NEUE BAIT – Neuerungen aufsichtskonform umsetzen

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

Finanz Colloquium Heidelberg, 2022

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

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
Informationssicherheitsbeauftrager
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

Finanz Colloquium Heidelberg, 2022

Inhaltsübersicht

Inhaltsverzeichnis

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 Bezahlmöglichkeiten (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. 1

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[1]. 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 2

1 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

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[2]. 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[3]. 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.

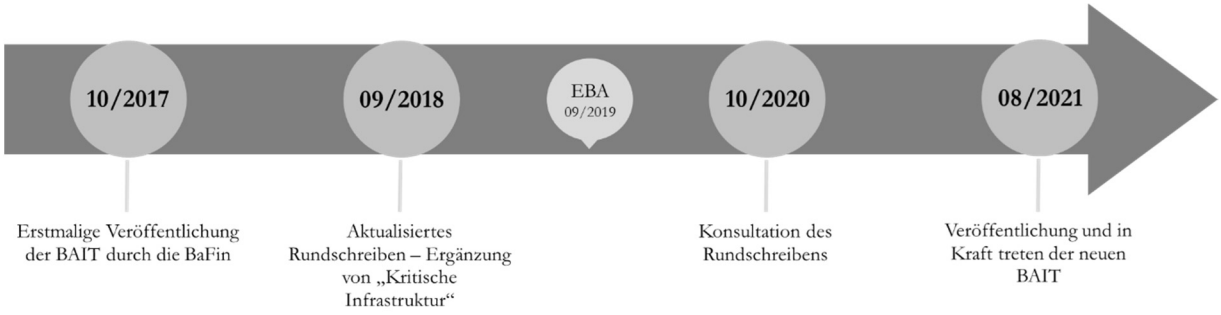

Abbildung A.-1: Zeitstrahl der BAIT

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

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

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[4].

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 Organisationebenen 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/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2021/fa_bj_2108_BAIT.html

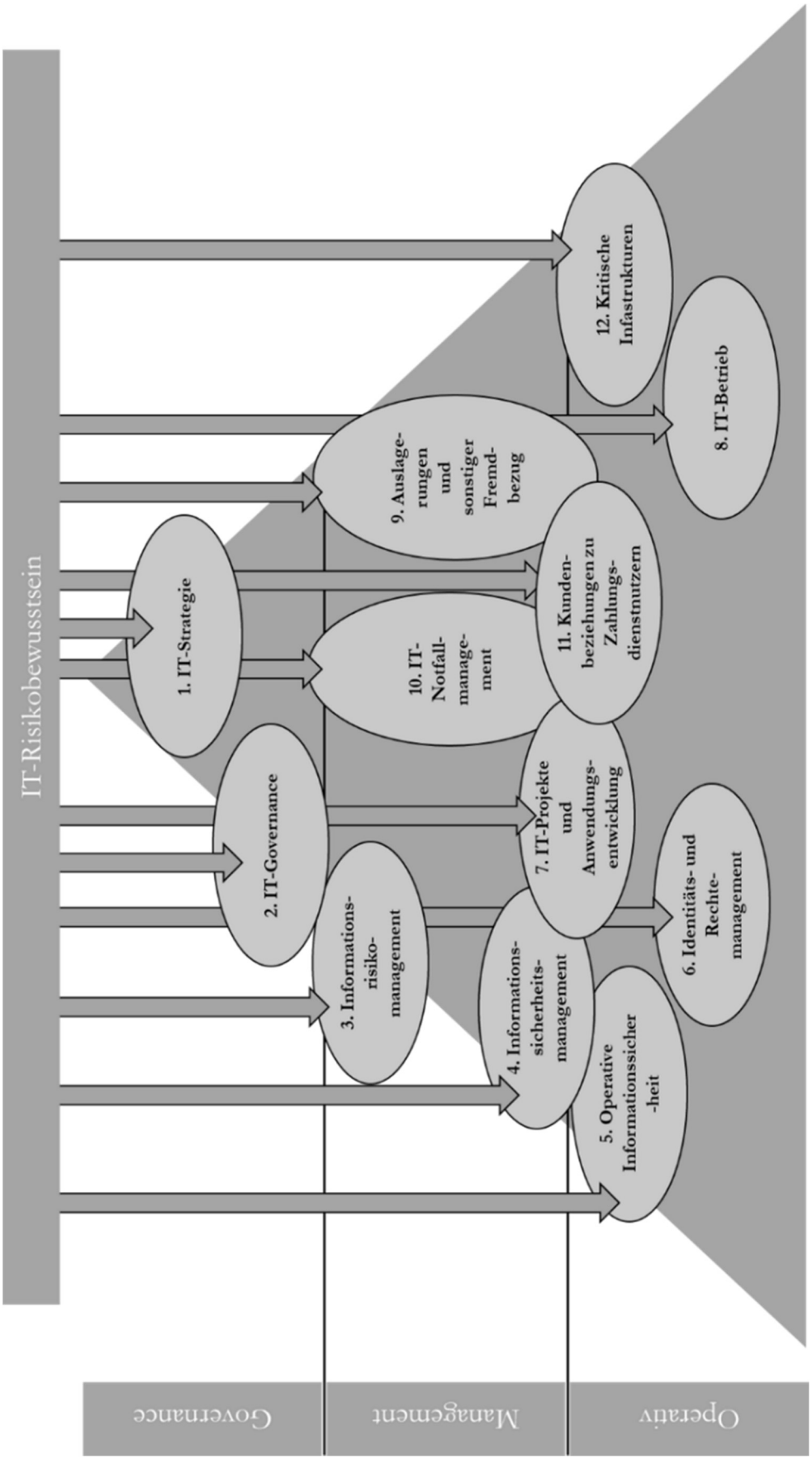

Abbildung A.-2: Die Struktur der BAIT Novellierung mit Unterteilung der BAIT-Module zwischen Governance, Management und Operativ

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[5]. 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

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[6]. 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).«[7] 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

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

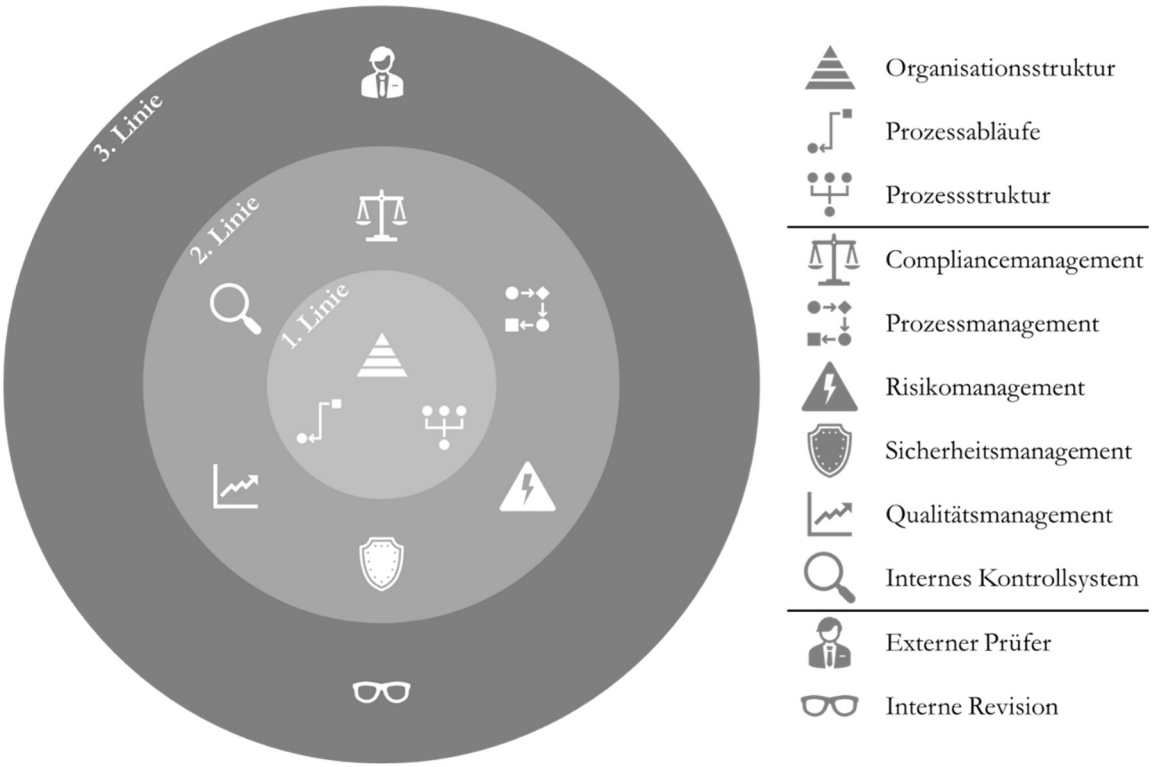

Abbildung A.-3: Das 3-Linien-Modell[8] *als Grundlage für die Errichtung einer angemessenen Organisation innerhalb eines Instituts unter Berücksichtigung von Anforderungen zur Vermeidung von Interessenskonflikten*

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 Anwendungsraum 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, Telekommunikationsdienst-leistungen, 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.