BAIT – eine weitere Herausforderung für Finanzdienstleistungsinstitute

Weiterentwicklung und Konkretisierung der Anforderungen

Dr. Bodo Chrubasik, Achim Schütz, Markus Elsbroek

Die Bankaufsichtlichen Anforderungen an die IT (BAIT) gelten als eine Konkretisierung der teils abstrakten Aussagen der Mindestanforderungen an das Risikomanagement (MaRisk) bezogen auf die Informationssicherheit bei Kreditinstituten und Finanzdienstleistern. Durch den höheren aufsichtlichen Druck werden Banken ihre Prozesse und Standards zur Umsetzung der IT-Strategie anpassen oder neu implementieren müssen. Der Beitrag informiert über Inhalt der BAIT, deren Zusammenspiel mit den MaRisk und entsprechende Handlungsfelder (Red.)

Bereits jetzt müssen Finanzdienstleistungsinstitute umfangreiche aufsichtsrechtliche Anforderungen erfüllen. Mit den im November 2017 finalisierten Bankaufsichtlichen Anforderungen an die IT (BAIT), veröffentlicht im Rundschreiben 10/2017 (BAIT)),[1] setzt sich der Trend der Weiterentwicklung und Konkretisierung der Anforderungen an die Informationstechnologie (IT) von Kreditinstituten fort. Dieser Trend steht im Einklang mit den erweiterten Anforderungen aus der Novelle der Mindestanforderungen an das Risikomanagement (MaRisk) 2017.

Durch die BAIT ist das Thema Informationssicherheit stark in den Fokus der Bankenaufsicht gerückt. Das Regelwerk BAIT legt unter anderem fest, wie die Berichts- und Informationspflicht zwischen dem neuen Informationssicherheitsbeauftragten und der Geschäftsleitung auszusehen hat. Außerdem finden sich darin Regeln zur Überprüfung der IT-Sicherheit im Alltagsbetrieb und in Bezug auf Datensicherung und Anwendungsentwicklung eigener Projekte sowie Festschreibungen zur Auftragsdatenverarbeitung durch Dritte.

Um mögliche kritische Prüfungsrisiken sowie eventuelle Schwachstellen und Handlungsfelder zu identifizieren, haben Finanzdienstleister den Status quo ihrer IT zu prüfen. Die BAIT zielen darauf ab, das Bewusstsein für das IT-Risiko und die IT-Sicherheit in den Instituten zu erhöhen. Inhaltlich sollen die BAIT als eine weitergehende Konkretisierung der zum Teil abstrakten und interpretationsbedürftigen Aussagen der MaRisk in Bezug auf die Themen der IT in Kreditinstituten verstanden werden – speziell für die im AT 7.2 MaRisk („technisch-organisatorische Ausstattung“) geregelten Sachverhalte. Die BAIT sind mit Fokus auf das Management von IT-Ressourcen und ein

1) Vgl. BaFin (2017): Bankaufsichtliche Anforderungen an die IT (BAIT), Rundschreiben 10/2017 (BA), Bonn.

DIE AUTOREN:

Quelle: BM-Consult

Dr. Bodo Chrubasik, Göttingen,

ist Experte für das Thema Auslagerungsmanagement. Er berät Banken, Leasing-Gesellschaften und Finanzdienstleister auf dem Gebiet der MaRisk und begleitete diverse Sonderprüfungen nach § 44 Gesetz über das Kreditwesen.

E-Mail: b.chrubasik@bm-consult.de

Quelle: BM-Consult

Achim Schütz, Göttingen,

ist geschäftsführender Partner der Bank Management Consult GmbH & Co. KG. Die Beratungsschwerpunkte liegen bei regulatorischen Themen wie MaRisk, in der Umsetzung komplexer Reorganisationen sowie dem Prozessmanagement bei Automobilbanken, Leasing-Gesellschaften und Objektfinanzierern.

E-Mail: a.schuetz@bm-consult.de

Quelle: BM-Consult

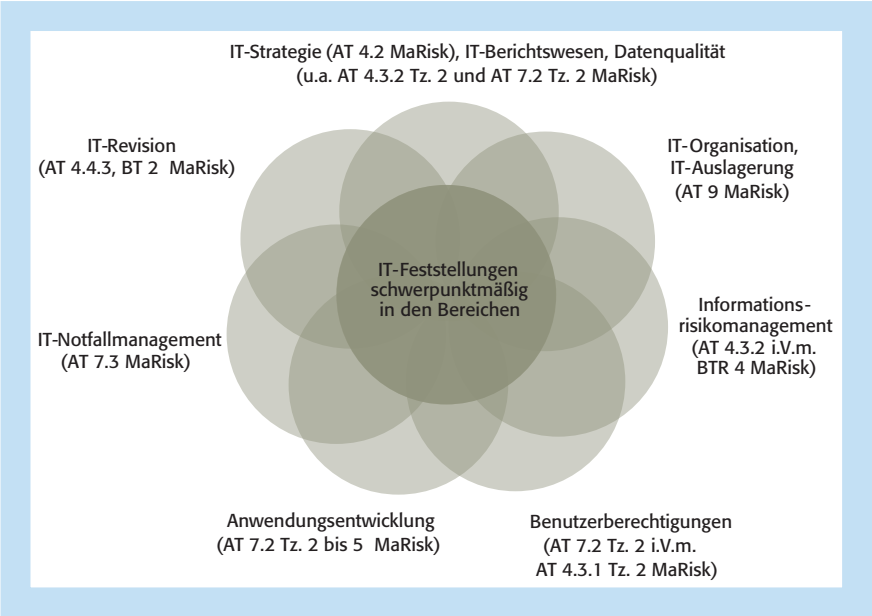
Markus Elsbroek, Göttingen,

ist Partner der Bank Management Consult GmbH & Co. KG. Seine Beratungsschwerpunkte liegen in den Bereichen digitale Transformation, agile Architekturen sowie im Sourcing- und Providermanagement inklusive BAIT bei Banken und Versicherungen.

E-Mail: m.elsbroek@bm-consult.de

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH

Abbildung 1: Wesentliche Feststellungen bei IT-Prüfungen



Quelle: Essler, R./ Gampe, J., Seite 18 [5]

gesamtheitliches Risikomanagement (IT-Sicherheit) in den Instituten formuliert.[2] Die in den Erläuterungen der BAIT gegebenen Hinweise an Inhalt und Umfang der Umsetzung der Anforderungen sind ein wichtiges Hilfsmittel für die Institute bei dieser Umsetzung.

Wie die MaRik interpretieren auch die BAIT die generellen Anforderungen des § 25a Absatz 1 Satz 3 Nr. 4 und Nr. 5 Kreditwesengesetz (KWG). Da die Institute zunehmend IT-Dienstleistungen von Dritten beziehen, auch im Rahmen von Auslagerungen, wird ebenfalls der § 25 b KWG in diese Interpretation einbezogen. Der Anwenderkreis der BAIT ergibt sich aus AT 2.1 MaRisk.

Die BAIT spiegeln die seit Jahren praktizierte Auslegung seitens der Aufsicht in bankgeschäftlichen IT-Prüfungen gemäß § 44 KWG wider und adressieren dabei insbesondere Themen, bei denen die Aufsicht in IT-Prüfungen der vergangenen Jahre wesentliche Mängel identifiziert hat (siehe Abbildung 1).[3] Leckner, Prüfungsleiter IT-Prüfungen bei der Deutschen Bundesbank, hat unter Rekurs auf das Konsultationspapier auf einer BAIT-Tagung dies sinngemäß wie folgt beschrieben: „Viele dieser Anforderungen befinden sich in diesem Konsultationspapier, nicht weil sie neu sind, sondern weil die Prüfungspraxis leider eindeutig zeigt, dass hier viele Banken immer noch viel Nachholbedarf haben.“ [4]

Der Ausgangspunkt für die BAIT liegt in der zentralen Bedeutung der IT in Kreditinstituten. So ist beispielsweise das Bankgeschäft heute vor allem Informationsverarbeitung. Alle wesentlichen Geschäftsprozesse von Kreditinstituten werden durch IT unterstützt oder sogar über die IT vollständig abgewickelt. IT ist die Basisinfrastruktur für sämtliche fachliche, aber auch alle nichtfachlichen Prozesse bei Banken. Der Trend zur Digitalisierung bestimmt immer mehr das Bankgeschäft.[6]

Durch die zunehmende Digitalisierung entstehen in der Regel unüberschaubare sicherheitskritische Datenmengen. Damit rücken auch IT-Sicherheit, Datensicherheit und Datenschutz stärker in den Fokus. Schadensauswirkungen durch einen Ausfall der IT-Systeme eines Kreditinstituts werden immer geschäftskritischer. Verschärfend hat das Risiko eines Angriffs auf IT-Systeme in den vergangenen Jahren stark zugenommen. Damit sind Schwachstellen in der IT eines der größten Risiken für die deutsche Finanzwirtschaft.[7] Die Aufsicht hat nun mit den BAIT neue Standards für eine sichere Ausgestaltung der IT-Systeme und der zugehörigen Prozesse formuliert sowie Anforderungen an die IT-Governance spezifiziert und transparent gemacht, die so in den MaRisk nicht beschrieben sind.

Neben der Notwendigkeit, den aus der Digitalisierung im Finanzsektor beschleunigt veränderten Anforderungen Rechnung zu tragen, war ein weiterer Aspekt, der zur Formulierung der BAIT geführt hat, der Wunsch der Kreditwirtschaft an die Aufsicht, die generischen Vorgaben der MaRisk für die IT zu detaillieren.[8]

Inhalt und Kontext der BAIT

Die BAIT selbst sind analog den MaRisk als Verwaltungsanweisung konzipiert, prinzipienorientiert gestaltet und modular aufgebaut. Die prinzipienorientierten Anforderungen des Rundschreibens tragen – analog zu den MaRisk – dem Proportionalitätsprinzip Rechnung: Dies wird insbesondere in der Textziffer (Tz.) 3 der Vorbemerkungen deutlich hervorgehoben und ermöglicht den Instituten damit eine risikoorientierte Umsetzung. Die modulare Struktur

2) Siehe hierzu auch die einzelnen Beiträge im Banken-Times Spezial (2017): Sonderausgabe BAIT, Heidelberg.
3) Essler, R./Gampe, J. (2018): IT-Sicherheit – Aufsicht konkretisiert Anforderungen an die Kreditsicherheit, in: BaFin-Journal 1/2018, Seite 17-21.
4) Riediger, H./ Uribe, J. (2017): BAIT-Tagung in Heidelberg – Quintessenzen, in: Banken-Times Spezial: IT/Orga/Neue Medien 9/2017 Heidelberg, Seite 45-47.
5) Vgl. Essler, R./Gampe, J (2018) ebenda.
6) Siehe hierzu beispielhaft Alt, R./Puschmann, T. (2016): Digitalisierung der Finanzindustrie, Wiesbaden 2016.
7) Vgl. Hufeld, F. in Kraus, A. U. (2017): Bankaufsichtliche Anforderungen an die IT – der immerwährende Kampf gegen die „bösen Jungs“, in: Die Bank 5/2017, Seite 32-35.
8) Vgl. Konsultation 2/2017 Bankaufsichtliche Anforderungen an die IT (BAIT), Bonn 2017.

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH

der BAIT eröffnet die notwendige Flexibilität für künftig erforderliche Anpassungen oder Ergänzungen.

Da die BAIT laut Aufsicht keine neuen Anforderungen an die Institute beziehungsweise ihre IT-Dienstleister kodifizieren, sondern lediglich Klarstellungen ohnehin schon vorhandener Anforderungen darstellen, sind keine Umsetzungsfristen oder Übergangsregelungen vorgesehen. Die BAIT kommen mit der Veröffentlichung sofort zur Anwendung.

Mit den MaRisk sind die BAIT über konkrete Hinweise auf Textziffern in den MaRisk verknüpft. Die in den MaRisk enthaltenen Vorgaben bleiben durch die BAIT unberührt und sind weiterhin umzusetzen. Sie werden allerdings im Rahmen ihres Gegenstandes weiter vertieft. So werden in der BAIT konkrete Anforderungen der Kreditinstitute an die IT in Bezug auf eine zu erstellende IT-Strategie definiert sowie die Themen Informationsrisikomanagement, Informationssicherheitsmanagement und Benutzerberechtigungsmanagement spezifiziert, wie sie in MaRisk nicht beschrieben sind. In diesem Sinne liefern die BAIT eine Konkretisierung der MaRisk und eine Erweiterung um die genannten Themen. Der Konkretisierung der MaRisk wird grundsätzlich Rechnung getragen durch die Referenzierung auf die MaRisk in der ersten Textziffer jedes Moduls.

Abbildung 2: Kontext der BAIT

§ 25a Absatz 1 KWG, § 25b KWG

↑ Präzisiert

BAIT

I. Vorbemerkung
II. Anforderungen
1. IT-Strategie
2. IT-Governance
3. Informationsrisikomanagement
4. Informationssicherheitsmanagement
5. Benutzerberechtigungsmanagement
6. IT-Projekte, Anwendungsentwicklung (inklusive durch Endbenutzer in den Fachbereichen)
7. IT-Betrieb (inklusiveDatensicherung)
8. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

↓ Konkretisiert

MaRisk

AT 1		Vorbemerkung
AT 2		Anwendungsbereich
	AT 2.1	Anwenderkreis
	AT 2.2	Risiken
	AT 2.3	Geschäfte
AT 3		Gesamtverantwortung der Geschäftsleitung
AT 4		Allgemeine Anforderungen an das Risikomanagement
	AT 4.1	Risikotragfähigkeit
	AT 4.2	Strategien
	AT 4.3	Internes Kontrollsystem
	AT 4.3.1	Aufbau- und Ablauforganisation
	AT 4.3.2	Risikosteuerungs- und Controllingprozesse
	AT 4.3.3	Stresstests
	AT 4.3.4	Datenmanagement, Datenqualität und Aggregation von Risikodaten
	AT 4.4	Besondere Funktionen
	AT 4.4.1	Risikocontrolling-Funktion
	AT 4.4.2	Compliance-Funktion
	AT 4.4.3	Interne Revision
	AT 4.5	Risikomanagement auf Gruppenebene
AT 5		Organisationsrichtlinien
AT 6		Dokumentation
AT 7		Ressourcen
	AT 7.1	Personal
	AT 7.2	Technisch-organisatorische Ausstattung
	AT 7.3	Notfallkonzept
AT 8		Anpassungsprozesse
	AT 8.1	Neu-Produkt-Prozess
	AT 8.2	Änderungen betrieblicher Prozesse oder Strukturen
	AT 8.3	Übernahmen und Fusionen
AT 9		Auslagerungen

Quelle: Essler, R./Paust, M., Seite 6 [10]

Die BAIT sind nunmehr der zentrale Baustein für die IT-Aufsicht im Bankensektor in Deutschland.

Sie richten sich primär an die Geschäftsleitung und zielen darauf,

- auf Grundlage des § 25a Absatz 1 KWG einen flexiblen und praxisnahen Rahmen für die Ausgestaltung der IT in den Instituten, insbesondere für das Management der IT-Prozesse und IT-Ressourcen sowie für das IT-Risikomanagement vorzugeben,
- das unternehmensweite IT-Risikobewusstsein im Institut und gegenüber Dienstleistern, an die Daten und Prozesse ausgelagert sind (Auslagerungsunternehmen), zu schärfen sowie
- die Erwartungshaltung der Aufsicht an die Institute transparenter zu gestalten.[9]

Die BAIT interpretieren – wie auch die MaRisk – die gesetzlichen Anforderungen des § 25a Absatz 1 Satz 3, 4 und 5 KWG (siehe Abbildung 2). Die Aufsicht erläutert in den BAIT – und auch in den MaRisk – was sie als Teil des Risikomanagements unter einer angemessenen technisch-organisatorischen Ausstattung der IT-Systeme unter besonderer Berücksichtigung der Anforderungen an die Informationssicherheit sowie eines angemessenen Notfallkonzepts versteht. Dabei werden die Anforderungen hinsichtlich der sicheren Ausgestaltung der IT-Systeme sowie zugehörigen IT-Prozesse („Integrität“, „Verfügbarkeit“, „Authentizität“ sowie „Vertraulichkeit“ der Daten) sowie die diesbezüglichen Anforderungen an die IT-Governance spezifiziert.

Da die Institute zunehmend IT-Services sowohl im Rahmen von Auslagerungen von IT-Dienstleistungen als auch durch den sonstigen Fremd-

9) Vgl. Essler, R./Paust, M. (2017): Konkretisierung der MaRisk durch ein Rundschreiben zu Bankaufsichtlichen Anforderungen an die IT (BAIT), 4. Informationsveranstaltung IT-Aufsicht bei Banken, Vortragsunterlage, Bonn; Kraus, A. U. (2017), ebenda.
10) Essler, R./ Paust, M. (2017), ebenda.

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH

bezug von IT-Dienstleistungen von Dritten beziehen, wird auch der § 25b KWG in diese Interpretation einbezogen und präzisiert. Schnittstellen zu den aufsichtsrechtlichen Anforderungen an Auslagerungen sind ebenfalls berücksichtigt.

Aus den BAIT ergeben sich für die Themen operative Anforderungen, Steuerung und Governance spezifische Handlungsfelder in insgesamt acht Themenbereichen (siehe Abbildung 3):[11]

- Textziffer 1-2: IT-Strategie,
- Textziffer 3-7 IT-Governance,
- Textziffer 8-14 Informationsrisikomanagement,
- Textziffer 15-22 Informationssicherheitsmanagement,
- Textziffer 23-30 Benutzerberechtigungsmanagement,
- Textziffer 31-44 IT-Projekte und Anwendungsentwicklung,
- Textziffer 45-51 IT-Betrieb (inklusive Datensicherung),
- Textziffer 52-56 Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen.

IT-Strategie

In der Textziffer 2 werden die absoluten Mindestinhalte der IT-Strategie vorgegeben. Dabei erfolgt eine grundsätzliche Orientierung an der Agenda der BAIT. Bei der Formulierung der IT-Strategie muss es sich um objektiv überprüfbare Kriterien handeln.[12]

Entsprechende Handlungsfelder sind unter anderem:

- Sicherstellung der Konsistenz der IT-Strategie mit der Geschäftsstrategie,
- Darstellung der strategischen Entwicklung der IT-Aufbau- und Ablauforganisation (IT-Prozesse) sowie der IT-Auslagerungsstrategie,
- Festlegung gängiger IT-Standards und Etablierung dieser in den IT-Prozessen und dem Informationssicherheitsmanagementsystem,[13]
- Festlegung der Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation (inklusive Commitment der Geschäftsführung zur Bedeutung der Informationssicherheit),
- Darstellung des Zielbilds der IT-Architektur in Form eines Überblicks über die IT-Anwendungslandschaft,
- Formulierung von Aussagen zum Notfallmanagement unter Berücksichtigung der IT-Belange sowie
- Formulierung von Aussagen zur Individuellen Datenverarbeitung (IDV, Hardware- und Softwarekomponenten).

IT-Governance

IT-Governance umfasst die Führung und die organisatorischen Strukturen und Prozesse, die sicherstellen, dass die Unternehmensziele durch den IT-Einsatz unterstützt und vorangetrieben werden. Kernelemente bei der IT-Governance sind die Sicherstellung der Funktionstrennung zur Vermeidung von Interessenkonflikten und die Festlegung und Implementierung von Richtlinien, Kriterien und Standards zur Entscheidungsfindung, Überwachung, Messung, Weiterentwicklung und Verbesserung der Leistung der IT und insbesondere auch für das Informationsrisiko- sowie Informationssicherheitsmanagement. Zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche durch die Geschäftsleitung sind angemessene quantitative oder qualitative Kriterien festzulegen und deren Einhaltung ist zu überwachen. Im Kontext der IT-Governance wird auf die Notwendigkeit einer quantitativ und qualitativ angemessenen Personalausstattung hingewiesen.

Entsprechende Handlungsfelder sind unter anderem:

- Festlegung IT-Aufbau- und IT-Ablauforganisation,
- Bestimmung IT-Risikosteuerungs- und IT-Controllingprozesse,
- Etablierung eines Informationssicherheitsmanagements,
- Gewährleistung einer quantitativ und qualitativ angemessenen Personalausstattung der IT und
- Sicherstellung einer angemessenen technisch-organisatorischen Ausstattung.

11) Vgl. Wöhler, J. (2017): Darstellung der sich ergebenden Handlungsfelder aus den neuen BAIT, in: Q_PERIOR Audit & Risk Newsletter 4/2017, Seite 20-22; auch Riediger, H. (2017): Aktuelle Entwicklungen und Inhalte der BAIT, in: Banken-Times Spezial, Sonderausgabe BAIT, Heidelberg; auch Glocker, A. (2018): BAIT 2017 – Herausforderung Informationssicherheit, Heidelberg.

12) Nach Riediger, H. (2017) ist das Fehlen solcher Kriterien einer der Hauptkritikpunkte in bankgeschäftlichen Prüfungen gemäß § 44 KWG.

13) Vgl. Wiesenmaier, M. (2017): BAIT-konforme Umsetzung von IT-Standards, in: Banken-Times Spezial IT/Orga, Heidelberg, Seite 54-55.

Abbildung 3: Themenbereiche der BAIT

Quelle: Chrubasik, Schütz, Elsbroek, Bank Management Consult

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH

Im Thema Informationsrisikomanagement ist insbesondere die Bedeutung der jeweiligen Fachabteilung als „Datenowner“ hervorzuheben.[14] Dies impliziert, dass die Fachabteilungen zwingend in das Informationsrisikomanagement einzubinden sind.

Management des Informationsrisikos

Der auch gegenüber den MaRisk neue Begriff Informationsverbund erweitert die Betrachtungsperspektive. Damit sind neben den geschäftsrelevanten Informationen ebenso die Geschäftsprozesse, IT-Systeme sowie Netz- und Gebäudeinfrastrukturen als Basis für die Aktivitäten der Schutzbedarfsfeststellung und für die Ableitung eines Sollmaßnahmenkatalogs zur Gewährleistung der Umsetzung der Schutzziele in den voneinander sauber abzugrenzenden Schutzbedarfskategorien anzusetzen.

Entsprechende Handlungsfelder sind unter anderem:

- Definition der mit dem Informationsrisikomanagement verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege,
- Einrichtung angemessener Risikosteuerungs- und -controllingprozesse (Risikoanalyse und Restrisikoüberwachung) sowie Berichtswege und Berichtspflichten,
- Gewährleistung einer angemessenen Interaktion mit und Übernahme in das Op-Risk-Management,
- Ermittlung des Schutzbedarfs für die Schutzziele Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität mittels Business-Impact-Analyse für die Geschäftsprozesse und mittels Schutzbedarfsanalyse für die IT-Anwendungen und -Systeme sowie
- Durchführung eines Abgleichs zwischen Sollmaßnahmen und den wirksam umgesetzten Maßnahmen (Ist) sowie gegebenenfalls Durchführung weiterer risikoreduzierender Maßnahmen.

Management der Informationssicherheit

Informationssicherheit wird explizit in Bezug auf die IT-Strategie thematisiert. Das Thema Informationssicherheitsmanagement beschreibt eine klassische Tätigkeit des Internen Kontrollsystems und fordert die Implementierung von Richtlinien und Konzepten, um die Ablauforganisation im IT-Bereich zu konkretisieren und die Überwachung auf Einhaltung der Vorgaben zu ermöglichen.

Entsprechende Handlungsfelder sind unter anderem:

- Beschluss und Implementierung einer Informationssicherheitsleitlinie,
- Etablierung der organisatorisch und prozessual unabhängigen Funktion des Informationssicherheitsbeauftragten und Institutionalisierung einer mindestens vierteljährlichen Berichterstattung an die Geschäftsleitung,
- Definition von Informationssicherheitsprozessen,
- Definition konkretisierender, den Stand der Technik berücksichtigender Informationssicherheitskonzepte,
- Etablierung angemessener Prozesse für Informationssicherheitsvorfälle sowie
- Sicherstellung quantitativ und qualitativ angemessener Personalressourcen.

Auf die Einrichtung der Funktion desInformationssicherheitsbeauftragten (ISB) sowie dessen Vertreter legt die Aufsicht besonderen Wert (Tz. 18) und stellt deutlich seine Aufgaben dar.[15] Der ISB unterstützt die Geschäftsführung beim sicheren Betrieb von IT und der Definition einer institutsspezifischen IT-Sicherheitsarchitektur. Der ISB ist eindeutig in der „2nd Line of Defense“ positioniert[16], gemäß Tz. 20 grundsätzlich nicht auslagerbar und unabhängig von der operationellen IT und Revision auszugestalten.

Die Aufsicht hat für regional tätige Institute sowie kleine Institute eine Öffnungsklausel geschaffen, nach der unter bestimmten Voraussetzungen die Funktion des ISB nicht zwingend im eigenen Haus vorgehalten werden muss und mehrere Institute einen gemeinsamen ISB bestellen.[17] In solchen Fällen ist allerdings in jedem Institut eine Ansprechperson für den ISB zu benennen.[18]

In bestimmten Fällen ist es möglich, einem Mitarbeiter mehrere Beauftragungsfunktionen (beispielsweise auch die des Datenschutzbeauftragten) zu übertragen, wenn potenzielle Interessenkonflikte vermieden werden.

Unter Umständen müssen die Organisationsrichtlinien angepasst werden, um eine Einbindung des ISB in die Themenfelder sicherzustellen, die nun explizit für seinen Wirkungsbereich definiert sind. Diese Felder sind mit den BAIT klar beschrieben und betreffen Aufgaben wie:

- Beratung der Geschäftsleitung in allen Fragen der Informationssicherheit,
- Erstellung von Leitlinien und Konzepten zur IT-Sicherheit sowie deren Überprüfung und Kontrolle,
- Steuerung des Informationssicherheitsprozesses im Institut sowie dessen Überwachung bei Dienstleistern,
- Feststellung und Untersuchung von Informationssicherheitsvorfällen,
- Durchführung von Sicherheitsaudits zur Erkennung von Schwachstellen,

14) Vgl. Riediger, H. (2017) ebenda.
15) Vgl. Bona-Stecki, M. (2017): Stellung des Informationssicherheitsbeauftragten, Heidelberg.
16) Vgl. Daumann, M. (2018): BAIT und Informationssicherheitsbeauftragter – Aufgabenverteilung und Begrifflichkeiten bei der Umsetzung, in: Die Bank 3/2018, Seite 18-19; auch Biona-Stecki, M. (2017); Wichtig ist in diesem Zusammenhang, die Aufgaben des ISB klar abzugrenzen von den Aufgaben der 1st LoD.
17) Vgl. Riediger, H. (2017) ebenda.
18) Vgl. Bona-Stecki, M. (2017) ebenda.

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH

- Initiierung und Überwachung von IT-Sicherheitsmaßnahmen,
- Initiierung und Koordination von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit sowie
- Ansprechpartner für Fragen der Informationssicherheit innerhalb des Instituts und für Dritte.

Der Funktion des ISB wird die Verantwortung für die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Instituts und gegenüber Dritten zugeschrieben. Für den Stelleninhaber ist die Übernahme dieser Funktion und damit die Verantwortung für ein breites Spektrum an Aufgaben eine große Herausforderung. Dabei sollen Prinzipien wie „Unabhängigkeit" und „Funktionstrennung" gewährleistet werden, um mögliche Interessenkonflikte zu vermeiden. Die Funktion des ISB ist aufbauorganisatorisch und prozessual unabhängig auszugestalten (Trennung von den Bereichen, die für den Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind) – und das bei einem umfangreichen und breiten Aufgabenkatalog mit hohen Kompetenzanforderungen.

Zur Ermittlung der quantitativen Angemessenheit der Funktion des ISB sind die Aufgaben unter Berücksichtigung der fachlichen Anforderungen gängiger Standards zu analysieren. Dazu gehören unter anderem die Feststellung der Anzahl der Mitarbeiter, der Grad der Heterogenität der IT-Landschaft und IT-Verfahren, der Anteil der IT-Anwendungen mit Schutzbedarf, der höher als normal eingestuft wird.

Bezüglich der qualitativen Angemessenheit muss der ISB über entsprechende Fachkenntnisse verfügen, insbesondere in den Bereichen IT, Compliance und Prozessmanagement, diese Kenntnisse immer auf dem neuesten Stand halten und auch ausgeprägte soziale Kompetenzen besitzen, um seine Aufgaben wahrnehmen zu können.[19]

Unabhängig von der Funktion des ISB verbleibt die Gesamtverantwortung für die Informationssicherheit bei der Geschäftsleitung.

Management der Benutzerberechtigung

Das Themenfeld Benutzerberechtigung ist deutlich umfangreicher und detaillierter als die entsprechenden Formulierungen in den MaRisk. Nun werden explizit (Soll-) Berechtigungskonzepte gefordert, die sich am vorab festgelegten Schutzbedarf zu orientieren haben, eine minimale Rechtevergabe und die Funktionstrennung weiterhin gewährleisten. Darüber hinaus sind Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen für Benutzer einzurichten, welche durch Genehmigungs- und Kontrollprozesse sicherstellen, dass die Vorgaben des Berechtigungskonzepts eingehalten werden. Eine übergeordnete Verantwortung für Prozesse zur Protokollierung von Berechtigungen muss erkennbar vorhanden sein.

Entsprechende Handlungsfelder sind unter anderem:

- Definition und Etablierung eines Benutzer- und Berechtigungsmanagements,
- Sicherstellung der Einhaltung der Vorgaben des IT-Berechtigungskonzepts durch Genehmigungs- und Kontrollprozesse für die Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von IT-Berechtigungen für Benutzer,
- Etablierung eines Re-Zertifizierungsprozesses zur Überprüfung, ob die eingeräumten IT-Berechtigungen weiterhin benötigt werden und ob diese den Vorgaben des IT-Berechtigungskonzepts entsprechen sowie
- Einrichtung angemessener Protokollierungsprozesse.

In Anlehnung an AT 8.2 der MaRisk rückt die Auswirkungsanalyse von IT-Projekten in den Vordergrund. Entsprechend fokussiert das Themenfeld IT-Projekte auf die Projektrisiken aus „Run-the-Bank"- und „Change-the-Bank"-Prozessen.

Zentrale Anforderungselemente sind die Qualitätssicherungs- sowie die Abnahme- und Freigabeprozesse.

IT-Projekte und Anwendungsentwicklung

Im Thema Anwendungsentwicklung werden Anforderungen für den gesamten Entwicklungsprozess formuliert und dabei auch die IDV berücksichtigt.

Entsprechende Handlungsfelder sind unter anderem:

- Festlegung einer Regelung der organisatorischen Grundlagen von IT-Projekten (inklusive Qualitätssicherungsmaßnahmen) und von Kriterien für deren Anwendung,
- Einrichtung einer angemessenen Steuerung von IT-Projekten unter Risikogesichtspunkten (Einzelprojektsteuerung),
- Einrichtung einer angemessenen Überwachung und Steuerung des Portfolios der IT-Projekte (Projekt-Portfoliosteuerung),
- Umsetzung einer regelmäßigen beziehungsweise anlassbezogenen Berichterstattung an die Geschäftsleitung über IT-Projekte und IT-Projektrisiken,
- Einrichtung eines angemessenen Anforderungsmanagements,
- Festlegung angemessener Prozesse und Verfahren für die sichere Anwendungsentwicklung,
- Sicherstellung der Schutzziele nach Produktivsetzung der entwickelten Anwendung,
- Sicherstellung einer angemessenen Versionierung,
- Durchführung angemessener Testverfahren vor Produktivsetzung (Testmanagement),

19) Vgl. Uribe, J. (2017): Coaching von IT- und Informationssicherheitsbeauftragten, Banken-Times Spezial IT/Orga, Heidelberg Seite 51-52.

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH

- Sicherstellung der Überwachung des Regelbetriebs nach Produktivsetzung,
- Etablierung eines angemessenen Verfahrens für die Klassifizierung/Kategorisierung (Schutzbedarfsklassen) sowie
- Formulierung einer IDV-Richtlinie.

IT-Betrieb inklusive Datensicherung

Der IT-Betrieb hat die Erfüllung der Anforderungen, die sich aus der Umsetzung der Geschäftsstrategie sowie den IT-unterstützten Prozessen ergeben, umzusetzen.

Entsprechende Handlungsfelder sind unter anderem:

- Gewährleistung einer angemessenen Verwaltung der Komponenten der IT-Systeme (Inventarisierung) sowie deren Beziehungen zueinander (IT-Landkarte und Datenflüsse),
- Sicherstellung einer angemessenen Steuerung des Portfolios der IT-Systeme,
- Ausgestaltung und Umsetzung der Prozesse zur Änderung von IT-Systemen in Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt,
- Konzipierung und Sicherstellung eines geordneten Prozesses zur Aufnahme, Dokumentation, Bewertung (im Hinblick auf mögliche Umsetzungsrisiken), Priorisierung, Genehmigung sowie Koordination und sicheren Umsetzung von Anträgen zur Änderung von IT-Systemen (Change-Management),
- Einrichtung eines Prozesses zur Erfassung, Bewertung, Priorisierung (hinsichtlich möglicherweise resultierender Risiken) und gegebenenfalls Eskalation von Meldungen über ungeplante Abweichungen vom Regelbetrieb (Störungen) und deren Ursachen (Incident-Management) sowie
- Umsetzung eines Datensicherungskonzepts zur Regelung von Vorgaben für die Verfahren zur Datensicherung sowie regelmäßige Überprüfung und gegebenenfalls Anpassung seiner Effektivität.

Auslagerungen und sonstiger Fremdbezug

Durch die BAIT nähern sich die Vorgaben zum sonstigen Fremdbezug von IT-Dienstleistungen den Vorgaben an Auslagerungen in den MaRisk AT 9. Insbesondere im Hinblick auf Risiken, die auf (externe) Dienstleister zurückzuführen sind, stellen die BAIT die gleich hohen Anforderungen an die Steuerung des sogenannten Fremdbezugs von IT-Dienstleistungen wie an Auslagerungen.[20] Insoweit sind Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen nicht „schwarz" oder „weiß", sondern Hilfsmittel bei der Frage, wie tiefgehend man den Fremdbezug zu analysieren hat.[21]

In jedem Fall ist wegen der grundlegenden Bedeutung der IT für das Institut vorab eine Risikobewertung – auch für den sonstigen Fremdbezug von IT-Dienstleistungen – durchzuführen, deren Ergebnis maßgeblich für die Überwachung der vom Dienstleister zu erbringenden Leistung ist. Durch die gesamthafte Betrachtung können die vollständige Risikosituation für das Institut ermittelt und Konzentrationsrisiken bei IT-Dienstleistungen erkannt werden sowie die aus der Risikoanalyse abgeleiteten Maßnahmen angemessen in der Vertragsgestaltung berücksichtigt werden.[22]

In den BAIT werden Anforderungen an jeglichen Fremdbezug von IT-Dienstleistungen gestellt, unabhängig davon, welchen Umfang dieser ausmacht und welchem Einsatzzweck im Institut dieser zugrunde liegt. Die BAIT formulieren Anforderungen an den sonstigen Fremdbezug von IT-Dienstleistungen, ohne aber das den MaRisk zugrunde liegende Proportionalitätsprinzip umfassend zu berücksichtigen.

Nach den BAIT umfassen IT-Dienstleistungen alle Ausprägungen des Bezugs von IT, dazu zählen insbesondere die Bereitstellung von IT-Systemen, Projekte/Gewerke oder Personalgestellung (BAIT Tz. 52).

Die Auslagerungen der IT-Dienstleistungen haben die Anforderungen nach AT 9 der MaRisk zu erfüllen. Dies gilt nach den BAIT (Tz. 52) auch für:

- Auslagerungen von IT-Dienstleistungen, die dem Institut durch ein Dienstleistungsunternehmen über ein Netz bereitgestellt werden (zum Beispiel Rechenleistung, Speicherplatz, Plattformen oder Software) und
- deren Angebot, Nutzung und Abrechnung dynamisch und an den Bedarf angepasst über definierte technische Schnittstellen sowie Protokolle erfolgen (Cloud-Dienstleistungen).

Bei jedem Bezug von Software sind nach den MaRisk die damit verbundenen Risiken angemessen zu bewerten (AT 7.2 Tz. 4). Ebenso muss vor jedem sonstigen Fremdbezug von IT-Dienstleistungen eine Risikobewertung durchgeführt werden. Sie kann unter Rückgriff auf das Proportionalitätsprinzip in Art und Umfang institutsindividuell festgelegt werden (BAIT Tz. 53). Dabei sind die für Informationssicherheit und Notfallmanagement des Instituts verantwortlichen Funktionen angemessen einzubinden.

Entscheidet sich ein Institut, Software und IT-Betrieb vom selben IT-Dienstleister zu beziehen, so konzentrieren sich dort die IT-Risiken. Umso dringlicher ist es in dem Fall, den Dienstleister wirksam zu steuern. Damit muss das Institut auch über

20) Zu Auslagerungen in der Kreditwirtschaft im Kontext der MaRisk siehe Chrubasik, B./Schütz, A. (2018): Auslagerungen in der Kreditwirtschaft – Aufsichtsrechtliche Anforderungen, Institutsspezifische Herausforderungen, Praxisbezogene Umsetzungshilfen, Göttingen.
21) Vgl. Kühn, R. (2017): Prüfung von Softwarebezügen im Licht der neuen MaRisk und BAIT, in: Banken-Times Spezial, Sonderausgabe BAIT, Heidelberg.
22) Vgl. Essler, R./Gampe, J. (2018) ebenda.

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH

den Sachverstand verfügen, der es in die Lage versetzt, die IT-Risikoberichte des Dienstleisters nachvollziehen und gegebenenfalls reagieren zu können.

Im Rahmen der Auslagerung von sonstigem Fremdbezug von IT-Dienstleistungen ist darüber hinaus sofort auch sicherzustellen, dass:

- die Auslagerung im Einklang mit den Strategien unter Beachtung der Risikobewertung gesteuert wird (BAIT Tz. 54),
- eine vollständige, strukturierte Vertragsübersicht vorgehalten wird (BAIT Tz. 54 Erläuterungen),
- die Leistungserbringung entsprechend der Risikobewertung angemessen überwacht wird. Hierzu können die institutsinternen Steuerungsmechanismen genutzt werden und kann die Steuerung auf der Basis einer Bündelung der Verträge (Vertragsportfolio) erfolgen (BAIT Tz. 54),
- die aus der Risikobewertung abgeleiteten Maßnahmen angemessen in der Vertragsgestaltung berücksichtigt sind (BAIT Tz. 55). Dies umfasst Vereinbarungen zum Informationsrisikomanagement, zur Informationssicherheit und zum Notfallmanagement, die im Regelfall den Zielvorgaben des Instituts entsprechen,
- die vom Institut akzeptierten und genehmigten Restrisiken überwacht und in den Prozess des Managements der operationellen Risiken überführt werden (BAIT Tz. 55),
- bei Relevanz die Möglichkeit eines Ausfalls des Dienstleisters berücksichtigt und diesbezügliche Exit- und Alternativstrategien entwickelt und dokumentiert werden (BAIT Tz. 55) sowie
- die Risikobewertungen regelmäßig und anlassbezogen überprüft und gegebenenfalls inklusive der Vertragsinhalte angepasst werden (BAIT Tz. 56).[23]

Die Vorgaben aus BAIT Tz. 55 gelten auch im Fall der Einbindung von Subunternehmern.

Neben den Anforderungen im Themenfeld Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen sind weitere auslagerungsrelevante Vorgaben auch in den Themenfeldern IT-Strategie und Informationssicherheitsmanagement aufgeführt. So ist vom Institut

- eine IT-Strategie festzulegen und darin unter anderem Aussagen zur strategischen Entwicklung der Auslagerung von IT-Dienstleistungen zu formulieren (Tz. 2),
- ein Informationssicherheitsbeauftragter zu institutionalisieren, der unter anderem die Aufgabe hat, den Informationssicherheitsprozess im Institut zu steuern und zu koordinieren sowie diesen gegenüber den IT-Dienstleistern zu überwachen (Tz. 18) – bei kleinen beziehungsweise regional tätigen Instituten sind dabei Sonderregelungen möglich (Tz. 20) – und
- die IT-Dienstleister zur sofortigen und umfassenden Unterrichtung des Informationssicherheitsbeauftragten über alle bekannt gewordenen IT-sicherheitsrelevanten Sachverhalte zu verpflichten, die das Institut betreffen (Tz. 19).

BAIT im Kontext der digitalen Transformation

Die in den BAIT konkretisierten Themenbereiche sind nach Regelungstiefe und -umfang nicht abschließender Natur. Jedes Institut bleibt folglich auch insbesondere jenseits der Konkretisierungen der BAIT gemäß § 25a Absatz 1 Nr. 4 KWG in Verbindung mit AT 7.2 Tz. 2 MaRisk verpflichtet, bei der Ausgestaltung der IT-Systeme und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards und grundsätzlich auf den Stand der Technik abzustellen. Dies gilt insbesondere vor dem Hintergrund der anhaltenden und fortschreitenden digitalen Transformationen. Institute, die sich jenseits der Digitalisierung (Implementierung digitaler Technologien in aktuelle Prozesse) mit neuen Geschäftsmodellen sowie innovativen Aufbau- und Ablaufstrukturen befassen (digitale Transformation) sollten ihre Herausforderungen bei der Umsetzung der BAIT kennen. Die folgende Aufzählung beschreibt die dringlichen.

- Die IT-Strategie und die daraus abgeleiteten, weiterführenden Dokumente sollten eindeutige Aussagen und Rahmenbedingungen beschreiben, wo, wie, warum und in welcher Fertigungstiefe sogenannte Cloud-Solutions in die IT-Architektur der Institute Einzug halten und inwieweit diese die Business Strategie unterstützen,
- umfangreiche Installierung eines Master Data Managements unter Berücksichtigung der IT-Architektur sowie länderspezifischer Datenschutzverordnungen (insbesondere im Kontext internationaler Geschäftsmodelle).
- Die „sinnvolle“ Etablierung von aufsichtsrechtlich notwendigen Prozessen und Strukturen bei gleichzeitiger Implementierung notwendiger innovativer Methoden, um weiterhin als Unternehmen agil am Markt agieren zu können.
- Die Implementierung eines quantitativ und qualitativ angemessenen IT-Betriebs vor dem Hintergrund geforderter digitaler Kostensynergien.
- Die Umsetzung der BAIT in das Auslagerungsmanagement (im weiteren Sinne) des Instituts von der Auslagerungsinitiierung über die Auslagerungssteuerung bis zur Auslagerungsbeendigung, inklusive der Auswirkungen auf die Risikoanalyse.

Auswirkungen und Trends

Der aufsichtsrechtliche Druck auf Kreditinstitute im Bereich der IT wird sich durch die BAIT weiter erhöhen. Zusammen mit den MaRisk sind neue Anforderungen an die IT entstanden,

23) Vgl. BaFin (2017) ebenda; auch Wöhler, J. (2017) ebenda sowie S&P Unternehmensberatung (2017): BAIT veröffentlicht – das Wichtigste auf einen Blick, München.

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH

die durch entsprechende technische und organisatorische Maßnahmen von neu zu definierenden Verantwortlichen umzusetzen sind.

Die Bundesanstalt für Finanzdienstleistungsaufsicht spezifiziert mit den BAIT lange geforderte Standards zur IT-Strategie und dem Informationsrisikomanagement. Vor allem die IT-Strategie ist als wesentlich neuer Bestandteil anzusehen, der durch BAIT erstmalig umfangreich präzisiert wird.

Um den neu definierten Anforderungen der IT-Strategie gerecht zu werden, wird es für viele Banken notwendig sein, die IT-Architekturen und damit auch die IT-Infrastrukturen in zahlreichen Gesichtspunkten zu modernisieren. Möglicherweise wird sich der Trend des IT-Outsourcings durch die neuen Voraussetzungen an die IT-Sicherheit weiter verstärken, da die bankinterne IT den steigenden Vorgaben ohne entsprechende Veränderungen vermutlich nicht entsprechen kann. Die bereits vorherrschenden Trends wie Cloud, SaaS („Software as a Service"), IaaS („Infrastructure as a Service"), PaaS („Platform as a Service") und die damit einhergehende vielseitige Flexibilisierung in der Ausgestaltung werden weiter an Bedeutung gewinnen.[24]

Des Weiteren sind Prozesse und Standards zur Umsetzung der IT-Strategie anzupassen beziehungsweise neu zu implementieren. Dies wird für die Banken nur durch die Schaffung neuer Verantwortlichkeiten in Bezug auf die IT-Sicherheit und der Erhöhung des IT-Budgets zu gewährleisten sein.

Aufgrund der Interdependenzen der BAIT zu den MaRisk-Neuerungen aus der 5. Novelle, beispielsweise in den Themenfeldern Auslagerungen und Risikoreporting, ist es zwingend, die neuen IT-Anforderungen aus den MaRisk und den BAIT gesamthaft zu betrachten und zu bewerten.[25] Bei der Umsetzung einzelner Handlungsfelder sind die Fachbereiche als wichtige Stakeholder zwingend einzubinden. Letztlich sind sie Nutzer beziehungsweise Eigentümer der Daten und betreiben in vielen Instituten dezentrale IT-Applikationen und IDV.

Die modulare Struktur der BAIT gibt der Aufsicht die notwendige Flexibilität für weitere inhaltliche Anpassungen oder Ergänzungen. Derzeit sind beispielsweise Themen wie Cybersicherheit, IT-Notfallmanagement und spezielle Vorgaben des BSI-Gesetzes (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) in der aktuellen Diskussion und Prüfung hinsichtlich einer Aufnahme in das Gesamtwerk.[26] ◄

24) Vgl. Schöbe, K./Endres, T (2016): Bankaufsichtliche Anforderungen an die IT (BAIT), in: Q_PERIOR Audit & Risk Newsletter 3/2016, Seite 8-13.
25) Zu den MaRisk 6.0 siehe Chrubasik, B./Schütz, A. (2018), ebenda.
26) Essler, R./Gampe, J. (2018) ebenda.

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH