Matthias Döring / Frank-Michael Manneck

BAIT in der Praxis – Herausforderungen für die IT in Banken

Mit den neuen bankaufsichtlichen Anforderungen an die IT (BAIT)[1] ergänzt die BaFin ihre Anforderungen an die IT der Institute nach §25a Abs. 1 und §25b KWG um ein zusätzliches Rundschreiben zur Konkretisierung der MaRisk[2]. Nach der Anfang des Jahres zwischen Februar und Mai durchgeführten Konsultationsphase folgte die finale Veröffentlichung der BAIT am 3. November 2017 bezugnehmend auf die unmittelbar zuvor erfolgte Veröffentlichung der neuen MaRisk.

Die Inhalte: breites Spektrum und hoher Anspruch

Die Ergänzung der MaRisk wurde notwendig, nachdem diese in der neuen Fassung zwar Anknüpfungspunkte an typische IT-Themen und -Prozesse bietet, genauere Details, wie diese auszugestalten sind, aber offenlässt. Des Weiteren bereitet die BaFin mit der Veröffentlichung der BAIT den Boden zur Umsetzung der ebenfalls 2017 veröffentlichten Leitlinien der EBA[3] zur Überprüfung und Bewertung der informations- und kommunikationstechnologischen Risiken der Institute durch die nationalen Behörden. Diese Leitlinien sind von den nationalen Aufsichten ab dem 1. Januar 2018 anzuwenden.

Die bankaufsichtlichen Anforderungen stellen, wie die MaRisk auch, eine Mindestanforderung für alle Institute dar. Unter Berücksichtigung des Proportionalitätsprinzips ist die Anwendung unmittelbar von allen Instituten verbindlich anzuwenden und sollen in allen zukünftigen IT-Prüfungen der Aufsicht Berücksichtigung finden. Die BAIT sind in acht Kapitel beziehungsweise Themen unterteilt:

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 (inklusive Datensicherung)
8. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

Dr. Matthias Döring, Senior Manager, d-fine GmbH, Frankfurt am Main, und Frank-Michael Manneck, Abteilungsleiter Non-Financial Risk, VÖB-Service GmbH, Bonn

Dass die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten der Informationsverarbeitung, wie die Autoren den Begriff des Informationsverbunds umschreiben, in der aufsichtlichen Praxis den heutigen Stellenwert einnimmt, dürften vor rund zehn Jahren nur wenige Experten vorausgesehen haben. Doch mit der Aufarbeitung der Ursachen der Finanzkrise und der gleichzeitigen Aufwertung der Banktechnik als wichtiger Wettbewerbsfaktor der Branche gilt es auch die in der IT-Technik schlummernden Gefahren im Auge zu behalten. Das Informationsrisikomanagement wird damit zu einer wichtigen Stellschraube einer guten Unternehmenssteuerung und hat für die hiesige Bankenaufsicht inzwischen den gleichen Stellenwert wie die Ausstattung der Institute mit Kapital und Liquidität. So jedenfalls hat es die BaFin Anfang November auf ihrer Homepage anlässlich der Veröffentlichung der Bankaufsichtlichen Anforderungen an die IT kommuniziert. (Red.)

Schon an Hand der Kapitelstruktur ist zu erkennen, dass die BAIT ein breites Spektrum an Themenfeldern ansprechen. Dementsprechend viele Organisationseinheiten in der IT sind betroffen. Und auch jenseits des IT-Bereichs wirken sich die BAIT auf die Fachbereiche (insbesondere wegen Kapitel 5 und 6), IT-Dienstleister (Kapitel 8) und die gesamte Geschäftsleitung des Instituts aus.

Verantwortung der gesamten Geschäftsleitung

Auf die Verantwortung der gesamten Geschäftsleitung (nicht nur des Geschäftsleiters IT) für die IT legt die BaFin außerordentlichen Wert. Zur Wahrnehmung dieser Verantwortung fordern die BAIT zum Beispiel regelmäßige Berichtspflichten des Informationssicherheitsbeauftragten an die Geschäftsleitung ein. Außerdem müssen die Ziele der Geschäftsleitung bezüglich der BAIT-Themen nachhaltig verfolgt werden. Dazu ist insbesondere die Erreichung der ausgegebenen Ziele turnusmäßig zu überwachen.

Strategie und Governance bilden für die Geschäftsleitung die notwendige Klammer, um ihre Vorgaben bezüglich des Umgangs mit IT-Risiken zu kommunizieren und verfolgen zu können. Dabei umfassen IT- und Informationssicherheitsrisiken alle Arten von Risiken, welche mit der Nutzung von Informationstechnologie oder dem Lebenszyklus der IT-Produkte (das heißt der Entwicklung, der Beschaffung, dem Betrieb) in Verbindung stehen.

Dies gilt insbesondere, wenn die Risiken auf externe Dienstleister zurückzuführen sind. So stellen die BAIT die gleich hohen Anforderungen an die Steuerung des sogenannten sonstigen Fremdbezugs von IT-Dienstleistungen wie an Auslagerungen.

Unter sonstigem Fremdbezug sind auch die Verwendung von Fremdsoftware und die Gestellung von externem Personal zu verstehen.

Neben der Breite des Spektrums an Themen ist auch die Tiefe der Anforderungen an einzelne Prozesse bemerkenswert. Zum Beispiel wird für das Informationssicherheitsmanagement gefordert, dass es nicht nur die Stufen der Planung, Umsetzung und Erfolgskontrolle beinhalten möge, sondern auch die der Optimierung und Verbesserung der Informationssicherheit berücksichtigen soll. Damit wird der in guten Praktiken höchstmögliche Reifegrad eines Prozesses zur Minimalanforderung an alle Banken (vergleiche zum Beispiel Reifegradmodelle nach COBIT, CMMI).

Ähnlich verhält es sich mit den Anforderungen an die Vergabe und Verwaltung von Benutzerrechten, welche grundsätzlich so sparsam wie möglich vergeben werden sollen. Jeder Mitarbeiter der Bank soll also nur über diejenigen Berechtigungen verfügen, die für die tägliche Arbeit unbedingt erforderlich sind.

Die ersten Schritte zur BAIT-konformen Bank

Die BAIT sind ab sofort für alle Banken in Deutschland ohne Übergangsfrist verbindlich zu beachten. Die Ausgangslage der Institute ist dabei sehr unterschiedlich. Während die von der EZB beaufsichtigten Institute gute Praktiken zur IT-Governance und gängige Standards zur IT-Sicherheit bereits umfassend im Einsatz haben und zum Teil noch mit der Verarbeitung von Feststellungen der letzten großen IT-Prüfungen beschäftigt sind, haben sich kleinere Institute mit dem Thema IT-Sicherheit eher wenig auseinandergesetzt und durften sich bisher auf ihre Dienstleister verlassen.

Für große Institute lohnt es sich, die BAIT unter zwei Gesichtspunkten zu betrachten. Einerseits stellen die BAIT sehr spezielle oder auch hohe Forderungen auf. So werden zum Beispiel bestimmte Mindestinhalte der IT-Strategie explizit genannt, mit denen sich das Institut auseinandersetzen muss (unter anderem zur strategischen Entwicklung der Aufbau- und Ablauforganisation, zur IT-Architektur und zum Notfallmanagement). Andererseits gibt die BAIT durch Fokussierung auf bestimmte Themen eine Indikation, mit welchen Prüfungsinhalten zukünftig konkret zu rechnen sein wird. In der Regel haben diese Institute bereits begonnen zu eruieren, welche Aspekte tatsächlich für sie neu sind oder prioritär angegangen werden sollten. Die Ergebnisse dieser Überlegungen werden in der Regel als neue oder neu priorisierte Anforderungen in laufenden Initiativen verortet und gelöst.

Konformität mit den BAIT erreichen und erhalten

Kleinere Institute greifen wegen des Umfangs der Anforderungen bereits für eine erste Selbsteinschätzung auf ihre Verbundstrukturen oder Berater zur Unterstützung zurück. In der Folge wird es für diese Institute entscheidend sein, inwiefern insbesondere auch die kommerziellen Anbieter von Software zur Verwaltung von Benutzerrechten und Dienstleisterverträgen mit ihren Produkten Lösungen für die erkannten Schwachstellen anbieten. In jedem Fall empfiehlt sich unabhängig von der Größe des Instituts die Ermittlung des Erfüllungsgrades der Anforderungen der BAIT im Rahmen eines Assessments.

Um Konformität mit den BAIT zu erreichen und diese dauerhaft zu erhalten, müssen die Institute einige schwierige Fragestellungen lösen. Dies wird an den folgenden Beispielen verdeutlicht. Die BAIT fordern unter anderem die Einrichtung und den Betrieb eines Informationsrisikomanagements (Kapitel 3).

Der erste Schritt bei jeder Art von Risikomanagement besteht in der Risikoinventur beziehungsweise der Identifikation der relevanten Risiken. Dies setzt voraus beziehungsweise beinhaltet eine möglichst vollständige Erfassung des Inventars von unter Risikogesichtspunkten zu behandelnden Dingen, die es im Unternehmen gibt. Im Fall informationstechnologischer Risiken sind dies unter anderem die Organisation, Personal, Hardware, Software, Dienstleisterverträge, Nutzerberechtigungen. In der Informationssicherheit wird dieses Inventar häufig als Informationsverbund bezeichnet. Der Informationsverbund umfasst die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten der Informationsverarbeitung.

Für die meisten Unternehmen besteht bereits in dem Aufbau und der Pflege des Informationsverbundes die allergrößte Herausforderung zur faktischen Erreichung der BAIT-Konformität. Eine Reihe von Gründen lassen sich hierfür als Ursache nennen.

Gängige Standards der Informationssicherheit

So ist zunächst nicht klar, in welches Modell sich die Bestandteile des Informationsverbundes einbetten sollten: Soll zum Beispiel eine Anwendung, welche auf einen Einzelvertrag mit einem Hersteller basiert, als ein Objekt betrachtet werden oder sollen Client- und Server-Komponenten, Front- und Backend, oder sogar einzelne Funktionskomponenten der Anwendung separat betrachtet werden? In welcher Weise stehen Hardware, Software, Cloud und durch Endbenutzer erstellte und betriebene Anwendungen zueinander in Beziehung?

Ist das Modell des Informationsverbundes dann erst einmal festgelegt, ist es im laufenden Betrieb so mit Daten zu bewirtschaften, dass immer ein möglichst vollständiger, aktueller Überblick über den Informationsverbund besteht. Zu guter Letzt machen es neue technologische Entwicklungen wie zum Beispiel Cloud oder Bitcoin erforderlich, das Informationsverbundmodell einem Lebenszyklus zu unterwerfen und regelmäßig zu erweitern oder anzupassen. Zum Glück für die Institute gibt es gängige Standards der Informationssicherheit, welche Vorschläge zur Modellierung auf Basis des aktuellen Stands der Technik machen und auch im Laufe der Zeit weiterentwickelt werden. Ein Beispiel sind die Schichtenmodelle des IT-Grundschutzes des BSI.[4)]

Koordiniert zur Konsistenz der Dokumentationslandschaft

Aktuell beschreiten die meisten Institute den Weg, die Modelle der gängigen Standards anzuwenden beziehungsweise die jüngsten Aktualisierungen aus diesen zu übernehmen. Dieses Vorgehen ist von der BaFin explizit gewünscht. Die Institute sollen sich an gängigen Standards orientieren und sich dazu auch in ihrer IT-Strategie äußern. Die BaFin erfindet die Informationssicherheit also nicht grundsätzlich neu. Dies lässt sich auch daran erkennen, dass viele der Anforderungen, Begriffe und Formulierungen in den BAIT aus gängigen Standards entlehnt sind.

Eine weitere nicht zu unterschätzende Aufgabe besteht in dem Umfang an Dokumentation, den Abhängigkeiten zwischen den Dokumenten und den unterschiedlichen Beteiligten, die an der Erstellung und Pflege oder als Verantwortliche mitwirken.

Unter anderem soll die IT-Strategie konform zur Geschäftsstrategie sein. Darauf aufbauend ist eine Informationssicherheitsleitlinie zu erstellen, welche ihrerseits konform zu den Strategien sein soll. Für bestimmte Bereiche sollen darüber hinaus konkretisierende Informationssicherheitsrichtlinien auf Basis der Informationssicherheitsleitlinie definiert werden. Die Liste der Dokumente und ihrer Abhängigkeiten, welche die BAIT fordern, ließe sich noch fortsetzen.

Neben dem reinen Aufwand ist vor allem die Zeitdauer zu berücksichtigen, die mit der Erstellung und Pflege dieser Dokumente verbunden ist. Änderungen, welche sich aufgrund neuer Erkenntnisse ergeben, müssen in konsistenter Weise in die Dokumentationslandschaft eingearbeitet werden. Dies erfordert intensive Abstimmungen zwischen allen Beteiligten. Eine in sich konsistente Dokumentationslandschaft zu einem Prüfungstermin vorlegen zu können und gleichzeitig bereits die neuesten Entwicklungen ins Auge zu fassen, ist schwer. Diesem Umstand kann durch Transparenz über die Abhängigkeiten und eine übergreifende, sorgfältige Planung anstehender Änderungsbedarfe und Meilensteine begegnet werden.

Überarbeitung der Dienstleisterverträge

Als letztes Beispiel der zu erledigenden Punkte auf der Agenda der BAIT sei die Überarbeitung der IT-Dienstleisterverträge genannt. Kaum ein Institut wird bezüglich dieses Punktes bereits heute BAIT-konform sein.

Neben den klassischen Auslagerungen zentraler Funktionen ist gefordert, auch den sonstigen Fremdbezug von IT-Dienstleistungen wie zum Beispiel die Stellung von Personal oder die Erstellung von Gewerken im Rahmen von IT-Projekten einer regelmäßigen Risikobewertung zu unterziehen. Daraus resultierende Maßnahmen können zu Anpassungsbedarfen an den Dienstleisterverträgen führen.

Bei der erstmaligen Umsetzung von Kapitel 8 der BAIT sind daher alle IT-Dienstleister festzustellen, deren Risiko zu bewerten, bestehende Verträge zu sichten und notwendige Anpassungsbedarfe mit den Dienstleistern zu verhandeln. Falls erforderlich sind Verträge auch gänzlich neu aufzusetzen.

Orientierung an guten Praktiken

Bei der Risikobewertung von Dienstleistern können zum Beispiel die Abhängigkeit vom Dienstleister und ein potenzieller Know-how-Verlust des eigenen Unternehmens als Kriterien berücksichtigt werden. Diskutiert werden kann, inwiefern das Risiko des Wegfalls eines Personaldienstleisters über das Risiko des Ausfalls der eigenen Mitarbeiter hinausgeht. Diese und vergleichbare Fragestellungen werden die Institute heute und auch in Zukunft immer wieder beschäftigen.

Mit den BAIT hat sich die BaFin dazu bekannt, dass sie die Informationstechnologie nicht nur als Segen für das Geschäft der Banken, sondern auch als eine Bedrohung für die Tätigkeit der einzelnen Institute ansieht, welcher durch entsprechende Strukturen und Abläufe in den Instituten begegnet werden sollte.

Mit den meisten der in der BAIT genannten Anforderungen hebt die BaFin bestimmte Aspekte hervor, welche sich in den IT-Bereichen der Unternehmen auch jenseits des Bankensektors bewährt haben. Diese guten Praktiken findet man in einschlägigen Rahmenwerken und Standards wieder. An einigen Stellen gehen die Anforderungen jedoch auch über gute Praktiken und gängige Standards der IT hinaus, zum Beispiel was den Umgang mit den von Fachbereichen selbst erstellten und betriebenen Anwendungen betrifft.

Aktuell sind die meisten Institute noch damit beschäftigt, die Inhalte der BAIT und deren Auswirkungen auf die eigene Organisation möglichst schnell einzuschätzen und zu analysieren. In der Folge sind einige komplexe Fragestellungen zu bearbeiten. Institute, welche sich bereits an guten Praktiken und gängigen Standards in der IT orientieren, sollten dabei gut aufgestellt sein.

Novellierungen schon absehbar

Aufgrund zu erwartender neuer technologischer Innovationen, weiterer Erkenntnisse aus der Prüfungspraxis und der Einbettung in den Kontext aus sich verändernden nationalen und europäischen Gesetzen und Verordnungen wird es für die gerade neu erschaffene BAIT in der Zukunft einige Novellierungen geben.

Ein besonderes Augenmerk wird darauf zu richten sein, welchen Schutz die BAIT in der Praxis tatsächlich bieten. Größte Auswirkungen auf die BAIT würde es bei schweren, möglicherweise öffentlichkeitwirksamen Vorfällen auf Grund unzureichender Vorgaben geben. Ob es dazu kommt, bleibt abzuwarten.

Fußnoten

1) BaFin, Rundschreiben 10/2017 (BA) vom 3. November 2017, „Bankaufsichtliche Anforderungen an die IT (BAIT)"
2) BaFin, Rundschreiben 09/2017 (BA) vom 27. Oktober 2017, „Mindestanforderungen an das Risikomanagement – MaRisk"
3) European Banking Association (EBA), EBA/GL/2017/05, „Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP)"
4) Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz: www.bsi.bund.de