Tomislav Maksimovic
Holger Biernat

Bankaufsichtliche Anforderungen an die IT (BAIT)

Konzepte zur Implementierung der neuen Vorgaben

Springer Gabler

Bankaufsichtliche Anforderungen an die IT (BAIT)

Tomislav Maksimovic • Holger Biernat

Bankaufsichtliche Anforderungen an die IT (BAIT)

Konzepte zur Implementierung der neuen Vorgaben

Springer Gabler

Tomislav Maksimovic
Barrus Consulting GmbH
Frankfurt am Main, Deutschland

Holger Biernat
Barrus Consulting GmbH
Frankfurt am Main, Deutschland

ISBN 978-3-658-25225-0 ISBN 978-3-658-25226-7 (eBook)
https://doi.org/10.1007/978-3-658-25226-7

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Die BaFin hat im Rundschreiben 10/2017 (BA) vom 03.11.2017 [1] ihre Anforderungen an eine Umsetzung von § 25a Abs. 1 S. 3 Nr. 4 und 5 KWG [27] formuliert. Die BAIT (Bankaufsichtliche Anforderungen an die IT) konkretisieren die Anforderungen zum internen Kontrollsystem, die personelle und technisch-organisatorische Ausstattung der Bank sowie zum Notfallkonzept. Für Institute kommen die Inkraftsetzung des Rundschreibens und damit der Anforderungen nicht überraschend: Im Jahr 2017 wurde der vorgelegte Text ausführlich von den Verbänden diskutiert und erst eine Woche vor dem Rundschreiben waren die MaRisk zum ersten Mal seit 2012 [36] novelliert worden [7]. Die Regeln sind noch Ausläufer des seit 2008 herrschenden „Regulierungstsunamis", mit dem die BaFin versucht hat, auf die neuen Anforderungen nach der Finanzmarktkrise zu reagieren. Sie zeigen weitestgehend Selbstverständlichkeiten aus der gelebten Praxis der Banken-IT auf.

Die Bankenaufsicht meldet sich mit den BAIT in einer Zeit zu Wort, in der die betroffenen deutschen Institute noch unter den Verschärfungen und Problemen der vergangenen Jahre leiden: die Erträge sind kaum noch auskömmlich, die Margen niedrig, die Zinsen im Minusbereich und Geldanlage wird bestraft. FinTechs, Digitalisierung, Big Data, KI Big Data [2], KI [29] sowie Blockchain sind Schlagworte der Gegenwart, mit denen sich Banken auseinandersetzen müssen. Die aktuelle Situation wird zu Anpassungen in der IT, aber auch zu Anpassungen im Geschäftsmodell führen. Eine Vernetzung von Arbeitsprozessen wird zwischen Banken und ihren Zulieferern zunehmend existenziell. Die BAIT kommen also genau zur rechten Zeit, um hier den aufsichtlichen Rahmen zu setzen.

Das Rundschreiben hat keine Umsetzungsfrist, da die Inhalte bereits früher, z. B. aus den Anforderungen des IT-Sicherheitsgesetzes [28] oder den MaSi, dem Rundschreiben 4/2015 (BA) – Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSi) [15], im Wesentlichen ableitbar waren. Es schafft nun allerdings Transparenz, welche konkreten Anforderungen die Aufsicht an die Banken hat. Zwar geht die Aufsicht davon aus, bereits bestehende Selbstverständlichkeiten zu beschreiben, jedoch besteht im Alltag der Institute trotzdem noch Anpassungsbedarf – und sei es nur in der verbesserten Darstellung bereits vorhandener Dokumente. Viele Banken haben bereits entsprechende Unterlagen, Prozesse und Regeln eingeführt, sei es im Rahmen angestrebter Zertifizierungen oder bei der notwendigen Umsetzung von begleitenden Gesetzen über Verordnungen bis hin zu Datenschutzregeln. Bisher waren einige dieser Prozesse in Banken nützlich und sinnvoll, nunmehr sind sie zwingend vorgeschrieben.

Es handelt sich bei den BAIT um Regeln der deutschen Aufsicht, abgeleitet aus supranationalen Regelungen, Vorgaben oder Benchmarks. Die Konkretisierung stellt eine Einschränkung des Handlungs- und Ermessensspielraums der Banken dar. Da die BAIT eine Reihe von Pflichten beschreiben und damit vieles bis in die Tiefe regeln, wird sich zeigen, inwieweit die doppelte Proportionalität in der Praxis tatsächlich Anwendung finden wird. Aus Sicht der Aufsicht wird die Ausgestaltung der IT transparenter werden, insbesondere dahingehend, welche Vorkehrungen die Banken im Allgemeinen und im Speziellen getroffen haben.

IT-Probleme sind immer auch operationelle Probleme. So gibt es in Zeiten der schnellen Berichterstattung oft eine Null-Fehler-Toleranz. Selbst kleine Fehler oder Unzulänglichkeiten können eine Welle von negativer Presse und schädlicher Entwicklungen hervorrufen. Skandale und technische Probleme schädigen das Vertrauen in den Finanzsektor Deutschlands als Gesamtheit. Das Vertrauen in den Bankenplatz Deutschland bzw. Europa aber muss die Aufsicht bewahren, will sie vermeiden, dass die Kundschaft sich ausländischen Anbietern zuwendet. In Zeiten des Internets sind Bankdienstleistungen weltweit verfügbar, wie die Erfahrung mit PayPal, Google Pay oder Apple Pay gezeigt hat.

Die Umsetzung der BAIT kann an Unzulänglichkeiten in vielen Bereich scheitern oder sich verzögern, sei es wegen zu geringer finanzieller Mittel aufgrund der schwachen Ertragslage oder falscher Prioritäten. Auch Know-how-Defizite im Bereich der IT spielen eine Rolle, denn Banken gelten gerade bei qualifizierten, jungen Menschen nicht mehr als der sichere, erstrebenswerte Arbeitgeber. Von daher tun die Banken gut dran, eine umfassende und tiefe Analyse des eigenen aktuellen Status-Quo durchzuführen, um Defizite aufzudecken, diese zeitnah zu beheben und damit das eigene ökonomische Risiko zu vermindern. Sie müssen das tun, um

auch der Aufsicht gegenüber zu zeigen, dass das Risiko, das sie selbst in der Wirtschaft darstellen, kleiner geworden ist, überschaubarer und jederzeit handhabbar, wenn sie Sanktionen der Aufsicht bis hin zu einer Einschränkung des Geschäftes über erhöhte Kapitalquoten vermeiden wollen.

Die BAIT schaffen einen einheitlichen Rahmen für alle Institute, die durch die BaFin beaufsichtigt werden. Allerdings gibt es institutsspezifische Unterschiede, die durch das jeweilige Geschäftsmodell, die Größe, die Internationalität oder das Budget bedingt sind.

Von daher tun Banken gut daran, ihre Konformität kurzfristig auf den Prüfstand zu stellen, sie zu dokumentieren und Handlungsnotwendigkeiten zügig und umgehend umzusetzen.

Frankfurt, im September 2018.

Die Ausführungen in diesem Buch beziehen sich auf die Veröffentlichung der BaFin vom 06.11.2017 mit den Ergänzungen vom 14.09.2018.

Aufbau dieses Buches

Dieses Buch gliedert sich in zwei Hauptabschnitte:

- Die grundsätzliche Situation von Banken im Hinblick auf ihre IT-Infrastruktur
- Die Regelungen der BAIT und in diesem Zusammenhang Vorstellung der relevanten Inhalte der MaRisk im Detail

Die BAIT und die MaRisk der Aufsicht treffen auf einen gelebten Ist-Zustand der IT in den Banken. Eine Art der Mindestanforderung zu definieren bedeutet für alle Banken einen neuen, einheitlichen Level an Aufwand. Das erste Kapitel stellt Probleme der Banken dar und damit den Hintergrund des Vorgehens der Aufsicht.

Die neuen Regelungen machen es notwendig, dass die Banken eine GAP-Analyse vornehmen, also einen ersten Check, der die Differenz Ist-Zustand und Soll-Zustand definiert. Wegen der Mannigfaltigkeit der Aufgaben, insbesondere auch der neuen revisionssicheren Dokumentationspflichten benötigt die Umsetzung einen relativ hohen Aufwand. Dieser Teil beinhaltet die Bedingungen und die wichtigsten Nebenbedingungen für eine erfolgreiche Umsetzung der BAIT.

Zu diesem Buch gehören als weitere Arbeitsunterlagen vertiefte Darstellungen von den notwendigen Rollen, den Dokumenten, die vorliegen müssen, Prozessen und Teilprozessen sowie Angaben zu Fristen und zum Turnus von Meldungen.

Inhaltsverzeichnis

Teil I

Grundsätzliche Situation von Banken im Hinblick auf ihre IT-Infrastruktur

Überblick zur IT in der Bankenwelt

1

Zusammenfassung

Immer wieder ist in den Nachrichten von technischen Problemen bei Banken zu lesen. Die Finanzbranche befindet sich nach der Krise 2008/2009 noch mitten in der Umstrukturierung und Anpassungsphase. In dieser Zeit des Umbruchs mit neuer Technik, die marktfähig wird, aber auch Unzulänglichkeiten, die noch bestehen, legt die Aufsicht ihre Anforderungen für die Finanzbranche vor. Die BAIT basieren auf Erfahrungen aus der Vergangenheit und schaffen ein gemeinsames Level. Die Banken-IT hat im Alltag aber verschiedene Probleme, die sie daran hindern, allen Anforderungen zeitnah und umfassend gerecht zu werden.

In diesem ersten Kapitel soll ein allgemeiner Überblick gegeben werden über den Stand der Bankenwelt insbesondere in Bezug auf IT-relevante Themen und ihr Umfeld. Das leitet dann zur Frage über, wieso die Aufsicht ein derartiges Papier wie die BAIT für einen Teilbereich der operationellen Risiken für notwendig hielt.

T. Maksimovic, H. Biernat, *Bankaufsichtliche Anforderungen an die IT (BAIT)*,
https://doi.org/10.1007/978-3-658-25226-7_1

1.1 Aktueller Stand IT-Sicherheit in der Bankenwelt

Skandale und Pannen führen dazu, dass Medien und damit die Gesellschaft auch solche Unzulänglichkeiten der modernen Bankensteuerung, die ihre Ursache direkt oder indirekt in der technischen Ausrüstung der Banken haben, wahrnehmen. Die Banken-IT ist stellt dabei einen viel größeren Bereich dar, als nur die nach außen sichtbare Versorgung der Kunden mit Daten oder Geld. Banken-IT beruht auf Technik, aber sie erfordert auch Know-how und umfasst Prozesse, die im Hintergrund beteiligt sind. Ohne eine technische Infrastruktur ließen sich die Bankdienstleistungen nicht erbringen. Mit der vorhandenen Infrastruktur aber ist der Aufwand in der Regel groß, die Veränderungsspielräume sind klein und der Mut zur Kraftanstrengung einer grundlegenden Modernisierung eine Frage der Zeit, des Geldes und des Wollens.

In der Presse sind immer wieder Beispiele für Pannen und Großschadenereignisse zu finden, wie die folgende Auswahl davon zeigt:

„Die japanischen Behörden haben eine Strafe gegen die Kryptobörse Coincheck angekündigt, bei der Hacker Digitalanlagen im Wert von umgerechnet ungefähr 430 Millionen Euro erbeuteten." (FAZ [44])

„Auch eine Cyberoperation kann unter bestimmten Bedingungen einen „bewaffneten Angriff" im Sinne von Artikel 51 VN-Charta darstellen, so die Bundesregierung." [39]. (Süddeutsche Zeitung [53])

„Die Bundesbank warnte allgemein vor Cyberangriffen, der deutschen Wirtschaft würden damit Schäden in Milliardenhöhe entstehen.

Hacker plünderten in Großbritannien bei einem Angriff 20.000 Konten. Sorglose Mitarbeiter gelten als das Kernproblem bei der Cyber-Kriminalität". (Reuters [52])

„Der Deutschen Bank entstand zwar kein Schaden durch eine Fehlüberweisung 28 Mrd., trotzdem forderte die Aufsicht eine Untersuchung zu dem Vorfall". (Handelsblatt [46])

„Die Presse berichete von einem Datenklau bei JP Morgan, 83 Millionen Konten waren gehackt worden". (n-tv [50])

„Geldautomaten wurden mit Malware gehackt, in einem anderen Fall war das Betriebssystem die Ursache, das nicht mehr unterstützt wurde". (IT Finanzmagazin [48])

„Bei einem anderen Vorfall wurden Scheinkonen bei Wells Fargo eingerichtet". (Consumer Finance Protection Bureau [32]) (cfpb)

„Das Zahlungssystem SWIFT meldete erneut einen Angriff auf eine Bank. Hier waren auf Endgeräten notwendige Updates nicht gelaufen". (Zeit [51])

„Die Schadsoftware „WannaCry", eine Ransomware, also eine Erpressungssoftware legte weltweit Industrien und Dienstleister lahm". (FAZ [51])

Neben den Schäden, die im Rahmen solcher Skandale entstehen und sichtbar sind, gibt es auch schleichende Verluste, die ihre Ursache nicht in Einmal-Ereignissen, sondern in den strukturellen Problemen der Banken haben. Sie führen

zu Reibungsverlusten und erhöhten Kosten, aber auch zu Nachteilen im Wettbewerb, wenn z. B. Konkurrenten in ihren Prozessen schneller sind und so Produkte zuerst auf den Markt bringen können. FinTechs, also Firmen, die technische Lösungen (tech) für Financial Services (fin) entwickeln, können zügig Produkte entwickeln, die potenziell dazu führen, dass die Kunden abwandern, wenn andere Angebote schneller, preiswerter oder in anderer Art vorteilhafter sind.

In der Vergangenheit sind bereits technisch-organisatorische Projekte von Teilen der Bankenwelt umgesetzt worden, die, wie beispielsweise die Online-Kontoeröffnung, einen Vorteil für den Kunden mitbringen. Nur ist die Geschwindigkeit, in der Innovationen entstehen, schneller, als die tatsächlich Mehrwert schaffenden Applikationen ihren Weg in die Schalterhalle oder das Onlinebanking der Banken finden. Auch hierzu gibt es verschiedene mediale Beispiele, die das Problem der Banken zeigen:

Deutsche Bank So hatte der derzeitige Vorstandsvorsitzende der Deutschen Bank in der Presse mitgeteilt, dass andere Banken mit weniger Personal auskämen, da bei ihnen auch die Prozesse besser seien. (Handelsblatt [45])

Commerzbank Die Wirtschaftswoche hatte berichtet, „Wie bei vielen anderen Instituten gleicht die EDV-Landschaft auch der Commerzbank einem grob zusammengesetzten Puzzle, dessen Teile nur durch große Flicken zusammengehalten werden." Später heißt es dazu „für eine grundsätzliche Renovierung reicht das Geld nicht." (Wirtschaftswoche [55])

FinTechs Das Geschäftsmodell der beschriebenen FinTechs ist ein Motor für Innovation, basierend auf neuen technischen Möglichkeiten. Die Bankenwelt sieht sich damit, aber auch in anderen Bereichen kurz vor den zwanziger Jahren des 21. Jahrhunderts vielen weiteren Optionen gegenüber. Eine Reihe davon soll im Folgenden dargestellt werden, die Liste ist allerdings nicht abschließend. Jedoch zeigt sie, dass die Banken-IT sich wandeln muss, wenn die Banken auch zukünftig noch eine große Bandbreite an Produkten anbieten möchten. Sie müssen diese Neuerungen integrieren, spätestens dann, wenn die Konkurrenz es tut. Die Geschwindigkeit wird der Markt vorgeben, das Instrumentarium, etwa Mobiltelefone, sind weit verbreitet, womit es Plattformen gibt, die es mit innovativen Vertriebsmitteln aber auch mit Kommunikationsmitteln zu füllen gilt.

Verzicht auf Bargeld Schweden arbeitet jetzt schon erfolgreich an der Abschaffung des Bargelds bis zum Jahre 2030 [31]. Geschäftstransaktionen müssen also eine technische Unterstützung haben, die im Hintergrund aller Geschäfte läuft. Für deutsche

Banken würde es ebenso eine Erleichterung sein, wenn verschiedene Arbeitsschritte bei Bezahlvorgängen wegfallen würden. Schon heute werden Münzen nicht mehr angenommen oder es fallen Gebühren für den Barverkehr an. Auf der anderen Seite sind die Möglichkeiten in Deutschland der bargeldlosen Bezahlung in Geschäften abseits von Kreditkarte oder Maestro (früher: EC-)Karte wenig bis kaum vorhanden, geschweige denn genutzt [38]. Mit innovativen Lösungen der FinTechs könnte sich das ändern.

Instant Banking Die Prozesse der Banken sind 2018 einer weiteren Belastung ausgesetzt worden [54], nämlich der Möglichkeit, dass Kunden Geldtransaktionen innerhalb von Sekunden durchführen können. Der Prozess von der Ausführung der Transaktion bei der Startbank bis zur Buchung bei der Zielbank, einem anderen Institut, sollte innerhalb von Sekunden durchlaufen sein. Dabei sind Prüfungen im Rahmen der Geldwäsche [49] ebenso erforderlich wie die Verrechnung zwischen den Banken. Diese Herausforderung hat notwendig gemacht, dass bestehende Banksysteme aufgerüstet werden oder aber neue Systeme eingeführt werden.

KI, Chats Eine ganz andere, innovative Software nutzt die künstliche Intelligenz für Problemlösungen. Erkenntnisse aus den Ergebnissen, die diese Software liefert, richtig zu interpretieren und sie umzusetzen, erfordert ein neues Herangehen an Problemlösungen. Die Lösungsvorschläge der KI können unkonventionell, schwer verständlich oder kaum nachvollziehbar sein. Als Lösung für alle komplexen Probleme gepriesen, steht sie gerade am Beginn ihres Einsatzes bei Banken und Finanzdienstleistern, etwa um Kommunikationsprozesse wie bei Chats zu verbessern oder die Geldanlage zu steuern.

Robo-Advisor Die Form der Umsetzung von Kundenwünschen durch Computer in Form von Robo-Advisern [30] ist für einige Fonds bereits zum Geschäftsmodell geworden. Die effiziente, zielgerichtete Beratung von Kunden und der Steuerung von Depots in Zeiten der höheren Anforderung an die Beratung und insbesondere deren Dokumentation (MiFID II) [19] ist eine neue Art der Kommunikation der Institute mit der Außenwelt.

1.2 Was sind die BAIT?

In der Situation umfangreicher Innovationen hinein definiert die Aufsicht nunmehr ihre Anforderungen, nach denen die Banken ihre Prozesse, ihre IT-Struktur und ihre Verwaltung aufsetzen sollen. Sie sind proportional und rechtsform- und

geschäftsmodellunabhängig. Das heißt, die BAIT gelten für kleine wie für große Institute und lassen auch die Spezialbanken nicht außer Acht.

Bedeutung BAIT BAIT ist die Abkürzung für „Bankaufsichtliche Anforderungen an die IT". Die BAIT präzisieren das KWG, sie stellen aber auch eine weitere Konkretisierung der IT-relevanten Passagen der MaRisk dar, die ebenso das KWG konkretisieren. Mit den BAIT will die Bankenaufsicht nach eigenem Bekunden einen flexiblen und praxisnahen Rahmen für das IT-Risikomanagement schaffen.

Die BAIT sind eine Verwaltungsvorschrift in Form eines Rundschreibens und sind demnach keine Verordnung. In Hinblick auf die Umsetzung macht das allerdings keinen Unterschied, denn die Aufsicht kann auf beide Arten zeigen, wie sie die Ausgestaltung wünscht. Sie sind für die Institute bindend. Externe Prüfer wie auch die interne Revision der Banken werden ihre Umsetzung untersuchen und in Prüfungsberichten darlegen. Eine mangelhafte und von den Wünschen der Aufsicht abweichende Umsetzung könnte, je nach Umfang des Mangels, verschiedene Folgen für die jeweiligen Banken haben.

Eine Reihe von Einflussfaktoren wirkt auf die Umsetzung ein:

- Größe des Kreditinstituts,
- Komplexität des Geschäfts,
- Notwendigkeit einer Risikoadjustierung sowie
- dessen Internationalität.

Alle diese Einflussfaktoren machen eine unterschiedliche Herangehensweise an eine Umsetzung der BAIT notwendig. So muss ein Institut, je größer es ist und je komplexer sein Geschäft ist, ausreichende Kontrollmechanismen haben.

1.3 Warum wurden die BAIT aus Sicht der Aufsicht geschaffen?

Die Aufsicht hat die BAIT nicht zum Selbstzweck geschaffen. Sie setzt mit ihnen Grundsätze um, die die internationalen Regulatoren aufgestellt haben. Das zugrundeliegende Problem von unzureichenden Kontrollmechanismen, bedingt durch mangelnde, sicherheitstechnische Ausstattung und fehlendes Bewusstsein um Risiken oder Know-how, ist in Zeiten der Vernetzung über das Internet nicht nur ein Problem der Banken, sondern von allen ans Netz angebundenen Teilnehmern. Banken haben in einer Volkswirtschaft allerdings wichtige Funktionen und sind damit besonders schützenswert, denn nur funktionierende und sichere Geldflüsse sowie

Möglichkeiten der Geldaufbewahrung und Finanzierung stellen ein Funktionieren der Wirtschaft sicher. Die Infrastruktur der Banken sieht sich, ebenso wie die anderen Teilnehmer der Wirtschaft, immer wieder auch Angriffen von Außen ausgesetzt. Die Bankenaufsicht befindet sich daher im Zugzwang, für mehr Sicherheit zu sorgen. Verschiedene Bundesämter haben sich des Themas bereits von anderer Seite angenommen. So haben das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine eigene Initiative zum Thema des Schutzes kritischer Infrastrukturen ins Leben gerufen. (BSI [21])

Erfahrungen der Vergangenheit Die bereits beschriebenen Erfahrungen der Vergangenheit, die aus früheren Problemen der Banken resultieren, gehören mitunter zu den Ursachen für das Vorgehen. Die Bankenindustrie hat es nicht geschafft, eigene Mindeststandards zu finden und zu definieren. Nun fassen die MaRisk und die BAIT einige supranationale Regelungen zusammen, die von allen Instituten in ihrem Bereich umzusetzen sind.

Bankenrettung In der Vergangenheit wurde eine Reihe von Banken im Zuge der Finanzkrise der Nullerjahre gerettet. Die finanziellen Anstrengungen für den Steuerzahler waren groß. Die Aufsicht möchte das in Zukunft vermeiden und hat daher nicht nur im Bereich der IT in den vergangenen Jahren das Level von Meldungen und Limitierungen nach oben geschraubt. Neben quantitativen Maßnahmen [5], wie der Erhöhung der Kapitalunterlegung für Geschäfte, Marktrisiken und operationelle Risiken, wird mehr Wert auf die qualitative Ausgestaltung von Prozessen und Systemen gelegt.

Sicherstellung und Erhaltung von Vertrauen Bankenkrisen haben neben dem finanziellen Aspekt für Steuerzahler, der zukünftig ausbleiben soll, immer auch noch einen anderen negativen Beigeschmack: Wenn Banken in Krisen geraten, stellt sich immer die Frage, wieso die Aufsicht nicht vorher eingeschritten ist. Die Aufsicht legt also mit den BAIT fest, wie sie sich die Ausgestaltung vorstellt. Einerseits, um für Klarheit zu sorgen, andererseits aber auch um zu zeigen, dass sie die technische Ausstattung und den Umgang der Banken mit Daten für wichtig hält. Nur so kann die Aufsicht verlorenes Vertrauen wieder zurückerlangen. Die deutsche Aufsicht schließt sich dem Vorgehen der Aufsichten in den anderen Industrienationen an, wonach Risiken aufzudecken, zu behandeln und zu limitieren sind.

Währungsproblematik Die Umstellung auf eine einheitliche Währung in weiten Teilen der EU mit allen damit verbundenen Problemen in der tatsächlichen Ausgestaltung hat das Vertrauen der deutschen Anleger in die Stabilität der

Währung nicht gefördert. Ausweichwährungen wie Bitcoin, als eine Verrechnungseinheit von Geld in technischer Form, erlangen weltweit immer mehr Aufmerksamkeit. Große Anleger haben in der Vergangenheit versucht, sich den deutschen Regeln zu entziehen. Das immer weiter aufgeweichte Bankgeheimnis ist ein zusätzlicher Grund, um den eigenen Wirtschaftsraum zu verlassen. Andererseits wird gerade ein Land wie Deutschland mit seiner Einlagensicherung weiterhin eine Anlaufstelle sein – zumindest für Privatkunden. Die Aufsicht muss also versuchen, das Vertrauen, das dem Bankenplatz Deutschland entgegengebracht wird, durch flankierende Maßnahmen zu unterstützen [18], um nicht nur die Einlagen, sondern allgemein die Abwicklung von Bankgeschäften sicherer zu machen.

Risiko Die Aufsicht hat dem Thema Risiko in der Vergangenheit große Aufmerksamkeit gewidmet. Mit den novellierten MaRisk und den neuen BAIT schenkt sie nunmehr auch dem Thema der Datenbeschaffung größere Beachtung und somit also dem Schritt vor der Berechnung des Risikos.

Gemeinsamer Level Weil die Regelungen für alle Institute gleichermaßen gelten, schaffen sie ein gemeinsames Level und damit eine gleiche Ausgangsbasis. Wettbewerbsvorteile durch Kostenersparnis bei den Kontrollen werden so erschwert, für die Banken wird eine Umstellung unabhängig von ihrer Größe aufwands- und kostenintensiv. Dabei hat aber auch niemand Vorteile, außer, er hat die Regelungen bereits vorher zumindest in ähnlicher Art und Weise umgesetzt.

Arbeitsteilung der Banken Banken befinden sich wegen verschiedener Regelungen, Marktverhältnisse oder Marktgegebenheiten gerade im Umbruch. Durch Regeln wie der Payment Services Directive (PSD2; Zahlungsdienstrichtlinie) oder die Bevorteilung von Geschäften mit zentralen Kontrahenten steigt die Arbeitsteilung bei den Bankprodukten. Die Verbindungen der Banken zu Zulieferern und Dienstleistern wird in Zukunft weiter intensiviert werden. Insofern kommen die neuen BAIT nicht zu spät, da sie am Anfang einer neuen Entwicklung stehen.

Das Bestreben der Aufsicht nach mehr Sicherheit lässt sich in verschiedene große Kategorien einteilen:

Risikobewusstsein schärfen Das Thema Risiko ist seit Jahren durch die Aufsicht forciert worden: Die Kennzahlen und Limite wurden verschärft, die Möglichkeiten der Institute beschnitten und Geschäftsmodelle mussten angepasst werden. All das sollte dazu geführt haben, dass das Risikobewusstsein gestiegen ist. Aus Sicht der Aufsicht scheint das allerdings nicht überall der Fall zu sein, da sie ihre Anforderungen nun derartig konkretisiert. Sie fordert von den Banken mehr Aktivitäten im

eigenen Haus, wobei das Informationsrisiko ein neues eigenständiges Risiko geworden ist, wenn es letztendlich auch noch dem operationellen Risiko zugeschlagen wird. Prüfungen, neue Prozesse, neue Funktionen – all das soll helfen, das Bewusstsein innerhalb der Institute zu steigern und auch die Mitarbeiter sollen sensibilisiert werden.

Studie zu Phishing Mails Dass eine laufende Sensibilisierung der Mitarbeiter konkret an ihrem Arbeitsplatz notwendig und sinnvoll ist, zeigt eine Untersuchung (Tagesspiegel [33]) zu Phishing Mails, also dem Versuch, Mitarbeiter unter Vorspielen falscher Tatsachen an ihrem Arbeitsplatz zur Weitergabe von Daten und Informationen zu verleiten. Bei einem Test der Berliner Polizei wurden 466 Phishing Mails im Rahmen einer User Awareness Schulung versendet, die Reaktionen wurden später ausgewertet. In 50 % aller Fälle wurde der darin enthaltene Link angeklickt. Allein schon auf diese Art und Weise wäre es möglich gewesen, schädlichen Code wie Viren oder auch Software einzuspeisen, die serverseitig ausgeführt werden. Die eigenen Zugangsdaten wurden 35 Mal auf der manipulierten Eingangsseite eingegeben und somit preisgegeben.

Um das Risikobewussten zu steigern, sollte es in den Banken eine Funktion geben, die diese Entwicklung vorantreibt. Die Steigerung oder zunächst auch die Einführung einer Risikokultur ist eine der neuen Aufgaben aus der Novellierung der MaRisk aus 2017. Dass eine derartige Maßnahme überhaupt von der Aufsicht angesprochen werden musste, zeigt auf, dass es Defizite gegeben hat und noch gibt.

1.3.1 Digitalisierung intern sicherer machen

Medienbrüche Die Digitalisierung an sich ist keine besonders neue Herausforderung und trotzdem bestehen aus Sicht der Aufsicht verschiedene Risiken: So haben die Banken bereits in der Vergangenheit viele ihrer Abläufe digitalisiert. Dennoch ist ein Großteil der Prozesse der etablierten Banken immer noch von Medienbrüchen gekennzeichnet. Die Abläufe sind also nicht durchgehen technisiert, sondern haben Unterbrechungen, die manuelles Eingreifen erfordern. So bestehen Datenstrukturen, die nicht maschinell aufeinander abgestimmt sind. Hinzu kommen neue Produkte und neue Marktchancen, für die oft noch keine integrierten Systeme existieren. Die betreffenden Erweiterungen müssen mühsam angeschlossen und Unzulänglichkeiten mit Workarounds geheilt werden.

Eine schlecht umgesetzte Digitalisierung erhöht die Risiken der Institute, die zu Ausfällen, Verzögerungen oder gar Schäden führen können. Hier möchte die Aufsicht durch die Dokumentationspflichten und auch für die Prozesse im Bereich des Änderungsmanagements mehr Transparenz schaffen. Ferner dürfen die Institute im

Bereich von neuen Produkten, Techniken und Prozesse nicht einfach auf das Instrument der Auslagerung zurückgreifen. Hier sind ebenfalls erhöhte Anstrengungen zu unternehmen, was bedeutet, dass Institute sich des Aufwands und des Risikos gegen Zahlung von Geld nicht entledigen können.

Geschäftsmodelle werden heute nachhaltiger und erfolgreicher durch Digitale Innovationen. Vergleicht man den Bankenbereich mit anderen Branchen, hat sich dieser erst relativ spät an die digitale Transformation gewagt. Solche Transformationen benötigen mitunter eine Digitalisierungsstrategie, welche wiederum mit der Gesamtstrategie in Einklang stehen muss.

Kosten-Risiko Trade-off Je weniger in der Vergangenheit digitalisiert wurde, desto höher ist der Aufwand heute und desto höher sind auch die Risiken. Möchte man einheitlich digitalisieren, so entstehen am Anfang hohe Kosten und hoher Aufwand. Wenn bestehende Prozesse und IT-Systeme lediglich angepasst werden, so mögen die Anschaffungskosten geringer bleiben, aber der Anpassungsaufwand wird hoch sein. In diesem Trade-off ist der individuell bestmögliche Weg zu suchen.

Auslagerung Schnittstellen, die benötigt werden, um Daten von einem System in ein anderes zu laden, stellen eine weitere Herausforderung dar, sie bilden aber auch einen Zeitfaktor: Es dauert seine Zeit bis alle Routinen durchlaufen sind und die gewünschten Daten zur Verfügung stehen. Eine Auslagerung etwa von Datenspeichern, um flexibler zu sein, bringt ganz neue IT-Landschaften hervor, die Einfallstore für Hacker werden zahlreicher. Die Auslagerung wurde von den Banken bisher aus Gründen der Rationalisierung betrieben und um Kosten zu sparen. Die MaRisk und die BAIT verbieten das nicht, aber sie machen es weniger attraktiv. Bisher verfolgten die Banken bei einer Auslagerung den Wunsch nach weniger Komplexität und nach weniger Know-how, das vorgehalten werden musste, also war eine Auslagerung oft eine Kostenverbesserung. Mit den zusätzlichen Anforderungen werden die Banken ihre Berechnungen neu aufmachen müssen und es ist davon auszugehen, dass an verschiedenen Stellen wieder ein Insourcing betrieben wird.

In diesem Umfeld treiben FinTechs die Banken vor sich her und haben die Taktzahl an marktfähigen Innovationen inzwischen deutlich erhöht. Somit beginnen die Erträge der Banken zu erodieren, während sie gleichzeitig versuchen müssen, ihre Kunden zu halten, zu investieren und aufgrund von Ertragsschwächen in anderen Segmenten, die Erträge zu steigern. Durch die Digitalisierung sind Kooperationen und Übernahmen mit und von FinTechs keine Seltenheit geworden.

Cyber-Angriffe, also Angriffe von außen verhindern Cyber-Angriffe sind ein Oberbegriff für alle Versuche, in ein Netzwerk einzudringen, um dort zu stehlen, zu verändern oder zu spionieren. Dazu brauchen die Verbrecher nicht mehr selbst in eine

Bank einzudringen, denn es reicht, den Angriff über das Internet zu betreiben. Die Schwachstellen, die mit einer Einbindung ins Internet einhergehen, stellen die größten Risiken der Finanzwirtschaft dar. Viren und Trojaner waren von jeher eine Gefahr für die Datensicherheit. Cyber-Angriffe sind nicht mehr nur abstrakte Gefahren aus dem privaten Bereich, sondern sind zu einer ernstzunehmenden und existenzbedrohenden Gefahr, insbesondere für sensible Bereiche der Wirtschaft geworden.

Direkte Angriffe über das Internet gehören zum Alltag. Sie werden in der Regel durch verschiedene Schutzmaßnahmen abgewehrt. Da der Trend in den Banken zu einer Flexibilisierung der Arbeitsplätze geht, werden auch ihre Systeme mobil, die Infrastruktur wird fragmentierter und das Risiko eines Daten- oder Informationsverlustes kann ohne genaue Kontrolle steigen. Das Ziel der Anstrengungen von Instituten muss es also sein, den Angriffen zu begegnen, denn einem mobilen Arbeiten oder dem Homeoffice werden sie sich letztendlich nicht entgegenstellen können. Mobiles Arbeiten steigert ebenfalls das Risiko, es ist aber nicht die einzige Möglichkeit, sich Cyberangriffen ausgesetzt zu sehen. Die Institute tun von daher gut daran, hier vorbeugend tätig zu sein. Cyber-Angriffe können, neben dem direkten Schaden vor allem sehr einfach das Vertrauen der Kunden in Banken zerstören. Aus Sicht der Bankenaufsicht besteht hier Handlungsbedarf, um das Vertrauen in Banken und den Bankenmarkt allgemein zu erhalten.

Business Continuity Management (BCM; Betriebliches Kontinuitätsmanagement) vorantreiben Die Ursachen für Ausfälle können vielfältig sein. DDOS Attacken (Cyber-Angriff durch Überlastung der IT-Infrastruktur) und Datendiebstahl können die Reputation eines ganzen Instituts gefährden. Als viel dringenderes Problem stellt sich ein Ausfall der IT-Systeme selbst dar, denn er erfordert schnelles Handeln und seine Lösung wird kurz- und mittelfristig Geld kosten. Noch eklatanter ist die ad-hoc Auswirkung, denn ein Ausfall kann nicht nur durch Hilfe, die benötigt wird, oder Ausweichmaßnahmen die Kosten steigern. Der Ausfall von Funktionen und Technik kann sogar das Überleben eines Instituts gefährden, wenn mangels der Möglichkeit, auf Daten zugreifen oder reagieren zu können, drohende Risiken nicht erkannt und abgemildert werden können.

Notfallpläne werden bereits im KWG gefordert. Wie die Ausgestaltung erfolgen soll, insbesondere auch, was richtig und angemessen ist, ist wie alle Umsetzungen proportional zum Risiko zu tun.

Die Probleme der Vergangenheit haben gezeigt, dass die Vernetzung kaum einfache Lösungen zulässt. Stattdessen müssen diese integriert sein. Das Kontinuitätsmanagement ist nicht nur ein Notfallplan für eine Ressource wie die IT, sondern es bezieht sich auf die Durchführungsmöglichkeit von Prozessen, unabhängig von einer bestimmten Problemstellung.

Risikodaten verlässlicher machen Die Aufsicht hat die Anforderungen an das Meldewesen hochgefahren [20]. Die Banken müssen nicht mehr nur aggregierte Daten melden, sondern vielmehr auch Details zu ihren Geschäften angeben. Diese Daten werden in der entsprechenden Detailtiefe bereits in den Fachabteilungen sowie im Risikomanagement verwendet. Nun gehen die Anforderungen noch weiter, da sie sich auf die Geschwindigkeit der Bereitstellung von Risikodaten und auf die Abstimmung der Daten untereinander beziehen. Damit soll ein hohes Sicherheitslevel bei der Bereitstellung der Risikodaten und die schnelle Bereitstellung von entscheidungsrelevanten Daten gewährleistet werden.

Auch diese Anforderung führt zu einem Aufwand im Hintergrund, denn so einfach die Aufgabe auf den ersten Blick klingen mag, so oft scheitert sie an Verarbeitungszyklen der Systeme, Datenmengen oder der Vereinheitlichung von Datenstrukturen.

1.4 Probleme der Banken-IT im Alltag

Die BAIT schaffen einen einheitlichen Rahmen für alle Institute, die durch die BaFin beaufsichtigt werden. Allerdings gibt es institutsspezifische Unterschiede, bedingt durch das jeweilige Geschäftsmodell, die Größe, die Internationalität oder das Budget. Diese können sich auf verschiedene Faktoren beziehen, die im Folgenden ausgeführt werden.

Technik Investitionen in Technik sind teuer, binden Ressourcen und stellen für eine Bank eine enge, oft langjährige Bindung an einen Software- bzw. Hardwarepartner dar. Dadurch, dass bestehendes Know-how mit einem Partner zusammen in für die Bank neue Technik umgesetzt wird, geht sie das Risiko des Wissenabflusses ein; einerseits, weil das Wissen der Bank durch den Partner für andere Produkte oder auch nur für eine Verbesserung der eigenen Produkte angewendet wird, andererseits macht sie mit der Verbesserung auch bisherige, eigene Schritte obsolet und eigenes Wissen in Teilen unnötig. Neue Technik ist immer auch eine Form der Rationalisierung indem Arbeitsschritte wegfallen. Ebenso kann sie zu einem Job-Enrichment oder -Enlargement führen. Beides wird bei den beteiligten Mitarbeitern neues Wissen erforderlich machen.

Menschen Die Arbeitsbilder, also die Aufgaben und Verantwortlichkeiten in einer Bank, sind unterschiedlich. Personen und Wissen sind nur bis zu einem gewissen Grad austauschbar. Die durch die Bankenaufsicht geforderte Trennung in Markt und Marktfolge ist dabei nur die gröbste, aber am ehesten sichtbare Trennung der

Aufgaben und Verantwortlichkeiten in den Instituten. Sie trennt in einen Bereich, der tatsächlich Geschäfte am Markt eigenverantwortlich abschließt, und all jene Bereiche, die dazu nicht berechtigt sind, weil sie andere Aufgaben bei der Abwicklung, Buchung oder Überwachung der Geschäfte haben.

Die Berufsbilder von Bankmitarbeitern können sich aber noch weiter unterscheiden. Neben den technischen Berufen, die bis hin zur Anwendungsentwicklung reichen, gibt es die Spezialisten in den Marktfolgebereichen für thematische Schwerpunkte wie Meldewesen oder Riskomanagement und Buchhaltung oder auch Revision und Compliance. Dazu gibt es jeweils unterstüzende Bereiche wie Personal oder auch technische Berufe, für die ein tieferes Bankwissen größtenteils nicht notwendig ist und in denen vielmehr andere Qualifikationen zählen. So vielfältig die Menschen im Unternehmen sind, sind es auch die Menschen um die Insitute herum, nämlich die anderen Stakeholder, wie auch die Kunden, seien sie nun Privatpersonen, wirtschaftlich Tätige oder Unternehmen. All diese Gruppen haben in Bezug auf die technische Verfügbarkeit einer Bank und deren Bereitstellung von Dienstleistungen unterschiedliche Ansprüche und Wünsche.

Umwelt Auch die Umwelt eines Institutes wird durch Stakeholder geprägt, die unterschiedliche Ansprüche haben, etwa die Versorgung auf dem Land, Steuereinnahmen, ökologische Unbedenklichkeit oder Engagement bis hin zu einer Frauenquote. Banken befinden sich also im Zwiespalt zwischen dem Möglichen und dem Gewünschten. Die BAIT schaffen einen einheitlichen Rahmen, auch wenn die Institute in unterschiedlichen Märkten agieren. So gibt es Institute, die eher lokal verhaftet sind, bis hin zu multinationalen Konzernen, für die Deutschland nur einer von vielen Standorten ist. Die Kunden der Bank agieren in unterschiedlichsten Branchen, was immer auch Unterschiede in der Risikobetrachtung mit sich bringt. Außerdem führt nicht jedes Engagement der Bank zwangsläufig auch zu einer Kundenbeziehung, so können Banken auch beispielsweise selbst durch den Kauf von Aktien oder Anleihen engagiert sein.

Rendite Eine der häufigsten Kennziffern, die für eine Performancebeurteilung herangezogen wird, ist die Rendite. Sie ist, bezogen auf das jeweils eingesetzte Kapital, Ausdruck der Ausschüttung von Gewinnen durch die Gesellschaft oder durch Kursgewinne, die die Einschätzung des Marktes darstellen. Ihre Betrachtung ist in der Regel periodisch. Wenn ein hoher Gewinn ausgewiesen werden soll, muss der Ertag entsprechend hoch sein oder die Aufwendungen und Kosten müssen entsprechend niedrig ausfallen. Die Ausgaben einer Bank, an denen gespart werden kann, umfassen neben Personalkosten auch Raumkosten oder Kosten für die technische