Bundesanstalt für
Finanzdienstleistungsaufsicht

BaFin

BaFin | Postfach 12 53 | 53002 Bonn

E-Mail

An die Verbände der Kreditwirtschaft

Bankenaufsicht

Hausanschrift:
Bundesanstalt für
Finanzdienstleistungsaufsicht
Graurheindorfer Str. 108
53117 Bonn | Germany

Kontakt:
Dr. Jens Gampe
Referat BA 51
Fon +49 (0)2 28 41 08-0
Fax +49 (0)2 28 41 08-1550
jens.gampe@bafin.de
www.bafin.de

Zentrale:
Fon +49 (0)2 28 41 08-0
Fax +49 (0)2 28 41 08-1550

Dienstsitze:
53117 Bonn
Graurheindorfer Str. 108

53175 Bonn
Dreizehnmorgenweg 13-15
Dreizehnmorgenweg 44-48

60439 Frankfurt
Marie-Curie-Str. 24-28

03.11.2017
GZ: BA 51-K 3142-2017/0011 (Bitte stets angeben)
2017/1376195
Übersendung der Endfassung der Bankaufsichtlichen Anforderungen an die IT (BAIT)

Anlagen: 1

Anschreiben an die Verbände

Sehr geehrte Damen und Herren,

die Informationstechnik ist – und deshalb steht sie auch zunehmend im Fokus von Angriffen – die Basisinfrastruktur für sämtliche bankfachlichen, aber auch alle nichtbankfachlichen Prozesse in den Instituten.

In einer globalisierten Finanzwelt, in der immer mehr Menschen digital bezahlen bzw. Geld transferieren und in der viele Anleger ihre Geldanlage online bestreiten, sind IT-Governance und Informationssicherheit keine Randthemen mehr, sondern haben auch für die Aufsicht inzwischen den gleichen Stellenwert, wie die Ausstattung der Institute mit Kapital und Liquidität.

Um den Geschäftsleitungen der Institute die Erwartungshaltung der Bankenaufsicht 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 transparent zu machen, wurden – insbesondere auch auf Anregung aus der Kreditwirtschaft – die Bankaufsichtlichen Anforderungen an die IT (BAIT) formuliert, deren offizielle Endfassung nunmehr vorliegt.

Dem vorangegangen waren im Fachgremium IT - mit Vertretern der Verbände, der Institute und der Wissenschaft - intensive Diskussionen zum Entwurf der BAIT, aus denen eine Reihe von konstruktiven Lösungsansätzen hervorgingen, die auch in diese Endfassung eingeflossen sind.

Bei der Erstellung der Endfassung des Rundschreibens wurden zudem zahlreiche Anmerkungen aus Ihren Stellungnahmen im Rahmen der öffentlichen Konsultation des BAIT-Entwurfs berücksichtigt.

Die Spitzenverbände der Kreditwirtschaft haben in ihrer abschließenden Stellungnahme betont, dass vor allem die Mitwirkung des Fachgremiums IT dazu beigetragen hat, die Anforderungen praxisgerecht auszugestalten. Diese positive Haltung bestärkt mich darin, auch künftig an diesem institutionalisierten Austausch festzuhalten.

Ich bedanke mich an dieser Stelle insbesondere für die konstruktive Zusammenarbeit aller Teilnehmer des Fachgremiums IT bei der Erarbeitung der BAIT.

Die BAIT interpretieren – wie die MaRisk auch - die gesetzlichen Anforderungen des § 25a Absatz 1 Satz 3 Nummern 4 und 5 KWG. Die Aufsicht erläutert darin, was sie unter einer angemessenen technisch-organisatorischen Ausstattung der IT-Systeme, unter besonderer Berücksichtigung der Anforderungen an die Informationssicherheit sowie eines angemessenen Notfallkonzepts, versteht. Da die Institute weiter zunehmend IT-Services, sowohl im Rahmen von Auslagerungen von IT-Dienstleistungen als auch durch den sonstigen Fremdbezug von IT-Dienstleistungen, von Dritten beziehen, wird auch der § 25b KWG in diese Interpretation einbezogen.

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

Soweit auf dezidierte Textziffern der MaRisk referenziert wird, sind diese in einer Gesamtschau mit den einschlägigen Textziffern in den BAIT anzuwenden. Die übrigen Textziffern der MaRisk bleiben unberührt. Dies gilt insbesondere für die Anwendung von AT 7.3 MaRisk (Notfallkonzept).

Die modulare Struktur der BAIT eröffnet die notwendige Flexibilität für künftig erforderliche Anpassungen oder Ergänzungen. des Gesamtwerks. Derzeit werden beispielsweise Anpassungen im Hinblick auf die Umsetzung der „G7 - Fundamental Elements of Cybersecurity" geprüft. Des Weiteren wird derzeit – in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik – ebenfalls geprüft, ein spezielles

Bundesanstalt für
Finanzdienstleistungsaufsicht

Modul „Kritische Infrastrukturen" zu erarbeiten und in die BAIT zu überführen. Dies soll ausschließlich für die Kritis-Betreiber des Sektors Finanz- und Versicherungswesen im Sinne des § 2 Abs. 10 BSI-Gesetz die notwendigen Anforderungen beinhalten, um den einschlägigen Vorgaben des BSI-Gesetzes nachzukommen.

Das Rundschreiben tritt mit Veröffentlichung in Kraft.
Da die BAIT keine neuen Anforderungen an die Institute bzw. ihre IT-Dienstleister kodifizieren, sondern lediglich Klarstellungen ohnehin schon vorhandener Anforderungen darstellen, habe ich keine Umsetzungsfristen vorgesehen.

Das BAIT-Rundschreiben ist als Rundschreiben 10/2017 (BA) diesem Schreiben als Anlage beigefügt. Die Dokumente können zudem unter www.bafin.de und www.bundesbank.de abgerufen werden.

Mit freundlichen Grüßen

Im Auftrag

Raimund Röseler

Dieses Schreiben wurde elektronisch erstellt und erhält daher keine Unterschrift.