ZIA Zentraler Immobilien Ausschuss e.V. – Leipziger Platz 9 – 10117 Berlin

Bundesanstalt für Finanzdienstleistungsaufsicht
Marie-Curie-Str. 24-28
Referat WA 46
60439 Frankfurt

**Nur per E-Mail an: Konsultation-07-19@bafin.de**
**Geschäftszeichen: WA 46-FR 1903-2018/0001**

Berlin, den 15. Mai 2019

**Stellungnahme im Rahmen der Konsultation 07/2019 – Entwurf eines Rundschreibens „Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)“**

Sehr geehrte Damen und Herren,

wir bedanken uns für die Zusendung des o.g. Entwurfs und der Gelegenheit hierzu Stellung nehmen zu können.

## I. Allgemeine Anmerkungen

Zu den Mitgliedern des Zentralen Immobilien Ausschuss e.V. (ZIA) gehören u.a. knapp 40 Kapitalverwaltungsgesellschaften, die offene und geschlossene Investmentvermögen auflegen und verwalten. Das KAIT-Rundschreiben ist für die Mitglieder des ZIA daher von großer Relevanz.

Wir unterstützen die BaFin in ihrem Anliegen, die IT-Sicherheit im Markt zu erhöhen und das IT-Risikobewusstsein in den Kapitalverwaltungsgesellschaften zu schärfen. Der zur Konsultation gestellte Entwurf des KAIT-Rundschreibens (KAIT-E) berücksichtigt die Diskussionen und Ergebnisse von drei Workshop-Terminen, die zwischen Dezember und Februar in den Räumen der BaFin mit ausgewählten Kapitalverwaltungsgesellschaften (KVG) und den Verbänden stattgefunden haben. Die frühzeitige Einbindung der Marktteilnehmer in die Entwicklung des Rundschreibens haben wir als sehr positiv empfunden. Durch den frühen und konstruktiven Dialog konnten bereits wichtige Impulse aus der Praxis für das Rundschreiben berücksichtigt werden.

Für die Ausgestaltung des KAIT-Rundschreibens, aber auch für die konkrete Anwendung und Auslegung der Vorgaben in der Praxis sollten stets die jeweiligen

Einzelfallumstände der betroffenen KVG mit einfließen. Dem unter Ziff. I.3 verankertem Proportionalitätsprinzip muss in Verbindung mit Ziff. 1.2. f. der KAMaRisk in diesem Zusammenhang eine hohe Bedeutung beigemessen werden. Dies gilt umso mehr, als dass der KAIT-E weitestgehend dem „Rundschreiben 10/2017 (BA) - Bankaufsichtliche Anforderungen an die IT (BAIT)“ sowie dem „Rundschreiben 10/2018 – Versicherungsaufsichtliche Anforderungen an die IT (VAIT)“ nachgebildet wurde. Die einzelnen KVGen unterscheiden sich in Größe, Komplexität und Geschäftsausrichtung nicht nur untereinander, sondern insbesondere auch im Vergleich zu Banken und Versicherungen. Diesen strukturellen Unterschieden sollte bei der Anwendung der KAIT unbedingt hinreichend Rechnung getragen werden.

Als zentralen Punkt der KAIT-E betrachten wir die Abgrenzung zwischen Auslagerung und sonstigem Fremdbezug von IT-Leistungen unter Ziff. II.8. Wir bewerten die auf Grundlage der Diskussionen in den Workshops erarbeiteten Abgrenzungskriterien der KAIT-E als sehr weitgehend, wenngleich wir im Vergleich zu der diskutierten Ausgangsversion praxistauglichere Verbesserungen sehen. Insgesamt hat sich an dieser Stelle gezeigt, dass eine Abgrenzung kaum durch griffige Kriterien ausgestaltet werden kann. Vor diesem Hintergrund sehen wir den gegenüber der BAIT und der VAIT sehr viel höheren Detailierungsgrad der Abgrenzungskriterien kritisch. Den Aspekten zum Proportionalitätsgrundsatz und der Einzelfallbetrachtung sollte gerade angesichts dessen eine überragende Bedeutung zukommen. (Weitere Ausführungen zu Ziff. II.8 s. unten S. 5).

## II. Anmerkungen im Einzelnen

Zu dem KAIT-E im Einzelnen möchten wir die nachfolgenden Punkte anmerken:

**Zu II. Kapitel 1, Ziff. 4 - IT-Strategie: Aufsichtsrat**
Das Rundschreiben legt in Textziffer 4 fest, dass die IT-Strategie bei Erstverabschiedung oder bei Anpassungen dem Aufsichtsrat der Kapitalverwaltungsgesellschaft (KVG) oder einem vergleichbaren Aufsichtsorgan zur Kenntnis zu geben ist. Es wird nicht näher konkretisiert, in welcher Form dies zu erfolgen hat.

Wir gehen davon aus, dass die IT-Strategie dem Aufsichtsorgan nicht zwingend durch Aushändigung des Original-Dokuments zur Kenntnis gegeben werden muss. Dem entsprechend sollte es auch möglich sein, die IT-Strategie oder etwaige Anpassungen durch eine entsprechende adressatengerechte Aufbereitung zu vermitteln, wie z.B. durch geeignete Zusammenfassungen, Präsentationen etc. Ein solches Vorgehen wird sich häufig angesichts des Umfangs und der Dichte technischer Details in der IT-Strategie anbieten.

Um diesen Prozess zu präzisieren und den Proportionalitätsgrundsatz des Rundschreibens zu betonen, empfehlen wir folgende Änderung der Textziffer 4:

*Die IT-Strategie ist bei Erstverabschiedung sowie bei Anpassungen dem Aufsichtsrat oder dem vergleichbaren Aufsichtsorgan der KVG **in geeigneter Form** zur Kenntnis zu geben und ggf. mit diesem zu erörtern.*

**Zu II. Kapitel 2, Ziff. 7 - IT-Governance: Verwahrstellen**
Textziffer 7 verweist darauf, dass die Geschäftsleitung neben der Umsetzung der IT-Aufbau- und Ablauforganisation in der eigenen KVG, diese Prozesse auch bzgl. der Schnittstellen zu Verwahrstellen und wichtigen Auslagerungsunternehmen zu verantworten hat.

Wir möchten darauf hinweisen, dass die Geschäftsleitung einer KVG insbesondere in Bezug auf Verwahrstellen keine Durchgreifmechanismen haben kann und somit eine Verantwortung der KVG-Geschäftsleitung diesbezüglich ausgeschlossen ist. Wir bitten diesen Punkt bei der Umsetzung des Rundschreibens entsprechend zu berücksichtigen.

**Zu II. Kapitel 3, Ziff. 12 – IT-Governance: IT-bezogene Geschäftsaktivitäten**
Nach Textziffer 12 hat die KVG sicherzustellen, dass die IT-bezogenen Geschäftsaktivitäten auf der Grundlage von Arbeitsablaufbeschreibungen (Organisationsrichtlinien) betrieben werden. IT-bezogene Geschäftsaktivitäten sind gemäß Erläuterungen alle Geschäftsaktivitäten, die durch IT umgesetzt oder unterstützt werden.

Nahezu alle Geschäftsprozesse einer KVG werden durch IT umgesetzt oder mindestens unterstützt. Würden sämtliche dieser Prozesse in den Organisationsrichtlinien festgehalten werden, würde deren Umfang zulasten der Nachvollziehbarkeit ausufern. Die Erläuterung sollte daher konkretisiert, bzw. eingeschränkt werden. Bspw. könnte auf solche Geschäftsaktivitäten abgestellt werden, die ***wesentlich*** durch IT umgesetzt oder unterstützt werden.

**Zu II. Kapitel 3, Ziff. 22 – Informationsrisikomanagement: Risikoanalyse**
Die derzeitigen Formulierungen in Textziffer 22 und die dazugehörigen Erläuterungen sind widersprüchlich. In der Erläuterungsspalte wird davon ausgegangen, dass die Risikoanalyse u.a. auch auf Grundlage eines Soll-Ist-Vergleichs erfolgen kann. Allerdings wird gleichzeitig in der konkreten Regelung zu Textziffer 22 die normative Aussage getätigt, dass die Risikoanalyse anhand eines Soll-Ist-Vergleichs zu erfolgen hat. Wir bitten, die Formulierungen entsprechend anzugleichen.

**Zu II. Kapitel 3, Ziff. 23 – Informationsrisikomanagement: Berichtsfrequenzen**
Gemäß Textziffer 23 soll die Geschäftsleitung mindestens vierteljährlich zu den Ergebnissen der Risikoanalyse informiert werden.

Die KAIT-E orientieren sich an dieser Stelle an den bankenaufsichtsrechtlichen Berichtsfrequenzen gemäß § 25c Abs. 4a Nr. 3d) und e) KWG, nach denen Risikoberichte mindestens vierteljährig vorzulegen sind. Die Übernahme der Berichtstaktung für Kreditinstitute würde nicht nur das aus den Spezifika und den Geschäftsmodellen hervorgehende Risikoprofil der KVGen im Vergleich zu Banken außer Acht lassen, sie stünde auch im Widerspruch zu Art. 60 Abs. 4 AIFM-VO, der lediglich eine mindestens jährliche Berichtspflicht über das Risikomanagement vorsieht.

Im Einklang mit den gesetzlichen Vorgaben und unter Berücksichtigung der Proportionalität sollten die KAIT lediglich **eine jährliche oder anlassbezogene Risikoberichtspflicht** vorsehen.

**Zu II. Kapitel 4, Ziff. 27-29 – Informationssicherheitsmanagement: Einrichtung der Funktion eines Informationssicherheitsbeauftragten**

Die Textziffern 27-29 der KAIT-E präzisieren die Regelungen für die Einrichtung einer Funktion des Informationssicherheitsbeauftragen innerhalb der KVG. Die Funktion ist dabei organisatorisch und prozessual unabhängig zu gestalten und grundsätzlich in der KVG vorzuhalten.

Wie bereits im Rahmen der Workshops dargelegt, erachten wir die Regelungen zum Informationssicherheitsbeauftragen KAIT-E als teilweise ungeeignet, da sie nicht mit den derzeitigen BSI-Empfehlungen zum IT-Grundschutz übereinstimmen.

Die BSI-Empfehlungen gehen davon aus, dass der Informationssicherheitsbeauftragte zur Wahrung der Unabhängigkeit direkt der obersten Leitungsebene zugeordnet sein muss. Dabei ist der Informationssicherheitsbeauftragte lediglich zu benennen. Die Einrichtung einer organisatorisch unabhängigen Funktion ist in den BSI-Empfehlungen demgegenüber nicht vorgesehen.

Das KAIT-Rundschreiben sollte die geltenden BSI-Empfehlungen bzgl. der IT-Sicherheit entsprechend berücksichtigen und keinen zusätzlichen prozessualen Mehraufwand für die KVGen erzeugen. Die Entscheidung, welche Einheit oder Person sich mit dem Thema Informationssicherheitsmanagement befassen soll, sollte im Ermessen der KVG liegen.

**Zu II. Kapitel 6, Ziff. 42 – IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen): Tests durch Dritte**

Zur Vermeidung von Redundanzen in Verbindung mit den Formulierungen in Textziffer 41 regen wir folgende Änderung in Textziffer 42 an:

> *Die IT-Systeme sind vor ihrer Übernahme in den produktiven Betrieb zu testen und von den fachlich sowie auch von den technisch zuständigen Mit-*

*arbeitern abzunehmen. Produktions- und Testumgebung sind dabei grundsätzlich voneinander zu trennen. ~~Diese Anforderungen gelten grundsätzlich auch bei wesentlichen Veränderungen der IT-Systeme.~~*

Außerdem möchten wir darauf hinweisen, dass die entsprechenden Erläuterungen zu Textziffer 42 in der Praxis kaum umsetzbar sind. Hierbei wird davon ausgegangen, dass bei automatisierten Änderungen, die durch Dritte durchgeführt werden, die KVG sich davon überzeugen muss, dass die notwendigen Tests bei diesem Dritten vorab durchgeführt wurden. Im Falle der Anwendung von Standardsoftware wie z.B. Office 365 ist eine solche Kontrolle der KVG faktisch nicht möglich. Wir möchten aus diesem Grund auch hier den Proportionalitätsgedanken des Rundschreibens betonen.

**Zu II. Kapitel 8, Ziff. 64 – Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen: Kriterien**

Zur grundsätzlichen Einschätzung der unter Ziff. 8, Ziff. 64 vorgesehenen Abgrenzung s. unsere Anmerkungen im einleitenden Teil. Zu der konkreten Ausformulierung möchten wir Folgendes anmerken:

Die Erläuterungsspalte unter Ziff. 64 enthält einen Positivkatalog von IT-Dienstleistungen, die in der Regel als Auslagerungen anzusehen sein sollen. Dieser – für sich genommen – sehr weitgehende Katalog wird anschließend durch verschiedene Kriterien eingeschränkt. Danach sind die katalogartig genannten IT-Dienstleistungen nur dann als Auslagerung zu werten, sofern diese längerfristig angelegt sind oder erhebliche oder kritische Auswirkungen auf die Portfolioverwaltung, das Risikomanagement oder sonstige geschäftskritische Prozesse haben oder haben können.

Wir möchten hierzu folgende Präzisierungen vorschlagen:

*In der Regel als Auslagerung von IT-Dienstleistungen zu bewerten sind:*

*[…Auflistung der IT-Dienstleistungen…],*

*sofern ~~diese~~ **die IT-Dienstleistung** längerfristig angelegt ~~sind~~ ist ~~oder~~ **und das Produkt (z.B. die Software)** erhebliche oder kritische Auswirkungen auf die Portfolioverwaltung, das Risikomanagement oder sonstige geschäftskritische Prozesse ~~haben~~ **hat** oder haben ~~können~~ **kann**.*

Begründung:

Zur Präzisierung empfehlen wir, das Kriterium der Langfristigkeit an das Dienstleistungsverhältnis und das Kriterium der erheblichen oder kritischen Auswirkungen an das Produkt (z.B. Software) zu koppeln. Durch Ersetzung des „oder“ durch ein „und“ schlagen wir ein kumulatives Vorliegen zwischen Längerfristigkeit und Auswirkungen vor. Wir erachten eine solche Anpassung angesichts des hohen Detailierungsgrades für angemessen. Die KAIT sollten – auch in Bezug auf ein zu

erwartendes „Nachziehen“ in den BAIT und den VAIT – nicht überstrenge Maßstäbe setzten, sondern einen flexibleren Rahmen beibehalten.

**Fehlen einer Übergangsregelung**

Der vorgelegte Entwurf enthält keine Übergangsregelung. Die neuen Anforderungen bedingen einen praktischen Vorlauf für organisatorische, technische und ggf. personelle Vorkehrungen. Die KVGen werden neue Prozesse einführen bzw. bestehende Prozesse prüfen und u.U. anpassen müssen. Hierzu gehören vor allem die Regelungen zum Informationssicherheitsbeauftragten und der Auslagerung von IT-Dienstleistungen.

Vor diesem Hintergrund empfehlen wir einen Übergangszeitraum von **mindestens sechs Monaten** nach Inkrafttreten.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Frederik Voigt
Abteilungsleiter Investitionskapital

Aleksandar Denic
Senior Referent Immobilien- und Kapitalmärkte