# Aktuelles Thema: Bankaufsichtliche Anforderungen an die IT– BAIT

Mit dem Rundschreiben 10/2017 veröffentlichte die BaFin im November 2017 die Bankaufsichtlichen Anforderungen an die IT (BAIT).

Der wesentliche Inhalt sind Anweisungen, um eine sichere Ausgestaltung der IT-Systeme sowie der zugehörigen Prozesse und diesbezüglicher Anforderungen an die IT-Governance in deutschen Kreditinstituten sicherzustellen, da die Informationstechnik die Basis sowohl für fachliche als auch nichtfachliche Prozesse einer Bank bildet.

Hintergrund der Veröffentlichung ist laut BaFin der Aspekt, dass immer mehr Anwender ihre Gelder digital verwalten, transferieren oder auch digital bezahlen. Dieser Aspekt sorgt dafür, dass in einer „globalisierten Finanzwelt die IT-Governance und Informationssicherheit für die Aufsicht inzwischen den gleichen Stellenwert wie die Ausstattung der Institute mit Kapital und Liquidität“ hat.

Grundlage für die BAIT ist die gesetzliche Anforderung des § 25a Absatz 1 Satz 3 Nr. 4 und 5 Kreditwesengesetz (KWG).

In ihr erläutert die Aufsicht, was sie unter einer „angemessenen technisch-organisatorischen Ausstattung der IT-Systeme versteht“. Besondere Beachtung hierbei kommen den Anforderungen an die Informationssicherheit und Notfallkonzepten zu. Aufgrund von zunehmenden IT-Auslagerungen an Dritte wird auch der § 25b KWG in diese Auslegung mit einbezogen.

*Was ist das Ziel von BAIT?*

BAIT hat als Ziel, einen verständlichen und flexiblen Rahmen für den Umgang mit IT-Ressourcen, des Informationsrisikos und der Informationssicherheit zu schaffen. Zusätzlich soll BAIT dazu beitragen, dass Bewusstsein für IT-Risiken innerhalb der Institute, aber auch gegenüber Dritten (Auslagerungsunternehmen) zu erhöhen. Zum ersten Mal ist nun auch transparent, was die Bankenaufsicht für Anforderungen an die Kreditinstitute in Deutschland bezogen auf die Steuerung und Überwachung des IT-Betriebs stellt. Hierzu zählen ebenfalls IT-Berechtigungen, IT-Projektmanagement und Anwendungsentwicklungen.

Einen besonderen Schwerpunkt legt die Aufsicht mit BAIT auf Themen, welche in den vergangenen Jahren bei zahlreichen IT-Prüfungen negativ aufgefallen sind. Zu diesen zählen:

- IT-Strategie

- Berichtwesen
- Datenqualität
- IT-Organisation inkl. IT-Auslagerung
- Informationsrisikomanagement
- Benutzerberechtigungen
- Anwendungsentwicklung
- IT-Notfallmanagement
- IT-Revision

Die Schärfung des Risikobewusstseins in den Instituten und besonders den Management-Ebenen ist eines der zentralen Ziele von BAIT. Als IT-Risiko definiert die Aufsicht alle Risiken für die Vermögens- und Ertragslage von Instituten, „die aufgrund von Mängeln entstehen, die das IT-Management beziehungsweise die IT-Steuerung, die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der Daten, das interne Kontrollsystem der IT-Organisation, die IT-Strategie, -Leitlinien und -Aspekte der Geschäftsordnung oder den Einsatz von Informationstechnologie betreffen“ (Zitat BaFin Fachartikel vom 15.01.2018 - https://www.bafin.de/dok/10362614).

Die acht Themenmodule der BAIT sind folgende:

1. IT-Strategie
2. IT-Gouvernance
3. Informationsrisikomanagement
4. Informationssicherheitsmanagement
5. Benutzerberechtigungsmanagement
6. IT-Projekte und Anwendungsentwicklung
7. Auslagerung und sonstiger Fremdbezug von IT-Dienstleistern
8. IT-Betrieb

Alle diese Ebenen sind von dem Erfordernis der Schaffung von Transparenz, sowie dem IT-Risiko im Allgemeinen betroffen.

Die BAIT selber enthält keine neuen Anforderungen an die Kreditinstitute, sondern es handelt sich um eine detaillierte Interpretation von bereits bestehenden Anforderungen (vgl. MaRisk). Aus diesem Grunde gibt es auch keine gesonderte Umsetzungsfrist für BAIT.

Diese Flexibilität erlaubt es der Aufsicht, die BAIT immer wieder zu ergänzen und zu aktualisieren.

In einer Veröffentlichung vom 03.08.2018 gab die BaFin bekannt, dass Sie aktuell in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Ergänzung (das sog. KRITIS Modul) der BAIT

erarbeitet. Das KRITIS-Modul richtet sich an Kreditinstitute die gemäß BSI-Kritis-Verordnung Betreiber kritischer Infrastruktur sind. Es beschreibt, welche zusätzlichen Anforderungen zu erbringen sind, „um den Nachweis gemäß § 8a Absatz 3 BSI-Gesetz durch den Jahresabschlussprüfer zu erbringen, der im Rahmen der Prüfung des Risikomanagements und der Geschäftsorganisation gleichzeitig die Erfüllung der Anforderungen des § 8a Absatz 1 BSI-Gesetz überprüft und bestätigt“ (Zitat BaFin Fachartikel vom 03.08.2018 - https://www.bafin.de/dok/11325264).

# Kontakt

Wenn Sie sich mit uns zum Thema BAIT austauschen möchten, das Thema vertiefen möchten oder eine strategische Beratung, „Check ups“ vor Ort oder eine operative Umsetzung wünschen, dann nehmen Sie gerne Kontakt mit unserem Ansprechpartner auf:

Frank Thole

E-Mail: frank.thole@wepex.de

WEPEX Unternehmensberatung

Mainzer Landstraße 51

60329 Frankfurt am Main

Telefon: +49 69 719140 – 92

Telefax: +49 69 719140 – 94