Bundesverband der Wertpapierfirmen e.V.
Am Sandtorkai 44, 20457 Hamburg

Bundesanstalt für Finanzdienstleistungsaufsicht
Referat WA 31
Postfach 12 53
53002 Bonn

per Mail:
Konsultation-02-17@bafin.de und b32_marisk@bundesbank.de

Ihr Zeichen
BA 51-K 3142-2017/0004

Ihre Nachricht vom
22.03.2017

Ort_Datum
Hamburg, 05.05.2017

Konsultation des Rundschreibens „Bankaufsichtliche Anforderungen an die IT“ (BAIT)

Sehr geehrte Damen und Herren,

in dieser Sache danken wir Ihnen verbindlich für die Möglichkeit der vorherigen Mitwirkung im Fachgremium IT sowie der Teilnahme an der vorliegenden Konsultation und machen von der Möglichkeit der Abgabe einer Stellungnahme zu dem geplanten Rundschreiben „Bankaufsichtliche Anforderungen an die IT“ auf diesem Wege gerne Gebrauch.

Voranschicken möchten wir den Hinweis, dass wir das Rundschreiben für materiell-rechtlich weitgehend gelungen und zielführend im Hinblick auf den hier ausgemachten Regelungsbedarf erachten. Die nachfolgenden Hinweise und Anmerkungen beziehen sich insoweit vor allem darauf sicherzustellen, dass das Regelwerk im Sinne des Beabsichtigten schwerpunktmäßig richtig verstanden und in der Praxis entsprechend umgesetzt wird.

I. Grundsätzliche Anmerkungen

1. Verhältnis zu MaRisk und Anwenderkreis

Zunächst regen wir einige sprachliche Verbesserungsvorschläge an, um noch deutlicher klarzustellen, dass die BAIT keine eigenständige und „neben“ den MaRisk stehende Konkretisierung der gesetzlichen Grundlagen darstellt bzw. vornimmt, sondern vielmehr die MaRisk den Rahmen vorgeben, innerhalb dessen die BAIT die Anforderungen an die IT weitergehend konkretisieren.

Darüber hinaus halten wir einen klarstellenden Hinweis für erforderlich, dass der Anwenderkreis der BAIT dem der MaRisk entspricht.

Bundesverband der Wertpapierfirmen e.V.

Sitz des Verbandes
Fasanenstraße 3
10623 Berlin

Postanschrift & Geschäftsstelle
Friedrichstraße 52
60323 Frankfurt/Main

Tel.: +49 (0) 69 92 10 16 91
Fax: +49 (0) 69 92 10 16 92
mail@bwf-verband.de
www.bwf-verband.de

Vorstand
Prof. Dr. Jörg Franke (Vorsitzender)
Carsten Bokelmann
Stefan Bolle
Dirk Freitag
Holger Gröber
Kai Jordan
Thorsten Klanten
Dr. Annette Kliffmüller-Frank

Geschäftsführer
Michael H. Sterzenbach
m.sterzenbach@bwf-verband.de

Justiziar
Dr. Hans Mewes
Am Sandtorkai 44, 20457 Hamburg
Tel.: +49 (0) 40 36 80 5 - 132
Fax: +49 (0) 40 36 80 5 - 333
h.mewes@bwf-verband.de

Bankverbindung
Deutsche Bank PGK Frankfurt
BLZ 500 700 24, **Kto.** 0 18 32 10 00

Weiterhin schlagen wir vor, auf die eigenständige Formulierung des Proportionalitätsprinzips zu verzichten und statt dessen ausschließlich auf die insoweit bereits in den MaRisk verankerten Regelungen zu verweisen. Auf diesem Wege wird die unzutreffende Annahme vermieden, dass beiden Regelwerken eigenständige Proportionalitätsprinzipen mit jeweils eigenen Kriterien zugrunde lägen. Zudem wird hierdurch zukünftig die Kohärenz beider Rundschreiben zueinander sichergestellt und vereinfacht. – Sollte seitens der Bundesanstalt und der Bundesbank entgegen unserem Petitum eine explizite Formulierung hierzu in den BAIT als notwendig erachtet werden, sollten u.E. die entsprechenden Textziffern der MaRisk wortgleich in die BAIT aufgenommen werden.

Zur Umsetzung der vorstehenden Anregungen schlagen wir konkret folgende Anpassungen der BAIT in Teil I (Vorbemerkung) Textziffern 1 bis 3 vor [Änderungen durch Streichungen/Unterstreichungen markiert]:

„1 Der Einsatz von Informationstechnik (IT) in den Instituten hat eine zentrale Bedeutung und wird weiter an Bedeutung gewinnen. Dieses Rundschreiben ~~gibt~~ konkretisiert auf der Grundlage des § 25a Abs. 1 und Abs. 3 sowie §25b des Kreditwesengesetzes (KWG) die Vorgaben der MaRisk. Es gibt einen flexiblen und praxisnahen Rahmen für die Ausgestaltung der IT der Institute, insbesondere für das Management der IT-Ressourcen und für das IT-Risikomanagement vor. ~~Es konkretisiert ferner die Anforderungen des § 25a Abs. 3 KWG (Risikomanagement auf Gruppenebene) sowie des § 25b KWG (Auslagerung).~~ Der Anwenderkreis dieses Rundschreibens entspricht AT 2.1 der Mindestanforderungen an das Risikomanaqment (MaRisk).

2 Die prinzipienorientierten Anforderungen tragen de~~m~~n in den MaRisk verankerten Proportionalitätsprinzipien Rechnung und ermöglichen den Instituten somit eine risikoorientierte Umsetzung. ~~Unter Berücksichtigung der Größe des Instituts sowie der Komplexität, einer besonderen Risikoexponierung oder Internationalität seiner Geschäftsaktivitäten kann gleichwohl die Erfüllung weitergehender als in diesem Rundschreiben explizit formulierter Anforderungen erforderlich sein.~~

3 Die in den ~~Mindestanforderungen an das Risikomanagement (~~MaRisk~~)~~ enthaltenen Anforderungen bleiben unberührt und werden im Rahmen ihres Gegenstands durch dieses Rundschreiben konkretisiert. Die in diesem Rundschreiben konkretisierten Themenbereiche sind nach Regelungstiefe und –umfang nicht abschließender Natur. Das Institut bleibt folglich auch insbesondere jenseits der Konkretisierungen dieses Rundschreibens gemäß § 25a Abs. 1 Nr. 4 KWG i. V. m. AT 7.2 Tz. 2 MaRisk verpflichtet, bei der Ausgestaltung der IT-Systeme und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards (z. B. der Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik und der internationale Sicherheitsstandard ISO/IEC 2700X) abzustellen.“

2. Modulstrukturierung

Im Rahmen der Vorbesprechungen im Fachgremium IT wurden seitens der Institusvertreter auf die Notwendigkeit klarer Begriffsdefinitionen hingewiesen. Hier sehen wir insbesondere in Bezug auf die verwendeten Begriffe *„Informationsrisikomanagement"* und *„Informationssicherheitsmanagement"* weiterhin Handlungsbedarf. Dies auch deshalb, weil es sich hierbei im Aufbau der BAIT um zwei eigenständige Module handelt, die nach unserem Verständnis gemeinsam das geforderte Managementsystem zur Steuerung der Informationssicherheit (ISMS) beschreiben und daher sehr eng miteinander verwoben sind. Die Abgrenzung, welche Teile des Ganzen in welchem Modul verortet sind, sind u.E. nicht eindeutig nachvollziehbar. Wir halten daher aus Gründen der Rechtssicherheit eine verständliche Erklärung der Begrifflichkeiten und eine klare Abgrenzung der beiden Module voneinander für erforderlich. (Hilfsweise käme insoweit auch die „Zusammenlegung" in einem Kapitel des Regelwerks in Betracht.)

3. Verhältnismäßigkeit und Risikoorientierung im Teil II Kapitel 8 (Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen)

Die MaRisk normieren weitgehende und spezifische Anforderung an das Management von Risiken bei Auslagerungen, die für das Institut wesentlich sind. Begriffsnotwendig – und sachlich geboten – werden hiervon nur solche Auslagerungen umfasst, die einen Bezug zur Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen aufweisen.

Eine solche Handhabung ist aus unserer Sicht sachgerecht, da die spezifischen und hohen Anforderungen damit unter Risikogesichtspunkten auf tatsächlich relevante Sachverhalte beschränkt werden. Ungeachtet dessen gelten für alle übrigen Auslagerungen sowie den sonstigen Fremdbezug von Dienstleistungen das Erfordernis einer angemessenen Geschäftsorganisation.

Die Konkretisierung dieser Regelungen durch die BAIT erscheint uns vor diesem Hintergrund verbesserungswürdig, denn es fehlt an den oben genannten Relevanzkriterien. Wir bitten daher um eine entsprechende Klarstellung, dass die materiellen Anforderungen des Kapitels 8 sich nur auf *wesentliche* Sachverhalte mit Bezug zur Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen beziehen.

4. Inkrafttreten

Sowohl der vorliegende Konsultationsentwurf als auch das Anschreiben der Bundesanstalt enthalten noch keine Hinweise zum Zeitpunkt des Inkrafttretens des neuen Regelwerks und zu etwaigen Übergangsfristen. Um den Instituten hier eine hinreichende Planungssicherheit zu gewährleisten, wäre eine frühzeitige Aussage zum geplanten Abschluss der Konsultation, dem In-

krafttreten des neuen Rechts und den Übergangsfristen wünschenswert. Wir geben insoweit insbesondere zu bedenken, dass in den Instituten hier durchaus signifikanter Umsetzungsbedarf entstehen dürfte, so dass eine angemessene Umsetzungsfrist bis zum materiellen Inkrafttreten des neuen Regelwerkes unabdingbar erscheint. Wir regen hier nachhaltig eine Umsetzungsfrist von einem Jahr an. (Es erscheint zweckmäßig, diesen Punkt auch zum Gegenstand der Erörterung in der kommenden Sitzung des Fachgremium IT zu machen.)

II. Spezifische Anmerkungen

1. Teil I (Vorbemerkung) Textziffer 3, dort dritter bzw. letzter Satz

„Das Institut bleibt folglich auch insbesondere jenseits der Konkretisierungen dieses Rundschreibens gemäß § 25a Abs. 1 Nr. 4 KWG i. V. m. AT 7.2 Tz. 2 MaRisk verpflichtet, bei der Ausgestaltung der IT-Systeme und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards (z. B. der Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik ~~und~~ oder der internationale Sicherheitsstandard ISO/IEC 2700X) abzustellen." [Änderung durch Streichung/Unterstreichung markiert.]

Begründung: Institute richten Ihre internen Verfahren i.d.R. an einem der genannten Standards aus. Die Änderung stellt einen sprachlichen Verbesserungsvorschlag dar, um dies klarer zum Ausdruck zu bringen.

2. Teil II Kapitel 2 (IT-Governance) Textziffer 3

Wir regen an, aus Gründen der Rechtssicherheit den Begriff IT-*„Risikosteuerungsprozess"* durch *„Informationsrisikomanagementprozess"* zu ersetzen. Dies würde auch eine sprachliche Eindeutigkeit zu den Begrifflichkeiten in Kapitel 3 sicherzustellen.

3. Teil II Kapitel 2 (IT Governance) Textziffer 6

„~~Interessenkonflikte und u~~Unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation sind zu vermeiden. Interessenskonflikten ist angemessen zu begegnen." [Änderungen durch Streichung/Unterstreichung markiert.]

Begründung: Interessenskonflikte können nicht per se vermieden, Ihnen sollte jedoch mit angemessenen Maßnahmen begegnet werden. Unvereinbare und damit abzugrenzende bzw. zu trennende Tätigkeiten gründen u.E. auf Interessenskonflikten, denen mit anderen Mitteln nicht (mehr) zu begegnen ist.

4. Teil II Kapitel 4 (Informationssicherheitsmanagement) Textziffer 20

Im Rahmen der Informationsveranstaltung der Bundesanstalt zum neuen Regelwerk wurde ausgeführt, dass eine „Kombination" der Funktionen des In-

formationssicherheitsbeauftragten und des Datenschutzbeauftragten als „teilweise problematisch“ erachtet würde. Wir können dies nicht nachvollziehen und vermögen insoweit keine Interessenskonflikte zu erkennen, die einer „personellen Bündelung“ dieser beiden Funktionen entgegenstünden. Insbesondere sehen wir es auch im Hinblick auf die Verhältnisse in „kleineren Häusern“ als geboten an, in Fragen der Unabhängigkeit, der Vereinbarkeit und der Auslagerbarkeit der verschiedenen „Rollen“ als Beauftragte und sonstiger geforderter Unternehmensfunktionen „Maß und Mitte zu halten“, damit auch solche Häuser mit begrenzten Personalressourcen sich regelkonform und angemessen organisieren können.

5. Teil II Kapitel 4 (Informationssicherheitsmanagement) Textziffer 23

Hier regen wir die Streichung des Einschubs *„mindestens vierteljährig“*. Ein derart „kurzfristig geprägtes“ zeitliches Intervall erscheint als Mindestanforderung für eine Berichterstattung an die Geschäftsleitung sachlich nicht angemessen, zumal über die ebenfalls geforderte anlassbezogene Berichterstattung sichergestellt ist, dass über außergewöhnliche Umstände und Sachverhalte unverzüglich berichtet wird.

6. Teil II Kapitel 6 (IT-Projekte, Anwendungsentwicklung) Textziffer 46

Wir verstehen unter einer Anwendung im Sinne einer IDV nicht jedes von einem Fachbereich mittels Standardsoftware erstelltes Arbeitsmittel (z.B. Excel-Sheet mit Berechnungen). Notwendig sind vielmehr eine gewisse Komplexität und Bedeutung dieser Hilfsmittel für die Geschäftsprozesse, um diese als IDV zu klassifizieren. Eine Bestätigung dieser Sichtweise – sei es durch einen klarstellenden Hinweis im Regelwerk, sei es durch ausdrückliche behördliche Bekundung im weiteren Abstimmungsprozess – halten wir für unbedingt erforderlich. Sollte entgegen unserer Auffassung seitens der Aufsicht ein „weites Begriffsverständnis“ bevorzugt werden, halten wir in der Textziffer 46 die explizite Aufnahme einer Öffnungsklausel zur „Aussteuerung“ nicht relevanter IDV-Anwendungen für notwendig, um einen risikoorientierten Umgang mit den Anforderungen der Verwaltungspraxis zu gewährleisten.

7. Teil II Kapitel 7 (IT-Betrieb) Textziffer 53

Hier bitten wir um Streichung des Einschubs *„mindestens jährlich“*. Im Hinblick auf eine risikoorientierte und am Proportionalitätsprinzip ausgerichtete Ausgestaltung des BAIT-Regimes erscheint die Vorgabe eines derart kurzen Regelturnus‘ für entsprechende Testläufe nicht für jedes einzelne Datensicherungsverfahren in jedem Institut angemessen. Auch gehen wir davon aus, dass separate Tests immer dann entbehrlich sein sollten, wenn die Wirksamkeit entsprechender Verfahren im produktiven Betrieb aufgrund notwendig gewordener Rücksicherungen bereits nachgewiesen wurden. Im Übrigen

bleiben ja auch die a.a.O. im Regelwerk normierten *anlassbezogenen* Testverfahren unberührt.

8. Teil II Kapitel 8 (Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen) Textziffer 56 (Änderung unterstrichen)

„Wegen der grundlegenden Bedeutung der IT für das Institut ist auch für jeden sonstigen Fremdbezug von IT-Dienstleistungen vorab eine angemessene Risikobewertung durchzuführen."

Begründung: Sowohl in den MaRisk (AT 7.2 Textziffer 4) als auch in Teil II Kapitel 8 Textziffer 54 der BAIT wird auf angemessene Maßnahmen zur Verwirklichung des Proportionalitätsprinzips abgestellt. Dies sollte auch in der konkretisierenden Textziffer 56 durch die vorstehend angeregte Ergänzung sichergestellt werden. Die Ausgestaltung einer durchzuführenden Risikobewertung muss dem Sachverhalt angemessen sein, weshalb in den Instituten i.d.R. auch „abgestufte" Bewertungsverfahren zum Einsatz kommen. Es sollte hier auch der Eindruck vermieden werden, dass ausnahmslos jeder Fremdbezug, selbst wenn er für das Institut offenkundig nicht von Relevanz ist, einem formellen und umfassenden Bewertungsverfahren unterzogen werden muss.

Sollten sich aus dem Kreis unserer Verbandsmitglieder noch weitere Anmerkungen oder Hinweise ergeben, würden wir diese ggf. noch nachreichen.

Gegen eine Veröffentlichung unserer Stellungnahme bestehen keine Bedenken.

Für Rückfragen in dieser Sache und jedwede weitere Abstimmung stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Dr. Hans Mewes

Justiziar