BCG

THE BOSTON CONSULTING GROUP

Working Paper - Diskussionsstand

Diskussionspapier BAIT: "Bankaufsichtliche Anforderungen an die IT"

Dr. Walter Bohmayr (VIE)

Marc Papritz (DUS)

Dr. Christian Schmid (MUN)

Jannik Leiendecker (MUN)

Dezember 2017

Die am 7. November 2017 durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) veröffentlichten und ohne Übergangsfrist gültigen "Bankaufsichtlichen Anforderungen an die IT" (BAIT) führen als "zentraler Baustein für die IT-Aufsicht über den Bankensektor"[1] zu Handlungsbedarf bei Instituten in Deutschland. Die BaFin kann jederzeit Maßnahmen zur Erfüllung der BAIT anordnen; bei Nichtumsetzung drohen in letzter Konsequenz rechtliche Folgen für die Geschäftsleitung.[2] Da die IT systemrelevanter Banken in Deutschland bereits seit 2016 im Fokus von Prüfungen durch die Europäische Zentralbank (EZB), die Bundesbank sowie die BaFin steht, ist die praktische Relevanz der BAIT sehr hoch.[3] Die BAIT haben damit Gültigkeit zusätzlich zu den bestehenden Standards zur Informationssicherheit, beispielsweise der Bank for International Settlements (BIS), der Society for Worldwide Interbank Financial Telecommunication (SWIFT) sowie der Datenschutzgrund-Verordnung der EU (DSGVO) oder des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (siehe auch Abbildung 1).

"IT-Governance und Informationssicherheit [sind] keine Randthemen mehr, sondern haben auch für die Aufsicht inzwischen den gleichen Stellenwert wie die Ausstattung der Institute mit Kapital und Liquidität." (BaFin-Rundschreiben 10/2017)

Die BAIT konkretisieren die "Mindestanforderungen an das Risikomanagement" (MaRisk)[4] im Hinblick auf die sichere und angemessene technisch-organisatorische Ausgestaltung der IT-Systeme, dazugehörige Prozesse sowie Anforderungen an die IT-Steuerung in acht Themenfeldern. In einem bereits anspruchsvollen Marktumfeld richten sich die BAIT auf zwei Arten an den CIO: Bei den Themenfeldern IT-Strategie, IT-Governance, IT-Projekte und Anwendungsentwicklung sowie IT-Betrieb verantwortet der CIO die Ausgestaltung notwendiger Maßnahmen sowie deren Umsetzung. Die Themenfelder Informationsrisikomanagement, Informationssicherheitsmanagement, Benutzerberechtigungsmanagement und Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen sind von übergreifender Natur. Die IT-seitige operative Umsetzung wird durch die CIO-Bereiche sichergestellt (Abschnitt 1 des vorliegenden Dokuments).

[1] "BAIT: BaFin veröffentlicht Anforderungen an die IT von Banken", Meldung der BaFin.
[2] Nach § 25a Absatz 1 Satz 3 Nummer 4 und 5 sowie § 25b KWG.
[3] Siehe auch Boersen-Zeitung.de, "EZB durchleuchtet IT großer Banken", 06.12.2016.
[4] Analog zu MaRisk basierend auf § 25a Absatz 1 Satz 3 Nummer 4 und 5 sowie § 25b KWG.

Bei der Umsetzung der Anforderungen können innovative technologische und organisatorische Maßnahmen einen Beitrag leisten (Abschnitt 2); die bankweite Compliance mit den BAIT kann entlang fünf konkreter Schritte sichergestellt werden (Abschnitt 3).

Abbildung 1

1. Neue Anforderungen an den CIO

Neben Aufgabenstellungen aus den BAIT, deren Ausgestaltung und Umsetzung direkt durch den CIO verantwortet werden, ist die Bindung zusätzlicher Ressourcen der CIO-Bereiche durch die (anteilige) operative Umsetzung weiterer Themenfelder aus den BAIT zu erwarten. Diese zusätzlichen personellen Aufwände müssen in einem Marktumfeld aufgebracht werden, in dem als Reaktion auf niedrige Zinsen, stagnierende Revenue-Pools und starken Wettbewerb eine branchenweite und kontinuierliche Reduzierung der Zahl der Beschäftigten zu beobachten ist: alleine zwischen 2014 und 2016 um etwa 5 %.[5]

[5] Deutsche Bundesbank, Monatsbericht September 2017, "Die Ertragslage der deutschen Kreditinstitute im Jahr 2016", Entwicklung der Mitarbeiterzahlen 2014: 639.050, 2016: 608.399.

Die Handlungsfelder, deren Ausgestaltung und Umsetzung primär in der Hoheit des CIO-Office liegen, beziehen sich primär auf Anforderungen aus den BAIT-Themenfeldern IT-Betrieb sowie IT-Projekte und Anwendungsentwicklung. Beispiele sind:

- **Steuerung des IT-Systemportfolios** durch Berücksichtigung der Abhängigkeiten von IT-Systemen zueinander sowie von Risiken alter IT-Systeme (Anforderung 46 und 47).
- **Datensicherungskonzept** abgeleitet aus Anforderungen an das Business-Continuity-Management und Durchführung regelmäßiger Wiederherstellungstests (Anforderung 51).
- **Strukturiertes, IT-projektübergreifendes Anforderungsmanagement** inkl. Priorisierung unter Berücksichtigung vorhandener IT-Ressourcen zur Absicherung der Umsetzung innerhalb von Zeitplan und Budget (Anforderung 33 und 36).
- **Schutz des Quellcode gegen Manipulation durch Entwickler,** beispielsweise mithilfe zusätzlicher Code-Reviews von am Entwicklungsprojekt unbeteiligten Mitarbeitern (Anforderung 39).
- **Unabhängige, formalisierte und dokumentierte Qualitätssicherung im Rahmen der Anwendungsentwicklung** (Anforderung 41). Dies kann insbesondere in agilen Umfeldern eine Herausforderung darstellen. Da Digitalisierung in der Regel ein agiles Arbeitsumfeld erfordert[6], können sich Zielkonflikte ergeben.
- **Übergreifendes IT-Projektportfoliomanagement,** insbesondere zur Mitigation von Risiken durch Abhängigkeiten zwischen einzelnen IT-Projekten (Anforderung 34).
- **Strukturierter Umgang mit Anwendungen aus Fachbereichen** (beispielsweise IDVs[7] wie Risikomodelle) durch Vorhalten eines zentralen Registers und Definition von Vorgaben entlang gemeinsamer Sicherheits- und Programmierstandards (Anforderung 43).

Auch Fachbereiche von den BAIT betroffen: In Fachbereichen entwickelte oder betriebene Anwendungen müssen ebenfalls die BAIT erfüllen. Institutsweite Standards für Anwendungsentwicklung und -betrieb können die Compliance mit den BAIT erleichtern.

[6] Siehe auch https://www.bcg.com/publications/2016/financial-institutions-people-organization-ralph-hamers-disrupting-banking-industry.aspx; https://www.bcg.com/publications/2015/financial-institutions-ron-van-kemenade-building-cutting-edge-banking-it-function.aspx.

[7] IDV: Individuelle Datenverarbeitung.

Durch die zusätzlichen Anforderungen der BaFin wird neben der Anpassung von IT-Systemen auch die laufende und anstehende Umsetzung weiterer umfassender regulatorischer Anforderungen noch aufwendiger – und das, obwohl diese bereits einen großen Anteil der aktuellen und zukünftigen Kapazitäten in der Anwendungsentwicklung binden.

Weiterhin enthalten die BAIT übergreifende Themenfelder. Der CIO ist für die IT-seitige operative Umsetzung verantwortlich:

- **Absicherung der ermittelten Schutzziele einzelner Anwendungen** durch entsprechende Maßnahmen in Anwendungsentwicklung und IT-Betrieb (Anforderungen 11 bis 13).
- **Anwendung und IT-seitige Umsetzung der Informationssicherheitsleitlinie und -richtlinien,** verantwortet vom Informationssicherheitsbeauftragten (aufbauorganisatorisch getrennt von den CIO-Bereichen) (Anforderungen 15 bis 19).
- **Umsetzung von Benutzerberechtigungskonzepten in IT-Systemen,** insbesondere zur Vermeidung von Rollenkonflikten oder Missbrauch von zu weitreichenden Berechtigungen, sowie Dokumentation der Berechtigungsvergabe (Anforderungen 23 bis 30).
- **Erstellung von Risikobewertungen bei Auslagerung und Fremdbezug von IT-Dienstleistungen** (beispielsweise Managed Services oder Managed Capacity) wie Anwendungen von Drittanbietern (z. B. Packaged Solutions oder Software as a Service) sowie regelmäßiger Review bestehender Bewertungen (Anforderung 53 und 56).

Durch die BaFin wird eine ausreichende, dem aktuellen technischen Stand und der aktuellen Bedrohungslage angemessene qualitative und quantitative Personalausstattung der IT-Organisation (sowie des Informationsrisiko- und Informationssicherheitsmanagements) gefordert (Anforderung 5). In Kombination mit den wachsenden Aufgabenstellungen durch die BAIT und bei der Umsetzung anderer Projekte mit Regulatorikbezug erscheint hier ein Mehrbedarf an IT-Ressourcen unausweichlich. Hier zeigen sich Parallelen zur regulatorischen und personellen Entwicklung der Risikocontrolling-Ressorts seit 2009.

2. Technologie kann helfen, zusätzliche Aufwände durch die BAIT zu begrenzen

Die Umsetzung der BAIT erfordert ein breites Spektrum an abgestimmten Maßnahmen. Um diese im Einklang mit der Notwendigkeit der Begrenzung der Kostenbasis zu realisieren, sind innovative organisatorische und technologische Maßnahmen erforderlich. Mögliche Maßnahmen in Governance und Organisation beinhalten den Aufbau eines aktiven Programmmanagements bei (zeit)kritischen Themen, um komplexen inhaltlichen Abhängigkeiten zwischen Projekten sowie besonderen Anforderungen an die Einhaltung von Standards zu begegnen. Agile Arbeitsweisen in der IT-Organisation ermöglichen eine beschleunigte und fokussierte Umsetzung notwendiger Änderungen und Erweiterungen, müssen jedoch an die BAIT angepasst werden, um beispielsweise die Unabhängigkeit von Testern sicherzustellen.

Technologische Maßnahmen, insbesondere solche, die bei der Automatisierung von Anwendungsentwicklung und Produktivsetzung unterstützen (DevOps[8]), können vom CIO genutzt werden, um einen Beitrag zur Erfüllung der BAIT zu leisten und gleichzeitig die IT-Kosten im Griff zu behalten, beispielsweise:

- Automatisierte Protokollierung von Build-, Test- und Deployment-Resultaten entlang des Software-Development-Life-Cycle inkl. Dokumentation der verwendeten Systemkonfiguration von Infrastruktur- und Plattform-Stacks (Anforderung 39 und 40). Dabei kann auch die Kodifizierung von Sicherheitsanforderungen und deren automatisiertes Testen (Compliance as Code) helfen.
- Automatisierte Bereitstellung von produktionsidentischen oder -nahen Testumgebungen sowie automatisierte Durchführung der Tests auf Basis standardisierter Testdaten. Automatisierte Feststellung der (erfolgreichen) Testabdeckung und Testfalldokumentation (Anforderung 41).
- Automatisierte Überwachung des Betriebs und Alarmierung bei Abweichungen von festgelegten Parameterkorridoren oder bei ungewöhnlichen Mustern. Automatisierter regulierender Eingriff (z. B. durch Zuschalten zusätzlicher Rechenkapazität bei Kapazitätsengpässen) von Monitoring-Programmen in den Betrieb (Anforderung 42 und 50).

[8] Siehe auch https://www.bcg.com/publications/2017/technology-digital-leaner-faster-better-devops.aspx.

3. Fünf Schritte zur Umsetzung der BAIT

Die "Bankaufsichtlichen Anforderungen an die IT" wurden als "zentraler Baustein für die IT-Aufsicht über den Bankensektor in Deutschland"[9] am 7. November 2017 veröffentlicht und sind ohne Übergangsfrist gültig. Für die Institute resultieren aus den Anforderungen an die IT Anpassungsbedarfe hinsichtlich Anwendungsentwicklung, Anwendungsbetrieb, IT-Auslagerungen, IT-Strategie und IT-Governance sowie im Informationssicherheits- und Informationsrisikomanagement. In Institutsgruppen ist von der Geschäftsleitung für ein angemessenes Risikomanagement auf Gruppenebene zu sorgen.[10]

Entlang von fünf konkreten Schritten kann die bankweite Compliance mit den BAIT sichergestellt werden:

1. **Erfassung der geänderten Anforderungen durch die BAIT:** Interpretation der Anforderungen an die IT hinsichtlich ihrer konkreten Operationalisierung, beispielsweise anhand einer Anforderungsdatenbank.
2. **Analyse der aktuellen Compliance mit den BAIT:** Qualitative und quantitative Analyse und Bewertung des aktuellen Erfüllungsgrades mit den konkretisierten Anforderungen sowie Identifizierung von Compliance-Lücken, beispielsweise anhand eines Schnelltests.
3. **Aufbau einer institutsweiten BAIT-Roadmap:** Ableitung notwendiger Maßnahmen und Verantwortlichkeiten anhand identifizierter Compliance-Lücken inkl. Ambitionslevel (beispielsweise gleichzeitige Erfüllung weiterer internationaler Standards) sowie Priorisierung und zeitliche Planung der Maßnahmen unter Berücksichtigung verfügbarer (IT-)Ressourcen.
4. **Laufende Abstimmung der BAIT-Roadmap sowie Umsetzung im Dialog mit der BaFin:** Zentral koordinierte Kommunikation mit der BaFin zur Abstimmung der ganzheitlichen BAIT-Roadmap inkl. Priorisierung der notwendigen Aktivitäten und Berücksichtigung weiterer gemeinsamer Aktivitäten wie beispielsweise anstehender Prüfungen.
5. **Umsetzung der Maßnahmen:** Umsetzung der identifizierten Maßnahmen entsprechend der mit der BaFin abgestimmten BAIT-Roadmap ebenfalls im engen und transparenten Austausch mit dem Regulator.

[9] "BAIT: BaFin veröffentlicht Anforderungen an die IT von Banken", Meldung der BaFin.
[10] MaRisk, AT 4.5.

Dr. Walter Bohmayr ist Senior Partner and Managing Director im Wiener Büro *(Bohmayr.Walter@bcg.com).*
Marc Papritz ist Partner and Managing Director im Düsseldorfer Büro *(Papritz.Marc@bcg.com).*
Dr. Christian Schmid ist Principal im Münchner Büro *(Schmid.C@bcg.com).*
Jannik Leiendecker ist Principal im Münchner Büro *(Leiendecker.Jannik@bcg.com).*