmanagement
- Management der Beziehungen mit Zahlungsdienstleistern
- Kritische Infrastruktur (Kritis)

---

4 Vgl. BaFin, BaFin novelliert ihre BAIT, 2021, abrufbar über [https://www.bafin.de/Shared-Docs/Veroeffentlichungen/DE/Fachartikel/2021/fa\\_bj\\_2108\\_BAIT.html](https://www.bafin.de/Shared-Docs/Veroeffentlichungen/DE/Fachartikel/2021/fa_bj_2108_BAIT.html)

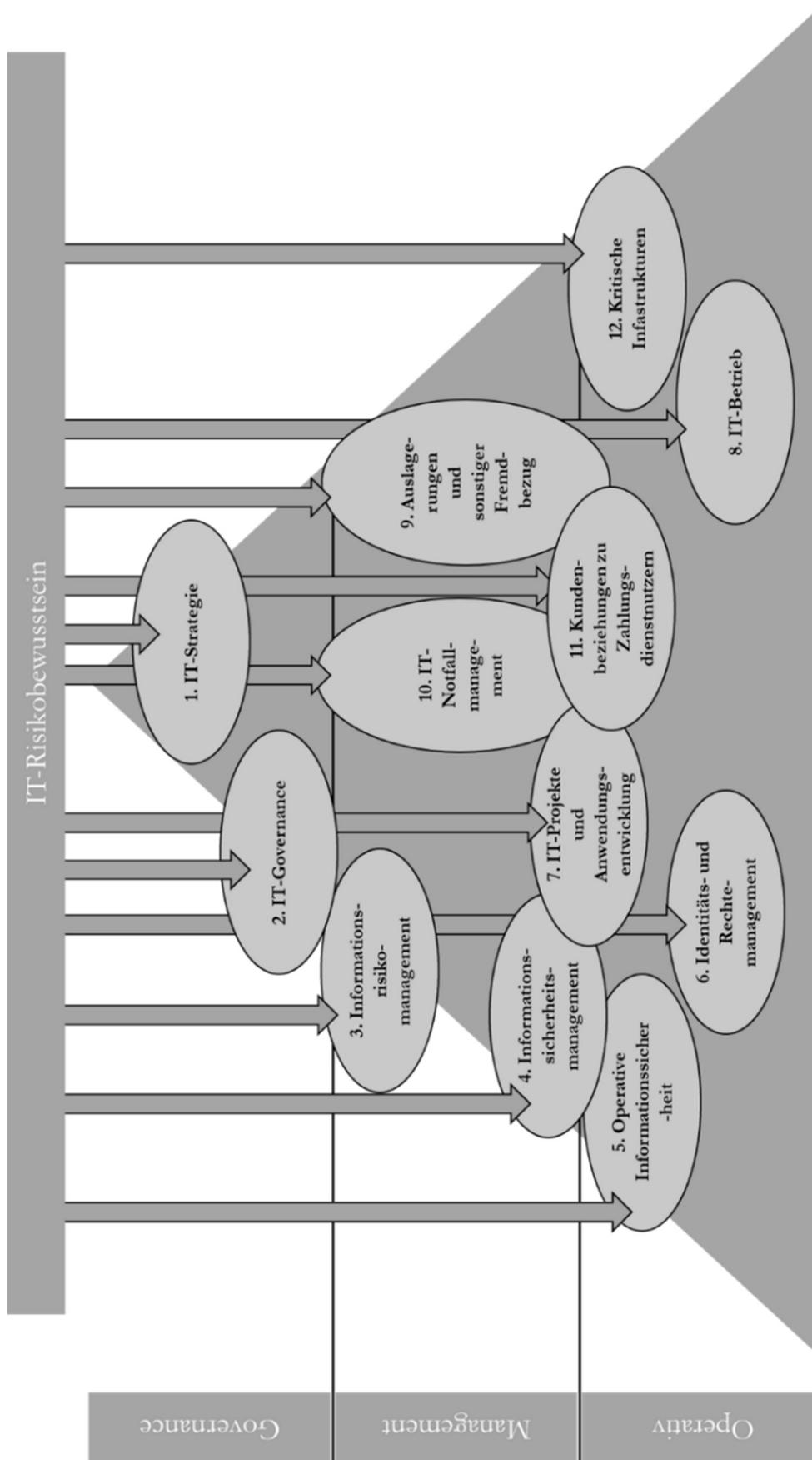


Abbildung A.-2: Die Struktur der BAIT Novellierung mit Unterteilung der BAIT-Module zwischen Governance, Management und Operativ

In der Novellierung gibt es Erweiterungen und Anpassungen bezüglich der Kapitel, die in der Novellierung nun als Module benannt sind. Durch die ergänzten Module IT-Notfallmanagement und Operative Informationssicherheit, die im Wesentlichen Aspekte zum Notfallmanagement sowie der Informationssicherheit und technische Verfahren umfassen, nehmen insbesondere Themen wie Netzwerksegmentierung und Schwachstellenmanagement an Bedeutung zu. In einigen Instituten besteht noch Handlungsbedarf bei der Härtung von IT-Systemen und der Verschlüsselung von Daten, so dass diese Themen wesentliche Aufwandstreiber darstellen<sup>5</sup>. 7

In diesem Buchkapitel wird auf die jeweiligen Änderungen je Modul eingegangen und mit Praxisbeispielen erläutert. Da sich der Inhalt der folgenden Kapitel dieses Buchs auf die aktuelle Fassung der BAIT (Rundschreiben 08/2021) bezieht, wird dieses Dokument zu Grunde gelegt und nicht weiter zitiert. 8

Dieses Buchkapitel dient der Herleitung eines tieferen Verständnisses der BAIT durch die Analyse der 12 Module, der Vorbemerkung sowie durch das Aufzeigen von Handlungsnotwendigkeiten und Praxisbeispielen je Modul. 9

## II. Vorbemerkung

Die BaFin hat die BAIT am 16.08.2021 zusammen mit der novellierten MaRisk veröffentlicht. Neben der Vorbemerkung besteht die BAIT aus 12 Modulen, die in den folgenden Kapiteln, auch unter Berücksichtigung der Anpassungen der MaRisk, näher beleuchtet werden. 10

Die Vorbemerkung der BAIT beschreibt den Zusammenhang zum KWG und der MaRisk. Hierbei wird auch die Bedeutung der IT in der Finanzwirtschaft herausgestellt, u. a. durch die Anwendungsempfehlung von Standards, wie dem BSI IT-Grundschutz und der ISO/IEC-27000-Reihe. Die erwähnten Standards entsprechen den Best Practices der Informationssicherheit und dienen der Absicherung von Informationswerten, ungeachtet ob in analoger (Papier, Akten etc.) oder digitaler Form. Diese Standards geben den Instituten bei Anwendung eine umfangreiche Methodensammlung für die Absicherung der verarbeiteten Informationen. 11

---

5 Vgl. *Ralf Kluge*, 2021, abrufbar über [https://www.fch-gruppe.de/Beitrag/18273/neue-bait-anforderungen-und-erste-praxisimplikationen#\\_ftn5](https://www.fch-gruppe.de/Beitrag/18273/neue-bait-anforderungen-und-erste-praxisimplikationen#_ftn5)

- 12 In der MaRisk ist hervorzuheben, dass der Anwenderkreis (nachfolgend AT 2.1) mehr in den Fokus rückt und direkt in Ziffer 1 erwähnt wird. Weiterhin wurde der Fachterminus »IT-Risikomanagement« gestrichen und durch die Begrifflichkeiten »Informationssicherheitsmanagement« und »Informationsrisikomanagement« ersetzt<sup>6</sup>. Der Stellenwert von Informationen nimmt nun eine sehr exponierte Stellung ein, was unter anderem durch die Streichung der zuvor IT-zentralen Begrifflichkeiten unterstrichen wird.
- 13 Wie bereits in der Version von 2017 und in der MaRisk wird auf die doppelte Proportionalität hingewiesen. »Die prinzipienorientierten Anforderungen dieses Rundschreibens ermöglichen die Umsetzung des Prinzips der doppelten Proportionalität (vgl. insbesondere AT 1 Tz. 3, 5 und 7 sowie AT 2.1 Tz. 2 MaRisk).«<sup>7</sup> Unter der doppelten Proportionalität versteht man, dass die Steuerungsinstrumente eines Instituts und die Intensität der BaFin zu den Risiken des Instituts passen. Jedoch gibt es keinen expliziten Verweis auf die Proportionalität hinsichtlich der Ausgestaltung des IT-Betriebs (Tz. 8) des jeweiligen Instituts. Die Anforderungen an ein kleineres Institut mit wenig komplexen Geschäftsprozessen und einem weniger umfangreichen Geschäftsmodell können durch die Anwendung der Proportionalität weniger aufwändig in der Umsetzung der BAIT sein, wie bei einem großen Institut mit sehr komplexen Geschäftsprozessen und einem sehr umfangreichen Geschäftsmodell.
- 14 Ein Institut hat die Anforderungen der BAIT in einem angemessenen Rahmen umzusetzen. Das übliche 3-Linien-Modell (ehemals: 3-Lines-of-Defence) bietet sich in diesem Kontext an, um eine Organisation zu erschaffen, die potenziellen Interessenskonflikten durch eine angemessene aufbauorganisatorische Struktur gerecht zu werden. Zur Vollständigkeit wurden die einzelnen »Linien« nochmals entsprechend graphisch aufbereitet:

---

6 Vgl. *BaFin*, Mindestanforderungen an das Risikomanagement – MaRisk Erläuterungen zum Rundschreiben 10/2021 (BA), abrufbar über [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs\\_1021\\_MaRisk\\_BA.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html)

7 *BaFin*, Rundschreiben 10/2017 (BA) in der Fassung vom XX.XX.2020 (Konsultationsentwurf), 2020, abrufbar über: [https://www.bafin.de/SharedDocs/Downloads/DE/Konsultation/2020/dl\\_kon\\_13\\_20\\_BAIT.pdf?\\_\\_blob=publicationFile&v=4](https://www.bafin.de/SharedDocs/Downloads/DE/Konsultation/2020/dl_kon_13_20_BAIT.pdf?__blob=publicationFile&v=4)

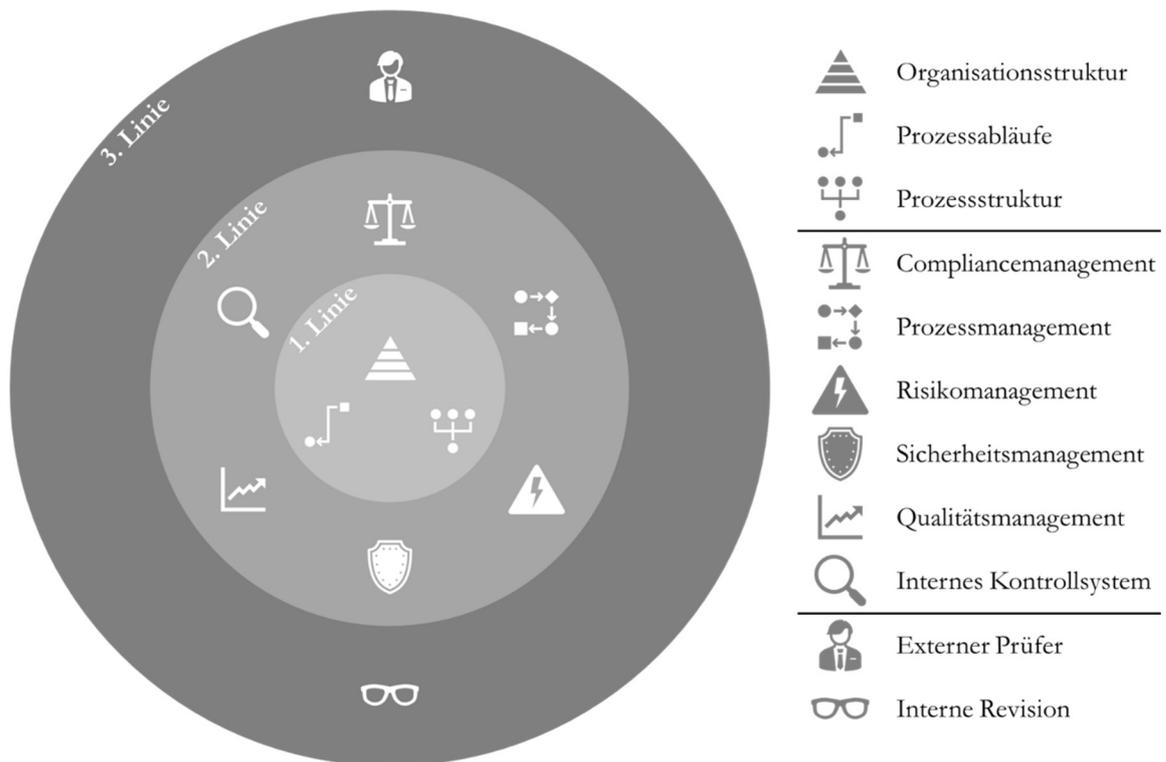


Abbildung A.-3: Das 3-Linien-Modell<sup>8</sup> als Grundlage für die Errichtung einer angemessenen Organisation innerhalb eines Instituts unter Berücksichtigung von Anforderungen zur Vermeidung von Interessenskonflikten

Die Trennung einzelner Funktionen durch das 3-Linien-Modell ermöglicht die pragmatische Umsetzung der BAIT anhand klar getrennter Verantwortlichkeiten für die einzelnen Module. In den nächsten Kapiteln werden die Anforderungen der einzelnen Module näher betrachtet. 15

Die Anforderungen der BAIT decken verschiedene wichtige Teilbereiche einer funktionierenden IT ab und legen Anforderungen fest, um im Anwendungsbereich der bankenaufsichtlichen Vorgaben ein einheitliches Niveau einer IT-Organisation und der damit verbundenen Prozesse und Kontrollen festzulegen. Die einzelnen Unterkapitel können losgelöst gelesen werden, um einen schnellen Überblick je Modul zu erhalten, oder als Ganzes gelesen werden, um ein umfangreiches Bild zu den bankenaufsichtlichen Anforderungen zu erhalten. Im nachfolgenden Kapitel wird das Modul IT-Strategie betrachtet. 16

8 Darstellung wurde auf Basis dieser Darstellung erstellt: <https://us.boc-group.com/grc-three-lines-of-defence>

### III. IT-Strategie

- 17 In der BAIT befasst sich das Modul IT-Strategie mit der Definition grundlegender Anforderungen zur Ausgestaltung der IT im Kontext der Geschäfts- bzw. Unternehmensstrategie. Die Geschäftsstrategie ist analog zu einer Unternehmensstrategie zu verstehen und dient primär dem Zweck, die zentrale Zielsetzung unter Berücksichtigung des Produktportfolios und der makroökonomischen Herausforderungen festzulegen. Die Geschäftsstrategie dient somit dem Zweck bspw. den Kunden einzigartige Finanzdienstleistungen zur Verfügung zu stellen, die die Konkurrenz nicht zu denselben Konditionen (z.B. Preise oder Servicequalität) anbietet und somit »einen Schritt voraus sind«. Die IT-Strategie baut auf der Geschäftsstrategie auf und übersetzt die Geschäftsziele für die IT, um eine Realisierung mit Unterstützung der IT bestmöglich umzusetzen.
- 18 Eine IT-Strategie dient als Leitfaden für die Ausrichtung der IT-Organisation eines Instituts, sie legt eine Vision, eine Mission sowie eine Erwartungshaltung und die notwendigen Schritte für dessen Erreichung fest. Primär dient die IT-Strategie der Sicherstellung des Unternehmenserfolgs sowie dessen Wachstum, bspw. durch die Verbesserung von IT-Services oder -Leistungen bei einer gleichzeitigen Senkung laufender Kosten. Entsprechend der zentralen Bedeutung einer IT-Strategie für das gesamte Institut muss der Erlass über den Gesamtvorstand bzw. die Geschäftsführung erfolgen. Im Rahmen des Erarbeitungsprozesses sollte sich der Umfang einer IT-Strategie an der Unternehmensgröße und -komplexität orientieren, und der Größe und Bedeutung der IT-Organisation angemessen begegnen.
- 19 Einzelne Aspekte wurden in Bezug auf die IT-Strategie konkretisiert. Die Berücksichtigung »möglicher sonstiger wichtiger Abhängigkeiten von Dritten (wie z. B. Zentralbankfunktionen, Informationsdiensten, Telekommunikationsdienstleistungen, Versorgungsleistungen [und weitere])« (Tz. 1.2 f.) spiegelt die Entwicklungen der vergangenen Jahre wider – die steigende Komplexität des Dienstleistungsportfolios im Umfeld dieser Institute, Änderungen in Bezug auf die Wahrnehmung von Angeboten durch die Kunden sowie die Veränderung der Risikoexposition in Bezug auf Lieferketten. In der Vergangenheit haben sich Fälle dieser Art in der öffentlichen Berichterstattung gehäuft – IT-Infrastrukturen und -Systeme wurde bspw. über Lieferketten kompromittiert und haben kritische Auswirkungen auf das Kerngeschäft sowie die Kunden gehabt.