Verband der Auslandsbanken in Deutschland e.V.
Association of Foreign Banks in Germany

Bundesanstalt für Finanzdienstleistungsaufsicht
Referat GIT 3 - Grundsatz IT-Aufsicht und Prüfungswesen
Graurheindorfer Straße 108
53117 Bonn

per E-Mail an b34_marisk-bait@bundesbank.de
und fachgremiumIT@bafin.de

17. April 2020

Stellungnahme des Verbands der Auslandsbanken in Deutschland e.V. (VAB) zum Entwurf der BAIT-Novelle vom 20. März 2020

Sehr geehrte Damen und Herren,

wir möchten uns für die Übersendung des Entwurfs der BAIT-Novelle sowie des Entwurfs eines überarbeiteten AT 7.3 MaRisk vom 20. März 2020 bei Ihnen bedanken. Gerne nehmen wir die Möglichkeit zur Stellungnahme hiermit wahr.

Der Verband der Auslandbanken in Deutschland (VAB) vertritt gegenwärtig über 200 ausländische Banken, Finanzdienstleistungsinstitute und andere Finanzunternehmen, die mit Tochtergesellschaften und Zweigstellen in Deutschland tätig sind. Sowohl die inländischen Tochtergesellschaften ausländischer Banken als auch die inländischen Zweigstellen ausländischer Banken (§§ 53, 53c KWG) sind Institute i. S. d. KWG und fallen somit grundsätzlich in den persönlichen Anwendungsbereich von MaRisk und BAIT.

Eingangs möchten wir Sie davon in Kenntnis setzen, dass vor dem Hintergrund der derzeitigen Herausforderungen, vor denen die Finanzwirtschaft wie wir alle beruflich und privat bei der Bewältigung der Auswirkungen der Covid-19-Pandemie stehen, viele Ansprechpartner in den Auslandsbanken leider nicht innerhalb der relativ kurz bemessenen Frist angemessen eine Einschätzung zu den vorliegenden Entwürfen an den Verband zurückmelden konnten. Daher sollte die Rückmeldefrist im Rahmen der öffentlichen Konsultation großzügiger festgelegt werden. Zudem bitten wir vor dem aktuellen Hintergrund darum, die Inkraftsetzung der novellierten BAIT und des neuen AT 7.3 MaRisk frühestens im Verlaufe des Jahres 2021 vorzusehen. Denn obgleich die EBA-

Andreas Kastl

Verband der Auslandsbanken
Weißfrauenstraße 12-16
60311 Frankfurt am Main
Tel: +49 69 975850 0
Fax: +49 69 975850 10
andreas.kastl@vab.de
www.vab.de

Interessenvertretung
ausländischer Banken,
Kapitalverwaltungsgesellschaften,
Finanzdienstleistungsinstitute
und Repräsentanzen

Eingetragen im Transparenzregister
der Europäischen Kommission,
Registrierungsnummer:
95840804-38

Leitlinien für das Management von IKT- und Sicherheitsrisiken vom 28. November 2019 (EBA/GL/2019/04) eine Anwendung ab dem 30. Juni 2020 vorsehen, würde eine spätere Umsetzung in der gegenwärtigen Situation sicherlich nicht auf Einwände der EBA oder der anderen NCAs stoßen. Dies würde es den Instituten ermöglichen, sich in der gegenwärtigen Situation auf die Aufrechterhaltung des Geschäftsbetriebes konzentrieren zu können.

Grundsätzlich begrüßt der VAB die Anpassung von BAIT und AT 7.3 MaRisk an die europäischen Vorgaben nach den EBA-Leitlinien, die gerade im Vergleich mit den aufsichtlichen Erwartungen, die andere NCAs an Institute in ihren EU-Mitgliedstaaten richten, zu einer größeren Vereinheitlichung der Aufsichtsniveaus beiträgt („*level playing field*“). Dies kommt der konzernweiten Planung und Realisierung von IT-Projekten und dem konzernweiten Management von IKT- und Sicherheitsrisiken jener Institutsgruppen zu Gute, die wie unsere Mitglieder grenzüberschreitend in mehreren Mitgliedstaaten tätig sind.

Im Einzelnen stellen sich bei der Durchsicht der Entwürfe jedoch Fragen zum generellen Verhältnis von BAIT und AT 7.3 MaRisk zu den Inhalten der EBA-Leitlinien, insbesondere in solchen Fällen, in denen die Leitlinienvorgaben wesentlich ausführlicher formuliert sind als die korrespondieren Vorgaben in den BAIT und AT 7.3 MaRisk. Dies ist etwa der Fall, wenn die Leitlinien im Kontext des Abschnitts 1.4.4. über den sicher(er)en Betrieb von IKT viele praxisbezogene Beispiele in Randnummer 36 nennen, und die korrespondierenden BAIT-Ausführungen zur operativen IT-Sicherheit in Textziffer 5.2 dies nicht spiegeln. Ein anderes Beispiel ist erkennbar in BAIT-Textziffer 4.8 zur institutsindividuellen Test- und Überprüfungsrichtlinie, deren Umsetzung in den EBA-Leitlinien mit umfänglichen Ausführungen in Abschnitt 1.4.6. (Überprüfungen, Bewertungen und Tests der Informationssicherheit), genauer in den Randnummern 41-48, beschrieben wird. Natürlich stellt die prinzipienorientierte Natur der BAIT eine wichtige Grundlage für eine verhältnismäßige und institutsindividuelle Umsetzung dar; dennoch sollte klargestellt werden, dass Institute, die auf freiwilliger Basis oder auch aufgrund von Praxisanforderungen, die sich aus einem EU-Gruppenkontext ergeben, konkretere Ausführungen in den EBA-Leitlinien befolgen und damit ebenfalls die Aufsichtserwartung der BaFin erfüllen.

Wir hoffen, Ihnen hiermit und in der nachfolgenden Anlage nützliche Einblicke in die aus unserer Sicht entstehenden Herausforderungen bei der Umsetzung der neuen Anforderungen eröffnen und auch konstruktive Lösungswege vorschlagen zu können.

Für Rückfragen steht Ihnen der Rechtsunterzeichner zur Verfügung.

Mit freundlichen Grüßen

Dr. Oliver Wagner Andreas Kastl

Anlage

Anlage:
Vorschläge des Verbandes der Auslandsbanken in Deutschland e.V. (VAB) zum Entwurf von überarbeiteten bankaufsichtlichen Anforderungen an die IT (BAIT)

Petitum 1: Aufsichtliche Einordnung der EBA-Leitlinien in den Vorbemerkungen zu den BAIT, dort: Nummer 5.

VORSCHLAG: In den Vorbemerkungen sollte in Nummer 5 der folgende Satz 2 angefügt werden: „$_2$Die Orientierung an den Inhalten der EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken vom 28. November 2019 (EBA/GL/2019/04) steht im Einklang mit der in diesem Rundschreiben formulierten Aufsichtspraxis.“

Begründung:

Insofern Institute, die auf freiwilliger Basis oder auch aufgrund von Praxisanforderungen, die sich aus einem EU-Gruppenkontext ergeben können, bestimmte Praxisbeispiele und umfangreichere Ausführungen in den EBA-Leitlinien befolgen, sollten damit ebenfalls die Aufsichtserwartung der BaFin im Hinblick auf die BAIT erfüllen. Denn mit der Überarbeitung der BAIT möchte die BaFin, wie im sog. *Compliance Table* bei der EBA angegeben, die Übertragung der Vorgaben der EBA-Leitlinien in ihre Aufsichtspraxis erreichen.

Petitum 2: Klarstellung zu externen IT-Dienstleistungen im Zusammenhang mit den Mindestinhalten der IT-Strategie, Kapitel (*früher: Modul)* 1: IT-Strategie, dort: Textziffer (*nachfolgend: Tz.*) 1.2, Erläuterung zu Buchstabe a.

VORSCHLAG: In der Erläuterung zu Buchtstabe a sollte der Satz 1 wie folgt ergänzt werden: „$_1$Beschreibung der Rolle, der Positionierung und des Selbstverständnisses der IT im Hinblick auf Personaleinsatz und Budget der IT-Aufbau- und IT-Ablauforganisation sowie die Darstellung und strategische Einordnung der externen IT-Dienstleistungen, die dem Institut durch ein Dienstleistungsunternehmen bereitgestellt werden (vgl. Kapitel 9).“

Begründung:

Bei der Darstellung von IT-Dienstleistungen im Rahmen der institutsindividuellen IT-Strategie sieht eine Änderung des Entwurfs vor, dass künftig nur noch sog. externe IT-Dienstleistungen speziell zu betrachten sein sollen. Diese risikoorientiere Fokussierung ist grundsätzlich zu begrüßen. In diesem Zusammenhang gehen wir davon aus, dass eben solche IT-Dienstleistungen als extern im Sinne dieser Erläuterung zu den Mindestinhalten der IT-Strategie anzusehen sind, die – in Anlehnung an die Vorbemerkung zu Kapitel 9 hinsichtlich „Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen“ in Tz. 9.1 Satz 2 – von einem Dienstleistungsunternehmen erbracht werden. Somit würde ein gemeinsames Verständnis von externen IT-Dienstleistungen sowohl für Zwecke der IT-Strategie (Kapitel 1) als auch für die Zwecke des Kapitels 9 hergestellt werden.

Petitum 3: Konkretisierung der sog. maßgeblichen Stellen im Zusammenhang mit der Umsetzung eines Systems zum Management der Informationsrisiken, Kapitel 3: Informationsrisikomanagement, dort: Erläuterung zu Tz. 3.2.

VORSCHLAG: Die Erläuterung zu Tz. 3.2 sollte wie folgt ergänzt werden:
„Zu den maßgeblichen Stellen gehören auch die Fachbereiche, die Eigentümer der Informationen sind und die ~~R~~Informationsrisiken tragen."

Begründung:

Nach Tz. 3.2 sollen bei der Umsetzung der Bestandteile eines Systems zum Management der Informationsrisiken auch bestimmte maßgeblichen Stellen mitwirken. In der entsprechenden Erläuterung sieht der Entwurf eine Konkretisierung vor, wonach als maßgeblichen Stellen im Sinne dieser Vorschrift nicht mehr nur jene Fachbereiche sein sollen, die Eigentümer der Informationen sind, sondern insbesondere solche, die auch Risiken tragen. Grundsätzlich ist diese Konkretisierung begrüßenswert, mag sie doch dazu führen, dass das System zum Management der Informationsrisiken effizienter in den Instituten umgesetzt werden könnte.

Jedoch stellt sich die Frage, wie in diesem Kontext diese Risiken richtig zu definieren sind. Es sollte daher klargestellt werden, dass die in Betracht kommenden Risiken eben nur jene sind, die im Rahmen der BAIT – als Konkretisierung der MaRisk – speziell zu betrachten sind: Informationsrisiken. Damit wird vermieden, dass die Institute beispielsweise alle operationellen Risiken (oder gar Kredit- oder Marktrisiken) in diesem Zusammenhang als relevant betrachten.

Petitum 4: Bitte um Konkretisierung der aufsichtlichen Erwartungshaltung hinsichtlich von Anlässen, die eine Überprüfung des Schutzbedarfs auslösen, Kapitel 3: Informationsrisikomanagement, Tz. 3.4.

Der Entwurf sieht eine gut nachvollziehbare Formulierung für Tz.3.4 Satz 1 vor, wonach das Institut sowohl regelmäßig als auch anlassbezogen den Schutzbedarf für die Bestandteile seines definierten Informationsverbundes zu ermitteln habe. Im Vergleich mit der bisherigen Textfassung ist diese Formulierung zu begrüßen. Die Anforderung nach der regelmäßigen Überprüfung, die nicht weiter konkretisiert ist, lässt den Instituten Spielraum, einen für die Institutssituation geeigneten Überprüfungsrhythmus festzulegen. Wir möchten daneben jedoch anregen, dass für die Zwecke der anlassbezogenen Prüfung eine nicht abschließende Liste von praxisrelevanten Beispielen für derartige Anlässe in der Erläuterungsspalte aufgenommen wird, die die Aufsichtserwartung wiederspiegeln bzw. verdeutlichen.

Petitum 5: Klarstellung der Zuständigkeiten im Zusammenhang mit dem Sollmaßnahmenkatalog und der Risikoanalyse, Kapitel 3: Informationsrisikomanagement, dort: Tz. 3.4 - 3.7.

In den Ausführungen zum Schutzbedarf in den Instituten sieht der Entwurf einige Anpassungen vor und benennt dabei eingangs auch konkrete Zuständigkeiten:

- gemäß Tz. 3.4 sei der Eigentümer der Information für die Ermittlung des Schutzbedarfes verantwortlich;

- gemäß Tz. 3.5 sollen die Schutzbedarfsklassifizierungen sowie die zugehörige Dokumentation durch das Informationsrisikomanagement überprüfen werden.

Nachfolgend wird in Tz. 3.6 ausgeführt, dass „das Institut" einen Sollmaßnahmenkatalog erstellen soll; der Entwurf wird hier nicht konkreter, indem er beispielsweise dem Informationsrisikomanagement auch diese Zuständigkeit zuschreibt. Auch bei der Durchführung der Risiko-Analyse (i. e. Vergleich der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen, also dem Ist-Zustand) nach Tz. 3.7 Satz 1 nennt auch der bisherige Wortlaut keine konkrete Zuständigkeit. Betrachtet man außerdem den Wortlaut in Tz. 3.7 Satz 3, wonach das Informationsrisikomanagement die Soll-Ist-Vergleiche (die Grundlage für die Risikoanalyse sind) zu koordinieren und zu überwachen, nicht jedoch durchzuführen habe, so kann der Eindruck gewonnen werden, dass die BAIT dem Informationsrisikomanagement diese Aufgaben nicht zuschreibt.

Es würde die Rechtssicherheit unseres Erachtens erhöhen, wenn die Aufsichtserwartung über die Zuständigkeiten den Erläuterungsspalten hinzugefügt wird, insbesondere in Bezug zur Durchführung der Risiko-Analyse nach Tz. 3.7 Satz 1, da hier eine konkrete Berichtspflicht gegenüber der Geschäftsleitung nach Tz. 3.9 daran anknüpft.

Petitum 6: Klarstellung des Verhältnisses von Informationsrisikomanagement zur Analyse der Bedrohungslage, Kapitel 3: Informationsrisikomanagement, dort: Tz. 3.8.

VORSCHLAG: Der Wortlaut in Tz. 3.8 sollte wie folgt geändert werden:
„Das Institut informiert sich laufend über Bedrohungen seines Informationsverbundes, prüft auf Schwachstellen~~,~~ und bewertet deren Auswirkung ~~und ergreift wirksame technische und organisatorische Maßnahmen~~."

Begründung:

Das in Kapitel 3 dargestellte Informationsrisikomanagement umfasst grundsätzlich die Definition und die Abstimmung der Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege, die mit dem Management der Informationsrisiken verbunden sind (Tz. 3.1 Satz 4), stellt Anforderungen an Überwachungs- und Steuerungsprozesse und definiert Berichtspflichten (Tz. 3.1 Satz 5). In der Erläuterung zu Tz. 3.6 wird in Bezug zum Sollmaßnahmenkatalog zudem betont, dass dieser lediglich die Anforderungen, nicht jedoch deren konkrete Umsetzungen, enthalten solle.

In diesem Zusammenhang stellt sich die Frage, weshalb Tz. 3.8 nicht nur Anforderungen zur Bedrohungsüberwachung und Schwachstellenbewertung aufstellt, sondern auch konkret zu ergreifende Maßnahmen nennt (es ist zu vermuten, dass dies auf die Formulierung der Randnummer 42 der EBA-Leitlinien zurückzuführen ist). Das Ergreifen wirksamer technischer und organisatorischer Maßnahmen im Zusammenhang mit Bedrohungen des Informationsverbundes und mit den möglichen Schwachstellen ist natürlich eine richtige und wichtige Anforderung; diese sollte jedoch konzeptionell in das neue Kapitel 5 über die operative IT-Sicherheit überführt und mit den dortigen Anforderungen abgestimmt werden.

Petitum 7: Klarstellung der Verantwortung der Geschäftsleitung, Kapitel 4: Informationssicherheitsmanagement, dort: Tz. 4.2.

VORSCHLAG: Die Erläuterung zu Tz. 4.2 sollte wie folgt geändert werden:
„Die Geschäftsleitung erkennt ihre Gesamtverantwortung für die Schaffung eines wirksamen Risikomanagementrahmens für die IKT- und Sicherheitsrisiken ~~Informationssicherheit~~ an."

Begründung:

Nach Tz. 4.2 habe die Geschäftsleitung die Informationssicherheitsleitlinie zu beschließen; dies deckt sich mit der Anforderung der EBA-Leitlinien, die in Bezug zur Informationssicherheitsleitlinie in Randnummer 28 Satz 4 ausführt: „Die Leitlinie sollte vom Leitungsorgan genehmigt werden".

Der Entwurf postuliert jedoch in der Erläuterung zur Tz. 4.2 eine Gesamtverantwortung der Geschäftsleitung für die Informationssicherheit. Die Herstellung und Überwachung der Informationssicherheit wird jedoch typischerweise delegiert; diese Delegation ist auch hauptsächlich Objekt der Regelungen der BAIT. Somit sollte die hier gemeinte Anerkennung einer Gesamtverantwortlichkeit der Geschäftsleitung in Anlehnung an die Ausführung in Randnummer 4 der EBA-Leitlinien näher konkretisiert werden; dort wird festgelegt, dass dem Leitungsorgan unter anderem eine Gesamtverantwortung für die Schaffung eines wirksamen Risikomanagementrahmens für die IKT- und Sicherheitsrisiken obliegt, nicht jedoch der Informationssicherheit (im Institut) selbst.