Frankfurt am Main,
14. Mai 2019

BVI[1]-Position zur Konsultation 07/2019
Entwurf eines Rundschreibens „Kapitalverwaltungsaufsichtliche Anforderungen an die IT“ (KAIT) nebst Schätzung des Erfüllungsaufwands

I. Allgemeine Anmerkungen

Wir begrüßen grundsätzlich die Initiative der BaFin, besondere aufsichtsrechtliche Vorgaben an das Management von IT-Ressourcen und das IT-Risikomanagement durch Kapitalverwaltungsgesellschaften in einem Rundschreiben festlegen zu wollen. In den Kapitalverwaltungsgesellschaften existieren bereits heute umfangreiche Prozesse zum Umgang mit Informationstechnik (IT). Diese basieren im Wesentlichen auf den allgemeinen gesetzlichen Verhaltens- und Organisationspflichten, die besondere Sorgfaltspflichten, Regeln zum Risikomanagement sowie Kontroll- und Sicherheitsvorkehrungen für den Einsatz von IT vorschreiben. Diese hat die BaFin seit 2009 in ihrem Rundschreiben über die Mindestanforderungen an Investmentgesellschaften (InvMaRisk) bzw. seit 2017 in ihrem Rundschreiben über die Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften (KAMaRisk) erläutert.

Wir verstehen den Entwurf der KAIT dahingehend, diese bestehenden Anforderungen weiter zu konkretisieren. Dies soll letztlich dazu dienen, die IT-Sicherheit im Markt zu erhöhen und das IT-Risikobewusstsein in den Kapitalverwaltungsgesellschaften zu schärfen. Hier hat unter anderem der BaFin-Workshop mit IT-Experten im Vorfeld der Konsultation gezeigt, dass Kapitalverwaltungsgesellschaften mit dem Thema sehr verantwortungsvoll umgehen und ihre IT-Systeme sowie die entsprechenden internen Prozesse kontinuierlich optimieren. Dies gilt nicht nur für Kapitalverwaltungsgesellschaften, die einer Banken- oder Versicherungsgruppe angehören und über die Gruppenaufsicht bereits zusätzlich mit den BaFin-Anforderungen an die IT für Banken und Versicherer (BAIT- und VAIT-Rundschreiben) konfrontiert sind, sondern auch für alle übrigen Häuser gleichermaßen. Die Diskussionen machten außerdem eine sehr heterogene Struktur der Kapitalverwaltungsgesellschaften in Deutschland und wesentliche Unterschiede in deren Geschäftsmodellen und Risiken deutlich. Dies wirkt sich auch erheblich auf die jeweiligen internen Prozesse im Umgang mit der IT aus. Der im Entwurf des Rundschreibens verankerte prinzipienorientierte Ansatz und der Proportionalitätsgrundsatz sind dabei sehr hilfreich.

Gleichzeitig haben wir aus dem vorangegangenen Workshop mit IT-Experten die Zielsetzung der BaFin vernommen, einen branchenübergreifenden und vergleichbaren Aufsichtsrahmen für Kapitalverwaltungsgesellschaften, Banken und Versicherer zu schaffen. Die KAIT sollen sich daher inhaltlich an den BAIT und VAIT ausrichten. Hierin sehen wir die große Herausforderung, die notwendige Balance zwischen existierenden Verwaltungspraktiken für andere beaufsichtigte Unternehmen (Banken, Versicherer) und den geschäftsspezifischen Besonderheiten von Kapitalverwaltungsgesellschaften zu finden. Dies beinhaltet, nicht nur praktische Gemeinsamkeiten und Unterschiede herauszuarbeiten, sondern auch die jeweiligen gesetzlichen Vorgaben angemessen und sachgerecht zu berücksichtigen.

[1] Der BVI vertritt die Interessen der deutschen Fondsbranche auf nationaler und internationaler Ebene. Er setzt sich gegenüber Politik und Regulatoren für eine sinnvolle Regulierung des Fondsgeschäfts und für faire Wettbewerbsbedingungen ein. Als Treuhänder handeln Fondsgesellschaften ausschließlich im Interesse des Anlegers und unterliegen strengen gesetzlichen Vorgaben. Fonds bringen das Kapitalangebot von Anlegern mit der Kapitalnachfrage von Staaten und Unternehmen zusammen und erfüllen so eine wichtige volkswirtschaftliche Funktion. Die 108 Mitgliedsunternehmen des BVI verwalten über 3 Billionen Euro Anlagekapital für Privatanleger, Versicherungen, Altersvorsorgeeinrichtungen, Banken, Kirchen und Stiftungen. Deutschland ist mit einem Anteil von 22 Prozent der größte Fondsmarkt in der EU und der am zweitschnellsten wachsende Markt.

BVI
Bundesverband Investment und Asset Management e.V.

Kontakt
Fon +49 69 15 40 90 0
www.bvi.de

BVI Berlin
Unter den Linden 42
10117 Berlin

BVI Brüssel
Rue du Trône 14–16
1000 Bruxelles

BVI Frankfurt
Bockenheimer Anlage 15
60322 Frankfurt am Main

Geschäftsführung
Thomas Richter Hauptgeschäftsführer
Rudolf Siebel Geschäftsführer

In diesem Zusammenhang ist hervorzuheben, dass die europäischen Aufsichtsbehörden ESMA, EBA und EIOPA (ESAs) zeitlich parallel zur laufenden Konsultation eines Entwurfs der KAIT die aktuelle Aufsichtspraxis für Informations- und Kommunikationstechnik (IKT) branchenübergreifend (z. B. Banken, Versicherer, MiFID-Firmen, Fondsgesellschaften, Ratingagenturen, CCPs) in sämtlichen EU-Rahmenwerken verglichen und Regelungslücken festgestellt haben.[2] Der Aufforderung der EU-Kommission in ihrem FinTech-Aktionsplan[3] vom März 2018 folgend schlagen die ESAs daher vor, die EU-Rahmenwerke entsprechend zu ergänzen. Dabei konzentrieren sie sich auf besondere Regeln zur IKT-Governance und Informationssicherheit, zur Vereinheitlichung der Meldeanforderungen sowie auf die Überprüfung von Konzentrationsrisiken bei kritischen externen Dienstleistungsanbietern mit Auswirkungen auf einzelne Unternehmen. Folgt die EU-Kommission den Empfehlungen der ESAs, müssten alle EU-Rahmenwerke branchenübergreifend (u. a. AIFM- und OGAW-Richtlinie) angepasst werden.

Angesicht der konkreten ESA-Vorschläge, **die bestehenden Regelungslücken zu füllen**, sehen wir in den Bereichen der IKT-Governance, Informationssicherheit und der Nutzung externer Dienstleister wesentliche Überschneidungen mit den beabsichtigten Anforderungen in dem KAIT-Entwurf. Aufgrund der Bedeutung des Themas erkennen wir das frühzeitige Regelungsbedürfnis der BaFin und lehnen zusätzliche Maßnahmen, die in dem Entwurf der KAIT enthalten und ohne konkrete Rechtsgrundlage von der Aufsicht eingefordert werden, nicht generell ab. Allerdings könnte das Rundschreiben im Vorgriff auf diese EU-Maßnahmen in Einzelbereichen striktere Vorgaben manifestieren, die den Wettbewerb in der EU maßgeblich beeinflussen und gerade für deutsche Kapitalverwaltungsgesellschaften besondere Hürden schaffen können. **Wir sehen dies insbesondere im Bereich der Auslagerung von IT-Dienstleistungen und bei den in dem Entwurf der KAIT festgelegten Anforderungen an die Einrichtung einer unabhängigen Funktion eines Informationssicherheitsbeauftragten. Wir bitten daher ausdrücklich, diese Anforderungen auch im Lichte der ESA-Empfehlungen und des besonderen EU-Rechtsrahmens nochmals kritisch zu prüfen.**

Ungeachtet dessen werden die neuen Anforderungen der KAIT zu einem wesentlichen einmaligen und wiederkehrenden Umsetzungsaufwand führen, den die BaFin selbst auf eine nicht unerhebliche Position im Millionen-Euro-Bereich für die Wirtschaft schätzt. Es ist daher äußerst fraglich, wie die Anforderungen des Rundschreibens ohne Übergangsfrist angemessen umgesetzt werden sollen. Dies gilt umso mehr, als in der Darstellung der BaFin wesentliche Positionen fehlen und der angegebene Erfüllungsaufwand den tatsächlichen Aufwand nicht abbildet. Wir halten daher eine **Umsetzungsfrist von mindestens zwölf Monaten** für zwingend erforderlich.

In diesem Zusammenhang ist auch dringend zu klären, ob und ab wann die besonderen Anforderungen der KAIT einer **Prüfung durch den Abschlussprüfer** unterliegen. Die seit 2015 angekündigte Neufassung der KAPrüfbV steht immer noch aus. Der letzte Konsultationsentwurf der KAPrüfbV enthält zur Prüfung der IT-Anforderungen allgemeine Anforderungen, die aus unserer Sicht die gesetzlichen Vorgaben angemessen abbilden. Angesichts des erweiterten Pflichtenumfangs in den KAIT und aufgrund der aktuellen Prüfungspraxis im Banken- und Versicherungsbereich befürchten wir, dass dem Prüfer zusätzliche Pflichten auferlegt werden könnten. Wir weisen daher bereits an dieser Stelle ausdrücklich darauf hin, dass der Prüfungsumfang des Abschlussprüfers nur die aufgrund von Gesetz geregelten Anforderungen und nicht die aufgrund von Regelungslücken zusätzlichen Aufsichtsanforderungen umfassen kann. Diese Spannungsverhältnis und der daraus resultierende Umfang der Prüfpflichten sollten daher in einem separaten Verfahren überprüft und erörtert werden.

[2] Abrufbar unter folgendem Link: https://www.esma.europa.eu/press-news/esma-news/esas-publish-joint-advice-information-and-communication-technology-risk.
[3] Abrufbar unter folgendem Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109.

II. Besondere Anmerkungen

In dem BaFin-Workshop im Vorfeld der Konsultation haben wir mit IT-Experten im Wesentlichen die rein praktischen IT-Verfahren und Auswirkungen bestimmter Vorgaben auf die einzelnen Prozesse von Kapitalverwaltungsgesellschaften erläutert, ohne die rechtlichen Fragen umfassend und abschließend zu analysieren. Zu den einzelnen Anforderungen des Entwurfs der KAIT haben wir daher folgende Anmerkungen, die insbesondere auch die rechtlichen Aspekte näher beleuchten:

1. Abgrenzung Auslagerung und Fremdbezug von Dienstleistungen

a) Keine starre Abgrenzung möglich

Wir begrüßen die Klarstellung der BaFin in den Erläuterungen zu Abschnitt II 8 Tz. 64 KAIT-E, dass es nicht ohne weiteres möglich ist, starre und zugleich praxisgerechte Kriterien für eine Abgrenzung zwischen Auslagerung und sonstigem Fremdbezug von Dienstleistungen bei Kapitalverwaltungsgesellschaften zu definieren. Die Kapitalverwaltungsgesellschaften sind daher gehalten, bei der Beauftragung eines Dritten die Abgrenzung selbst vorzunehmen. Dies entspricht im Wesentlichen der aktuellen Praxis und den bisherigen gesetzlichen und aufsichtlichen Vorgaben. § 36 KAGB legt aufgrund der EU-Vorgaben in der AIFM- und der OGAW-Richtlinie besondere Regeln zu Auslagerungen fest, die in den delegierten Rechtsakten auf EU-Ebene und durch weitere Auslegungshilfen der BaFin in den KAMa-Risk und dem BaFin-FAQ zur Auslagerung nach § 36 KAGB konkretisiert werden. Anhand derer haben Kapitalverwaltungsgesellschaften bislang angemessene Lösungen und Einzelfallentscheidungen getroffen. Auch die BaFin hat bislang in ihrem FAQ[4] zur Auslagerung die eigenverantwortliche Entscheidung der Kapitalverwaltungsgesellschaft bei der Beurteilung eines Sachverhalts als Auslagerung oder Fremdbezug von Dienstleistung in den Vordergrund gestellt.

b) Keine 1:1-Übertragung der Vorgaben aus BAIT und VAIT zur Auslagerung möglich

Wir können außerdem grundsätzlich nachvollziehen, dass seitens der Aufsicht ein Bedürfnis besteht, bestimmte Fallkonstellationen zu bilden, die offensichtlich als Auslagerung bzw. als Fremdbezug von Dienstleistungen eingestuft werden. Dies erleichtert die Aufsicht und schafft auch für die Praxis einheitliche Herangehensweisen.

Wir erkennen dabei besonders an, dass die BaFin einzelne Empfehlungen der IT-Experten mit Bezug zu den besonderen Geschäftsmodellen der Kapitalverwaltungsgesellschaften bereits berücksichtigt und die Vorgaben der BAIT und VAIT zu Auslagerungen von IT-Dienstleistungen nicht 1:1 übernommen hat. Denn unabhängig von den rein rechtlichen Fragen ist in dem Expertenworkshop sehr deutlich geworden, dass sich die Prozesse in den Kapitalverwaltungsgesellschaften aufgrund der unterschiedlichen Geschäftsmodelle wesentlich von denen der Banken und Versicherern unterscheiden. Dies berücksichtigt auch das Regelungsziel des jeweiligen Aufsichtsrechts: Während sich die Banken- und Versicherungsregeln darauf fokussieren, den Ausfall des Unternehmens zu verhindern, sind die Fondsregularien darauf gerichtet, die mit der treuhänderischen Verwaltung von Anlegergeldern einhergehenden Risiken einzudämmen. Dies hat im Übrigen auch die europäische Bankenaufsichtsbehörde EBA in ihrem Bericht[5] vom 25. Februar 2019 zur Auslagerung von kritischen und wesentlichen Funktionen bei

[4] Abrufbar unter folgendem Link: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/FAQ/faq_kagb_36_auslagerung_130710.html.
[5] Abrufbar unter folgendem Link: https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.

Instituten anerkannt. Darin hat sie insbesondere klargestellt, dass die Leitlinien nicht für bankkonzernzugehörige Fondsgesellschaften auf Einzelebene gelten sollen, sondern diese ihren eigenen sektorspezifischen Regeln nach der AIFMD und OGAW-Richtlinie unterliegen.

c) Sektorspezifische Regeln für Fondsgesellschaften berücksichtigen

Wie bereits von den ESAs kürzlich festgestellt[6], enthalten die europäischen Rahmenwerke für Fondsgesellschaften (AIFM- und OGAW-Richtlinie) bereits allgemeine Anforderungen für die Auslagerung von Aufgaben und Vorgaben für ein Auslagerungscontrolling. Hingegen fehlen für Versicherer und Banken gesetzliche Vorgaben. Hier hat lediglich die EBA für Banken bislang rechtlich unverbindliche Leitlinien zur Auslagerung von kritischen und wesentlichen Funktionen aufgestellt. Die EIOPA plant sogar erst im Laufe dieses Jahres, Leitlinien zur IT-Governance von Versicherern zu entwickeln.

In diesem Zusammenhang muss auch der Brief[7] der ESMA an die EU-Kommission zum Drittstaatenregime unter der MiFID II erwähnt werden. Ohne eine inhaltliche Wertung zu den dort adressierten Themen geben zu wollen, adressiert die ESMA Fragen zur Auslagerung von kritischen und wesentlichen Aufgaben. Insbesondere schlägt sie den Erlass konkreter Regeln unter der MiFID II nach dem Vorbild der Auslagerungsregeln unter der Delegierten Verordnung zur AIFM-Richtlinie vor. Es wäre verheerend, wenn nationale Aufsichtsbehörden neue Anforderungen an die Auslagerungsprozesse festlegen, während man in anderen Gremien auf EU-Ebene über neue gesetzliche Regeln nach dem Vorbild der AIFM-Richtlinie diskutiert. Diesem Diskussionsprozess sollte daher nicht durch zu strenge nationale und den europäischen Fondsregularien widersprechende Aufsichtspraktiken vorgegriffen werden. Dabei ist insbesondere zu beachten, dass Kapitalverwaltungsgesellschaften mit ihren Tätigkeiten im Wettbewerb mit anderen europäischen Anbietern stehen. Die Frage, ob es sich um eine Auslagerung von IT-Dienstleistungen handelt, muss daher auch im EU-Kontext und der Umsetzung in den anderen EU-Ländern bewertet werden. Gerade weil die AIFM-Richtlinie mit ihrer delegierten Verordnung im Vergleich zu den Regelungen im Banken-/Versicherungsbereich bereits umfassende Anforderungen an die Auslagerung festlegt, sollten zusätzliche aufsichtliche Anforderungen über ein BaFin-Rundschreiben auf ein Mindestmaß reduziert werden.

Unabhängig davon sind die besonderen rechtlichen Rahmenbedingungen für Fondsgesellschaften, die ihre Aufgaben des Risiko- und Portfoliomanagements regelmäßig IT-unterstützt wahrnehmen, bei der Abgrenzung entsprechend zu würdigen. Insbesondere stellt die Delegierte Verordnung (EU) 231/2013 (AIFM-VO) im Erwägungsgrund 82 fest, dass die Anforderungen an die Auslagerung für die im Anhang I der AIFM-Richtlinie genannten Verwaltungsfunktionen gelten sollen, zu denen IT-Dienstleistungen ausdrücklich nicht zählen. Erwägungsgrund 82 der AIFM-VO sieht hierfür ausdrücklich vor:

> *„… Die Einschränkungen und Anforderungen an die Übertragung von Aufgaben sollten für die in Anhang I der Richtlinie 2011/61/EU dargelegten Verwaltungsfunktionen gelten, wohingegen* ***unterstützende Aufgaben wie administrative oder technische Funktionen, die bei den Verwaltungsaufgaben eine Hilfe darstellen,*** *etwa logistische Unterstützung in Form von Reinigungsdiensten, Catering und Beschaffung von Dienstleistungen und Gütern des Grundbedarfs* ***nicht als Übertragung der Aufgaben des AIFM gelten sollten. Andere Beispiele für technische oder administrative Funktionen sind der Kauf handelsüblicher Standard-Software und die Inanspruchnahme von Software-Anbietern für Hilfe beim Betrieb handelsüblicher Systeme*** *oder die Inanspruchnahme personeller Unterstützung durch Zeitarbeitskräfte oder die Durchführung der Lohn- und Gehaltsabrechnungen.“*

[6] Abrufbar unter folgendem Link: https://www.esma.europa.eu/press-news/esma-news/esas-publish-joint-advice-information-and-communication-technology-risk.
[7] Abrufbar unter folgendem Link: https://www.esma.europa.eu/press-news/esma-news/esma-letter-european-commission-mifid-iimifir-third-country-regimes.

Dieser Ansatz resultiert aus den Feststellungen in Erwägungsgrund 31 der AIFM-Richtlinie, der wie folgt lautet:

> *„Die strengen Einschränkungen und Auflagen in Bezug auf die Übertragung von Aufgaben durch die AIFM sollten für die Übertragung des Portfolio- und Risikomanagements gemäß Anhang I gelten. Die Übertragung von Hilfsaufgaben, wie etwa vom AIFM als Teil seiner Leitungsaufgaben ausgeführte Verwaltungs- oder technische Funktionen, sollten nicht den in dieser Richtlinie festgelegten spezifischen Einschränkungen und Auflagen unterliegen."*

Nach unserem Verständnis geht der EU-Gesetzgeber daher von folgendem Ansatz aus:

1) Technische Unterstützungsdienstleistungen für die Verwaltungsaufgaben Risiko- und Portfoliomanagement sollen nicht den Anforderungen an die Auslagerung unterliegen.
2) Für die übrigen Bereiche sind Beispiele genannt, die explizit nicht als Auslagerung gelten sollen (hier: Kauf handelsüblicher Standard-Software oder die Inanspruchnahme von Software-Anbietern für Hilfe beim Betrieb handelsüblicher Systeme).
3) Alle übrigen Fälle sind nicht näher konkretisiert. Hier stellt sich die Frage, ob die Wesentlichkeit als Abgrenzungskriterium für diese Sachverhalte dienen könnte. Beispielsweise wäre dann eine unwesentliche Anpassung von Standardsoftware kein Sachverhalt, der zur Umsetzung der Auslagerungsregeln führt.

Der Entwurf der KAIT folgt bereits teilweise diesem Ansatz, indem im ersten Absatz der Erläuterungen zu Tz. 64 Regelbeispiele genannt werden, die in jedem Fall als Fremdbezug von Dienstleistungen anzusehen sind. Diesem Ansatz stimmen wir inhaltlich zu. Da Erwägungsgrund 82 der AIFM-VO lediglich auf die Inanspruchnahme von Software-Anbietern für „Hilfe" beim Betrieb handelsüblicher Systeme abstellt, bitten wir jedoch, den Begriff der „*Ad-hoc-Hilfe*" zu streichen und durch das allgemeine Wort der „*Hilfe*" zu ersetzen.

Ergänzend dazu wären wir jedoch für eine weitere Klarstellung dankbar, dass die Beauftragung oder Inanspruchnahme von lediglich unterstützenden IT-Dienstleistungen gerade nicht als Auslagerung anzusehen ist, auch wenn sie unmittelbar dem Portfolio- oder Risikomanagement dienen.

Darüber hinaus halten wir den Ansatz der Regelbeispiele, die im Absatz 2 der Erläuterungen zu Tz. 64 aufgezählt sind und die als Auslagerung zu bewerten sind, für zu generell und zu weitgehend. Die dort genannten Beispiele sind daran gebunden, dass sie längerfristig angelegt sind oder erhebliche oder kritische Auswirkung auf die Portfolioverwaltung, das Risikomanagement oder sonstige geschäftskritische Prozesse haben oder haben könnten. Dabei ist allein das Zeitelement „längerfristig" allein schon ausreichend, ohne dass es einer Wesentlichkeitsbetrachtung oder einer Bezugnahme zum Portfolio-/Risikomanagement bzw. zu den sonstigen geschäftskritischen Prozessen bedarf. Damit wären sämtliche IT-Dienstleistungen außerhalb dieser Prozesse ebenfalls immer als Auslagerung einzustufen, wenn sie längerfristig angelegt sind (z. B. die bloße Anpassung der Software an die Erfordernisse der KVG). **Hier wäre mindestens eine Koppelung des Zeitelements mit den wesentlichen Prozessen durch das Wort „*und*" erforderlich.** Zudem ist zwingend zu berücksichtigen, wie oft und in welchem Umfang sich die KVG dieser Dienstleistungen zur Unterstützung bedient. Deshalb sollte zusätzlich klargestellt werden, dass im Fall einer **nur einmaligen, gelegentlichen oder unwesentlichen Beauftragung** auch ein bloßer Fremdbezug von Dienstleistungen vorliegt, ohne dass es darauf ankommt, wie lange diese Dienstleistung in Anspruch genommen wird. Dies wäre jedenfalls auch Einklang mit dem Ansatz, den die EBA in ihren Leitlinien für Banken zugrunde gelegt hat.

d) Rechtsfolgenseite unklar

Unabhängig von den einzelnen Regelbeispielen, ist die an die Einstufung als Auslagerung geknüpfte Rechtsfolge unklar. Der Entwurf der KAIT legt lediglich fest, dass auf die Auslagerung der IT-Dienstleistungen nur die Anforderungen nach Ziffer 10 KAMaRisk und der BaFin-FAQ zur Auslagerung anwendbar sind. Formaljuristisch betrachtet müssten für Auslagerungen aber auch die Anforderungen des § 36 KAGB gelten, auf die hier nicht verwiesen wird. Die Rechtsfolgen würden sich in jedem Fall unterscheiden, weil nach § 36 KAGB Kapitalverwaltungsgesellschaften im Vergleich zu Banken und Versicherern hier deutlich höhere Anforderungen einhalten müssten. Hierzu zählen insbesondere die Rechtfertigung der Auslagerungsstruktur, die sorgfältige Auswahl und Qualifikation des Auslagerungsunternehmens, das Auslagerungscontrolling, eine Auslagerungsanzeige bei der BaFin vor Inkrafttreten der Auslagerung, die Übertragung auch auf Unterauslagerungen, besondere Haftung der KVG auch für Verschulden des Auslagerungsunternehmens und die Offenlegung im Verkaufsprospekt.

Wenn man allein die Rechtsfolgen betrachtet, wären nach unserem Verständnis auf Ebene der Kapitalverwaltungsgesellschaft folgende vier unterschiedliche Prozesse aufzusetzen:

Auslagerung von originären Aufgaben der KVG im Sinne von Anhang I der AIFM-RL (IT zählt nicht explizit dazu)	**NEU! Auslagerung von IT-Dienstleistungen**	**Fremdbezug von Dienstleistungen (ohne IT)**	**NEU! Sonstiger Fremdbezug von IT-Dienstleistungen**
• Anwendung der KAGB-Vorschriften nebst AIFM-VO (insbesondere Rechtfertigung der Auslagerungsstruktur, sorgfältige Auswahl und Qualifikation des Auslagerungsunternehmens, Auslagerungscontrolling, Auslagerungsanzeige, Unterauslagerung, besondere Haftung, Offenlegung im Verkaufsprospekt) • Anwendung Ziffer 10 KAMaRisk und BaFin-FAQ (d. h. eigenverantwortliche Risikoanalyse, ob ausgelagert werden darf, Gewährleistung der Kontinuität und Qualität auch bei Beendigung, Auslagerungsvertrag mit Informations-/Prüfungs-/Weisung-/Überwachungsrechten)	Nach Abschnitt II 8 Tz. 63 KAIT-E **nur** Verweis auf Anwendung von Ziffer 10 KAMaRisk und BaFin-FAQ zur Auslagerung	Allgemeine Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 28 KAGB	• Allgemeine Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß §§ 28-30 KAGB • **Besondere Anforderungen nach Abschnitt II 8 Tz. 65-68 KAIT-E** (d. h. besonderer Prozess zur Risikobewertung der IT-Dienstleistungen nebst Steuerung und Überwachung sowie Berücksichtigung in der Vertragsgestaltung)

Im Vergleich zu Banken und Versicherern erhöht dies den Umsetzungsaufwand wesentlich. Denn diese müssen bei der Einstufung als Auslagerung lediglich eine eigenverantwortliche Risikoanalyse durchfüh-

ren, ob die Aufgabe ausgelagert werden darf, dass die Erfüllung der Aufgaben auch bei Beendigung kontinuierlich und mit der entsprechenden Qualität gewährleistet und dass der Auslagerungsvertrag mit Informations-/Prüfungs-/Weisungs-/Überwachungsrechten ausgestattet ist. Von der Zielsetzung, auf nationaler Ebene einen branchenübergreifenden vergleichbaren Aufsichtsrahmen auch für den Bereich der Anforderungen an die Auslagerung von IT-Dienstleistungen zu schaffen, wäre man daher weit entfernt.

Es ist deshalb wichtig, die Abgrenzung der Auslagerung vom bloßen Fremdbezug von IT-Dienstleistungen besonders flexibel zu gestalten, um das bereits gesetzlich bestehende Regelungsgefälle zwischen Banken und Versicherern einerseits (keine gesetzlichen Regelungen) und Fondsgesellschaften andererseits (umfangreiche gesetzliche Regelungen) durch die KAIT nicht noch weiter zu verschärfen. Zudem sind auch Wettbewerbsnachteile für deutsche Kapitalverwaltungsgesellschaften im EU-Vergleich zu vermeiden. **Als Mindestmaßnahme wäre daher zwingend eine Klarstellung erforderlich, dass die strengen Anforderungen an die Auslagerung nach § 36 KAGB für die im Entwurf genannten Regelbespiele gerade nicht gelten, sondern allenfalls nur die Maßnahmen nach KA-MaRisk gefordert sind. Wir geben jedoch auch hier zu bedenken, dass angesichts der bestehenden Regelungslücke auch dieser Ansatz immer noch zu einem wesentlichen Aufwand bei den Kapitalverwaltungsgesellschaften und zu Unterschieden im Wettbewerb mit anderen EU-Fondsgesellschaften führen wird.**

2. Informationssicherheit (Abschnitt II 4 Tz. 27-29 KAIT-Entwurf)

Wir stimmen überein, aufsichtliche Anforderungen an die Informationssicherheit für Kapitalverwaltungsgesellschaften einheitlich festzulegen und sich hierbei an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu orientieren, weil hierfür keine gesetzlichen Vorgaben existieren. An dieser Stelle möchten wir betonen, dass die im BVI vertretenen Gesellschaften sich mit diesem Thema bereits umfassend auseinandergesetzt haben. Seit 2017 haben wir in den BVI-Wohlverhaltensregeln[8] festgelegt, dass ein Prozess zur Informationssicherheit mit klarer Aufgabenzuweisung einzurichten und die Kontrolle dieses Prozesses von geeigneten Einheiten oder Personen vorzunehmen ist, die nicht selbst für diesen Prozess verantwortlich sind (z. B. einem Informationssicherheitsbeauftragten). Auch danach erfordert das Thema IT-Sicherheit einen internen Prozess, damit Gefahren bzw. Bedrohungen abgewendet werden können. Hierfür sollten Kapitalverwaltungsgesellschaften über ausreichende Ressourcen verfügen, um den Sicherheitsprozess steuern, koordinieren, untersuchen und regelmäßig überprüfen zu können. Zudem müssen Aufgaben und Verantwortlichkeiten klar definiert werden. Diese müssen an die jeweiligen Geschäftsprozesse angepasst und auch am Proportionalitätsgrundsatz ausgerichtet sein. Der Entwurf der KAIT bietet hierfür bereits pragmatische Ansätze.

Wir wenden uns jedoch gegen folgende Ansätze in dem Entwurf der KAIT:

a) Gesamtverantwortung der Geschäftsleitung (Abschnitt II 4 Tz. 27 KAIT-Entwurf): Wir hatten in dem IT-Expertenworkshop mit der BaFin bereits das Verständnis geteilt, dass die Geschäftsleitung die Gesamtverantwortung für das Thema Informationssicherheit und die Zuweisung der damit verbundenen Aufgaben trägt und diese Gesamtverantwortung grundsätzlich nicht an Dritte weitergegeben werden darf. Dieser Grundsatz findet sich in dieser Deutlichkeit bedauerlicherweise nicht in dem Entwurf der KAIT wieder.

[8] Abrufbar unter folgendem Link: https://www.bvi.de/regulierung/selbstregulierung/wohlverhaltensregeln/.

Insbesondere ist die strikte Forderung in Abschnitt II 4 Tz. 27 KAIT-Entwurf, für jede Kapitalverwaltungsgesellschaft zwingend eine „Funktion“ eines Informationssicherheitsbeauftragten (ISB) einzurichten, nicht angemessen und auch nicht im Einklang mit den Empfehlungen des BSI. Vielmehr differenziert das BSI zwischen einer übergreifenden Organisationsstruktur für Informationssicherheit (in den KAMaRisk und den KAIT als „Prozesse“ und „Informationsmanagement“ umschrieben) und der Benennung eines ISB. Insoweit gehen die BSI-Empfehlungen davon aus, dass das Unternehmen für die Einrichtung eines Informationssicherheitsprozesses insgesamt selbst verantwortlich bleibt und als Teil dieses Prozesses ein ISB zu benennen ist.

Nach unserem Verständnis hat daher die Kapitalverwaltungsgesellschaft in Gesamtverantwortung der Geschäftsleitung einen internen Prozess für Informationssicherheit einzurichten und **als Teil dieses Prozesses einen Informationsbeauftragten zu benennen.** Die Anforderung zur Einrichtung eines entsprechenden internen Prozesses ist bereits allgemein in Abschnitt II 4 Tz. 24 KAIT-E festgelegt. **Abschnitt II 4 Tz. 27 KAIT-E** sollte daher dahingehend geändert werden, dass die Geschäftsleitung die Gesamtverantwortung trägt und keine Funktion des ISB einzurichten, sondern lediglich als Teil des Prozesses ein ISB zu benennen ist:

„27 ~~Die KVG hat die Funktion des Informationssicherheitsbeauftragten einzurichten. Diese Funktion umfasst~~ **Die Geschäftsleitung ist für den Informationssicherheitsprozess** ~~die Verantwortung für die~~ **zur** Wahrnehmung aller Belange der Informationssicherheit innerhalb der KVG und gegenüber Dritten **verantwortlich. Sie hat einen Informationssicherheitsbeauftragten zu benennen.** ~~Sie~~**Dieser** stellt sicher, dass die in der IT-Strategie, der Informationssicherheitsleitlinie und den Informationssicherheitsrichtlinien der KVG niedergelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch gegenüber Dritten transparent gemacht und deren Einhaltung überprüft und überwacht werden.	~~Die~~**Der** ~~Funktion des~~ Informationssicherheitsbeauftragte~~n~~ ~~umfasst~~ **hat** insbesondere die nachfolgenden Aufgaben: ▪ […]“

b) Unabhängigkeit des ISB: Von der Frage der Gesamtverantwortung ist die Einrichtung einer „organisatorisch und prozessual unabhängigen Funktion des ISB" zu trennen, die diese Aufgaben ausführen soll. Nach den Vorgaben im Entwurf der KAIT muss der ISB von den zuständigen Bereichen für den Betrieb und die Weiterentwicklung IT-Systeme organisatorisch und prozessual unabhängig sein. Diese Vorgabe käme einer Anforderung gleich, neben den bestehenden gesetzlich vorgeschriebenen unabhängigen Funktionen Compliance, Risikocontrolling und Interne Revision grundsätzlich eine weitere, unabhängige Organisationsfunktion einzurichten und laufend zu unterhalten. Dies geht weit über den gesetzlichen Rahmen in der AIFM- und OGAW-Richtlinie und des KAGB hinaus, der eine Funktionstrennung explizit nur für den Bereich des Risikocontrollings von den operativen Geschäften vorschreibt.

Die BSI-Leitlinien sehen außerdem eine derart strikte Funktionstrennung nicht vor. Diese sprechen zwar von einer „Funktion eines Informationssicherheitsbeauftragten“, fordern für diese aber keine Unabhängigkeit. Vielmehr empfiehlt das BSI, dass Zuständigkeiten und Kompetenzen innerhalb der Informationssicherheitsorganisation (einschließlich Vertreterregeln für wichtige Funktionen) klar definiert und zugewiesen sein müssen. Es muss daher im Ermessen der Kapitalverwaltungsgesellschaft bleiben, welche Einheit oder Personen mit dem Thema Informationssicherheit befasst ist und

in welcher Organisationseinheit dieser Prozess aufzusetzen ist. Der Begriff der „Unabhängigkeit“ taucht in den BSI-Empfehlungen nur insoweit auf, als die **Prüfungen des Informationssicherheitsprozesses** von qualifizierten und **unabhängigen** Personen durchzuführen sind. Hier geht es also um die Unabhängigkeit der Kontrolle, während der Informationssicherheitsbeauftragte selbst mit klaren Befugnissen ausgestattet sein muss.

Rein praktisch würde die strikte Funktionstrennung für Kapitalverwaltungsgesellschaften bedeuten, dass diese einen komplett neuen Organisationsprozess aufsetzen, eine unabhängige Funktion einrichten und aufgrund der Unabhängigkeit in den meisten Fällen neues Personal für einen ISB eingestellt werden müsste. Für derart eingreifende Maßnahmen fehlt es schlicht an gesetzlichen Vorgaben. Zudem gehen diese weit über das Verhältnismäßigkeitsprinzip und die BSI-Empfehlungen hinaus. Diese fordern lediglich, dass jedes Unternehmen einen ISB benennen muss, der für die Belange der Informationssicherheit zuständig ist, aber hierfür eigens keine Stelle geschaffen werden muss. Insbesondere bei Kapitalverwaltungsgesellschaften ohne wesentlich eigenen IT-Betrieb ist eine solche unabhängige Funktion äußerst fragwürdig. Zudem birgt die prozessuale Trennung von den Bereichen für den Betrieb und die Weiterentwicklung der IT-Systeme aufgrund der bestehenden Prozesse wesentliche Schwierigkeiten in der Abgrenzung. Denn die Nähe und der direkte Kontakt des ISB zu den IT-Betriebseinheiten bringt deutliche Vorteile im Tagesgeschäft (z. B. bei den Themen der Abgrenzung der Aufgaben vom Bereich der operativen Steuerung, Umgang mit Sicherheitsvorfällen, Sicherheitsüberwachung usw.). Dies gilt umso mehr, als Kapitalverwaltungsgesellschaften aufgrund ihrer Geschäftsorganisation regelmäßig gerade keine separaten Sicherheitseinheiten für einzelne Themen (z. B. Informationssicherheitsmanagementsysteme, sicherheitsbezogene Dienste, Überwachung und Prüfung usw.) vorhalten und dies auch nicht verhältnismäßig wäre.

Es ist daher zwingend in Tz. 28 KAIT-E klarzustellen, worauf sich die Unabhängigkeit zu richten hat und dass lediglich die Prüfung des Informationssicherheitsprozesses aufbauorganisatorisch von den Bereichen getrennt sein muss, die für den Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind:

„28 Die **Aufgaben** ~~Funktion~~ des Informationssicherheitsbeauftragten ~~ist organisatorisch und prozessual unabhängig~~ **sind unter Berücksichtigung eines angemessenen Interessenkonfliktmanagements** auszugestalten~~, um mögliche Interessenskonflikte zu vermeiden~~. **Die Prüfungen des Informationssicherheitsprozesses sind von qualifizierten und unabhängigen Personen durchzuführen.**	~~Zur Vermeidung möglicher Interessenkonflikte werden insbesondere folgende Maßnahmen beachtet~~*:* **Insbesondere folgende Schutzmaßnahmen gegen Interessenkonflikte kommen in Betracht:** ▪ ~~Funktions~~**Aufgaben**- und Stellenbeschreibung für den Informationssicherheitsbeauftragten und seinen Vertreter ▪ Festlegung der erforderlichen Ressourcenausstattung für ~~die Funktion des~~ **den** Informationssicherheitsbeauftragten ▪ ein ~~der Funktion~~ **den Aufgaben** zugewiesenes Budget für Informationssicherheitsschulungen in der KVG und die persönliche Weiterbildung des Informationssicherheitsbeauftragten sowie seines Vertreters ▪ unmittelbare und jederzeitige Gelegenheit zur Berichterstattung des Informationssicherheitsbeauftragten an die Geschäftsleitung ▪ Verpflichtung der Beschäftigten der KVG sowie der IT-Dienstleister zur sofortigen und umfassenden Unterrichtung des Informationssicher-

	heitsbeauftragten über alle bekannt gewordenen IT-sicherheitsrelevanten Sachverhalte, die die KVG betreffen ▪ Die **Prüfung des Informationssicherheitsprozesses** ~~Funktion des Informationssicherheitsbeauftragten~~ wird aufbauorganisatorisch von den Bereichen getrennt, die für den Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind. ▪ Der Informationssicherheitsbeauftragte nimmt keinesfalls Aufgaben der Internen Revision wahr.

- **„Funktion" grundsätzlich bei der Kapitalverwaltungsgesellschaft**: Angesichts der vorgenannten Überlegungen gehen wir von dem Verständnis aus, dass jede Kapitalverwaltungsgesellschaft originär für die Einrichtung des Prozesses für ein Informationsmanagement (einschließlich der Benennung eines Informationssicherheitsbeauftragten) verantwortlich ist. Diese Verantwortung darf auch nicht auf einen Dritten übertragen werden. Die in Tz. 29 gewählte Formulierung ist jedoch insoweit missverständlich, als sie diese Gesamtverantwortung mit den Aufgaben des Informationssicherheitsbeauftragten vermischt. Nach dem Entwurf der KAIT ist die Funktion des ISB grundsätzlich im eigenen Haus vorzuhalten. **Die Empfehlungen des BSI sagen jedoch ganz deutlich, dass die Aufgaben des Informationssicherheitsbeauftragten ohne Einschränkung auch von einem Dritten wahrgenommen werden dürfen, während das Unternehmen für die Einrichtung eines Informationssicherheitsprozesses insgesamt selbst verantwortlich bleibt.**

  Auch die von der BaFin im Expertenworkshop vorgebrachte Argumentation, dass aufgrund der Regelung in den BAIT (siehe dort Tz. 20 BAIT) ein entsprechender Aufsichtsansatz auch bei den Kapitalverwaltungsgesellschaften angesetzt werden müsse, überzeugt nicht. Denn in den VAIT für Versicherer ist die BaFin bereits von diesem Ansatz abgewichen und lässt eine Ausgliederung des ISB aufgrund der besonderen versicherungsrechtlichen Vorgaben **uneingeschränkt** zu (siehe dort Tz. 30 VAIT). Die Versicherungsaufsicht verweist lediglich darauf, dass bei der Ausgliederung der Funktion des ISB die hierfür jeweils geltenden Anforderungen zu erfüllen sind. Auch nach den gesetzlichen Vorgaben des KAGB dürfen grundsätzlich alle Aufgaben einer Kapitalverwaltungsgesellschaft an Dritte übertragen werden. **Wir fordern daher, dass die Aufgaben eines Informationssicherheitsbeauftragten uneingeschränkt von einem Dritten wahrgenommen werden dürfen und eine den VAIT entsprechende Regelung aufgenommen wird.** Tz. 29 KAIT-E ist daher wie folgt zu formulieren:

29 Jede KVG **soll** ~~hat die Funktion des~~ **den** Informationssicherheitsbeauftragten grundsätzlich im eigenen Haus vor~~zu~~halten."	KVGen können die ~~Funktion~~ **Aufgaben** des Informationssicherheitsbeauftragten grundsätzlich mit anderen Funktionen in der KVG kombinieren. Sofern eine Kombination mit der Funktion des Datenschutzbeauftragten erfolgen soll, sind ergänzend die datenschutzrechtlichen Voraussetzungen zu prüfen. ~~Nur in folgenden Fällen kann der Informationssicherheitsbeauftragte außerhalb der KVG angesiedelt werden:~~ KVGen ~~mit geringer Mitarbeiteranzahl und ohne wesentlichen eigenen IT-Betrieb, bei denen die IT-Dienstleistungen im Wesentlichen durch einen externen~~

	~~IT-Dienstleister erbracht werden,~~ können die ~~Funktion~~ **Aufgaben** des Informationssicherheitsbeauftragten auf einen fachlich qualifizierten Dritten **(z. B. im Konzern)** übertragen. ~~Konzernangehörige KVGen mit geringer Mitarbeiteranzahl und ohne wesentlichen eigenen IT-Betrieb, bei denen IT-Dienstleistungen im Wesentlichen durch konzernangehörige Unternehmen erbracht werden, können die Funktion des Informationssicherheitsbeauftragten auch auf den Informationssicherheitsbeauftragten eines übergeordneten Konzernunternehmens übertragen.~~ ~~In beiden Fällen~~ **In diesem Fall** ist in der KVG eine interne Ansprechperson für den Informationssicherheitsbeauftragten zu benennen. **Bei Übertragung der Aufgaben des Informationssicherheitsbeauftragten sind die Anforderungen an die Auslagerung gemäß § 36 KAGB zu erfüllen. Bei der Entscheidung für oder gegen die Übertragung auf einen Dritten hat die KVG das Ausmaß zu berücksichtigen, in dem IT-bezogene Geschäftsaktivitäten im eigenen Unternehmen oder durch externe Dienstleister betrieben werden. Aufbauend auf dieser Betrachtung muss die Frage eine Rolle spielen, wie eine sachgerechte Ausübung der Aufgaben des Informationssicherheitsbeauftragten gewährleistet werden kann.** Die Möglichkeit, sich externer Unterstützung per Servicevertrag zu bedienen, bleibt unberührt.

3. Strengere Regeln als in den BAIT bzw. VAIT

Der KAIT-E enthält an einzelnen Stellen neue bzw. strengere Anforderungen als die BAIT bzw. VAIT. Dem beabsichtigten vergleichbaren und branchenübergreifenden Aufsichtsrahmen für den Umgang mit IT wird damit nicht genüge getan. Insbesondere bei Kapitalverwaltungsgesellschaften, die einem Banken- oder Versicherungskonzern angehören, schafft dies Mehraufwand und unnötigen Diskussionsbedarf bei Erstellung gruppeneinheitlicher Vorgaben. Andererseits ist fraglich, weshalb Kapitalverwaltungsgesellschaften aufgrund ihrer besonderen Geschäftsstruktur zum Teil strengere Vorgaben als Banken oder Versicherer einhalten müssen. Im Einzelnen:

- **Abschnitt II 1 Tz. 4 KAIT-E (Einbindung des Aufsichtsrates in die IT-Strategie):** Die BAIT sehen keine vergleichbare Regelung vor, dass die IT-Strategie bei Erstverabschiedung sowie bei Anpassung dem Aufsichtsrat oder dem vergleichbaren Aufsichtsorgan zur Kenntnis zu geben und ggf. mit diesem zu erörtern ist. Wir halten gerade die Erörterung der Strategie mit dem Aufsichtsrat für eine überzogene Anforderung, weil dieser dadurch zu stark ins operative Geschäft eingebunden wird. Der Aufsichtsrat erhält ohnehin über die Berichte aus den Bereichen Risikomanagement und Compliance bereits sehr detaillierte Informationen. Wir bitten daher, diese Anforderung zu streichen.

- **Abschnitt II 2 Tz. 11 KAIT-E (Überwachungs- und Steuerungsprozesse):** Die Anforderung, für IT-Risiken angemessene Überwachungs- und Steuerungsprozesse einzurichten, ist weder in den BAIT noch in den VAIT vorgesehen. Wir halten eine solche Regelung nicht für erforderlich, weil bereits in den Abschnitten zuvor klargestellt wird, dass eine Kapitalverwaltungsgesellschaft konkrete Regeln zur IT-Aufbau- und IT-Ablauforganisation festlegen muss. Dies umfasst bereits entsprechende Prozesse zur Überwachung und Steuerung. Unabhängig davon geht Tz. 11 viel zu weit, weil diese Prozesse für *sämtliche* IT-Risiken fordert, ohne auf die Wesentlichkeit oder die Vorgaben der eigenen IT-Strategie der Kapitalverwaltungsgesellschaft abzustellen, auf deren Basis die Aufbau- und Ablauforganisation erfolgen soll. Wir bitten daher, Tz. 11 KAIT-E ersatzlos zu streichen.

- **Abschnitt II 2 Tz. 12 KAIT-E (Organisationsrichtlinien):** In den BAIT ist nicht vorgesehen, sicherzustellen, dass IT-bezogene Geschäftsaktivitäten auf der Grundlage von Arbeitsablaufbeschreibungen (Organisationsrichtlinien) betrieben werden. Die Erläuterungen im Entwurf der KAIT definieren zudem IT-bezogene Geschäftsaktivitäten als alle Geschäftsaktivitäten, die durch IT umgesetzt oder unterstützt werden. Da ein Großteil der Geschäftsprozesse einer Kapitalverwaltungsgesellschaft (insbesondere Fonds- und Risikomanagement) IT-unterstützt betrieben wird, müssten aufgrund der Regelung in Tz. 12 sämtliche bereits vorhandenen Organisationsrichtlinien entsprechend geprüft und um den jeweiligen IT-Bezug angepasst werden. Dies ist nicht mehr verhältnismäßig und kann auch so nicht gemeint sein. Vielmehr verstehen wir die Regelung ganz allgemein, dass die Kapitalverwaltungsgesellschaft in ihren Organisationsrichtlinien die IT-Prozesse (insbesondere Aufbau-/Ablauforganisation) beschreibt. Dies regelt bereits Abschnitt 6 Tz. 2 und 3 KAMaRisk für sämtliche Geschäftsaktivitäten einer Kapitalverwaltungsgesellschaft. Da Tz. 6 KAIT-E auf diese Regelung verweist, halten wir weitere Ausführungen nicht für erforderlich.

- **Abschnitt II 2 Tz. 13 KAIT-E (Qualifikation der Mitarbeiter):** Die hier festgelegten Anforderungen an die besondere Qualifikation der Mitarbeiter sind in den BAIT nicht festgelegt. Wir halten Ausführungen hierzu in den KAIT ebenfalls nicht für erforderlich, weil Kapitalverwaltungsgesellschaften bereits gesetzlich verpflichtet sind, dass ihre Mitarbeiter ausreichend qualifiziert sind (vgl. § 28 Abs. 1 Satz 2 Nr. 2 KAGB iVm. Art. 22 AIFM-VO).

- **Abschnitt II 2 Tz. 14-15 KAIT-E (Störungen und Notfallmaßnahmen):** Die hier festgelegten Anforderungen an den Umgang mit Störungen und die Notfallkonzepte sind weder in den BAIT noch in den VAIT festgelegt. Wir halten hier besondere Anforderungen in den KAIT ebenfalls nicht für erforderlich, weil Kapitalverwaltungsgesellschaften bereits gesetzlich verpflichtet sind, Notfallkonzepte (auch im Störungsfall) aufzustellen (vgl. § 28 Abs. 1 KAGB iVm. Art. 57(3) AIFM-VO).

- **Abschnitt II 4 Tz. 24 und 31 KAIT-E (Berichtspflichten an den Aufsichtsrat)**: Der Entwurf der KAIT enthält unter Ziffer 24 am Ende einen Verweis auf die KAMaRisk und bestimmt, dass der Informationssicherheitsbeauftragte auch an den Aufsichtsrat zu berichten hat. In Ziffer 31 ist wiederum nur von Berichten an die Geschäftsführung die Rede; weitere Vorgaben für den Bericht an den Aufsichtsrat finden sich nicht. Dies ist einerseits schon in sich inkonsistent. Andererseits geht dies auch über die Vorgaben der BAIT und VAIT hinaus, die keine Berichtspflicht des Informationssicherheitsbeauftragten an den Aufsichtsrat vorsehen. Wir schlagen daher vor, die Wörter „*sowie den Aufsichtsrat*“ in Ziffer 24 zu streichen.

  Nur äußerst hilfsweise, soweit keine Streichung erfolgt, wäre zwingend klarzustellen, dass für den Aufsichtsrat kein zusätzlicher IT-Sicherheitsbericht erstellt werden muss, sondern die Berichtspflicht auch über die ohnehin bereits regelmäßig vom Risikomanagement an den Aufsichtsrat gelieferten

Berichte erfüllt werden kann, indem hier ein zusätzlicher Passus zur Informationssicherheit aufgenommen wird.

4. Umgang mit Interessenkonflikten

Der Entwurf des Rundschreibens enthält an vielen Stellen die Aussage, dass Interessenkonflikte zu vermeiden sind. Dies geht über die gesetzlichen Anforderungen hinaus. Diese verlangen lediglich, dass die Kapitalverwaltungsgesellschaft Interessenkonflikte ermitteln und Maßnahmen zur Verhinderung von Schäden für Fonds und Anleger treffen muss. Darüber hinaus sind unvermeidbare Interessenkonflikte zulässig, solange die Anleger informiert werden und die Gesellschaft Verfahren und Strategien entwickelt (vgl. § 27 Abs. 4 KAGB und Art. 20 der OGAW-Durchführungsrichtlinie 2010/43/EU). Wir bitten daher, die Formulierungen jeweils anzupassen. Unsere Änderungsvorschläge entsprechen im Übrigen auch den gefundenen Formulierungen in den KAMaRisk, die die BaFin seinerzeit ebenfalls im Konsultationsverfahren entsprechend angepasst hat. Ein Gleichlauf der Aufsichtsregeln ist geboten. Im Einzelnen betrifft dies folgende Punkte:

- **Abschnitt II 2 Tz. 9 KAIT-E (vgl. hierzu auch Abschnitt 4.3 Tz. 4 KAMaRisk):**

  „~~**Interessenkonflikte und unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation sind zu vermeiden.**~~ **Bei der Ausgestaltung der IT-Aufbau- und IT-Ablauforganisation ist sicherzustellen, dass miteinander unvereinbare Tätigkeiten unter Berücksichtigung eines angemessenen Interessenkonfliktmanagements durchgeführt werden**."

- **Abschnitt II 3 Tz. 18 KAIT-E:**

  „Die Bestandteile eines Systems zum Management der Informationsrisiken sind unter Mitwirkung aller maßgeblichen Stellen und Funktionen kompetenzgerecht und ~~**frei von**~~ **unter Berücksichtigung eines angemessenen** Interessenkonflikt~~**en**~~**managements** umzusetzen.

- **Abschnitt II 4 Tz. 28 KAIT-E (vgl. unsere obigen Ausführungen zur Unabhängigkeit des ISB):**

  „Die **Aufgaben** ~~Funktion~~ des Informationssicherheitsbeauftragten ~~**ist**~~ **sind unter Berücksichtigung eines angemessenen Interessenkonfliktmanagements** ~~**organisatorisch und prozessual unabhängig**~~ auszugestalten~~**, um mögliche Interessenskonflikte zu vermeiden**~~.

- **Erläuterungen zu Abschnitt II 4 Tz. 28 KAIT-E:**

  „~~**Zur Vermeidung möglicher Interessenkonflikte werden**~~ Insbesondere folgende **Schutzm**~~**M**~~aßnahmen **gegen Interessenkonflikte kommen in Betracht** ~~**beachtet**~~: […]"

- **Abschnitt II 5 Tz. 33 Satz 2 KAIT-E:**

  „[…] Berechtigungskonzepte haben die Vergabe von Berechtigungen an Benutzer nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) sicherzustellen, die Funktionstrennung zu wahren und Interessenskonflikte des Personals ~~**zu vermeiden**~~**angemessen zu berücksichtigen**."

5. Abschnitt II 3 Tz. 23 und Abschnitt II 4 Tz. 31 KAIT-E: Frequenz der Berichte

Die aufsichtsrechtlichen Anforderungen an die Frequenz der Berichte von Banken und Kapitalverwaltungsgesellschaften unterscheiden sich. Während für Banken vierteljährliche Risikoberichte gesetzlich vorgeschrieben sind (vgl. § 25c Abs. 4a Nr. 3d-e KWG), müssen Kapitalverwaltungsgesellschaften Risikoberichte mindestens einmal jährlich erstellen (vgl. Art. 60(4) AIFM-VO). Diesem Umstand tragen die KAMaRisk bereits besonders Rechnung (vgl. Abschnitt 4.9 Tz. 2 KAMaRisk), wonach der Geschäftsleitung in regelmäßigen Abständen zu berichten und diese bei kritischen Sachverhalten unverzüglich zu informieren ist. Auf diese Regelung verweist der Entwurf der KAIT ausdrücklich. Da der Bericht über die Risikoanalyse des IT-Managements und zur Informationssicherheit regelmäßig Gegenstand des allgemeinen Risikoberichts der KVG sein wird, sollten diese "Berichte" zeitlich nicht auseinanderfallen. Viele Kapitalverwaltungsgesellschaften berichten bereits vierteljährlich. Allerdings muss es einer Kapitalverwaltungsgesellschaft auch unbenommen bleiben, z. B. aufgrund ihrer geringeren Risikosituation weiterhin nur von einer mindestens jährlichen Berichtspflicht Gebrauch zu machen. Wir regen daher an, **Abschnitt II 3 Tz. 23 KAIT-E** wie folgt anzupassen:

> "Die Geschäftsleitung ist regelmäßig, mindestens jedoch ~~vierteljährlich~~ **jährlich** ***[alternativ: im Turnus der Risikoberichte]***, insbesondere über die Ergebnisse der Risikoanalyse sowie Veränderungen an der Risikosituation zu unterrichten (Statusbericht)."

Ebenso sollte **Abschnitt II 4 Tz. 31 KAIT-E** im Hinblick auf die Berichtspflicht des Informationssicherheitsbeauftragten angepasst werden:

> "Der Informationssicherheitsbeauftragte hat der Geschäftsleitung regelmäßig~~, mindestens vierteljährlich,~~ über den Status der Informationssicherheit sowie anlassbezogen zu berichten."

6. Erfüllungsaufwand und Umsetzungsfrist

Das Rundschreiben KAIT führt erstmals einheitliche aufsichtliche Vorgaben für interne Prozesse an das Management von IT-Ressourcen, an das IT-Risikomanagement und zum Thema Informationssicherheit ein. Auch wenn KVGs bereits einzelne Prozesse vorhalten, müssen diese anhand der Vorgaben überprüft und angepasst sowie erstmals neu umgesetzt werden. Dabei haben wir folgenden wesentlichen Anpassungs- und Umsetzungsbedarf identifiziert:

- Festlegung einer nachhaltigen IT-Strategie
- Überprüfung und ggf. Anpassung der internen Organisationsrichtlinien nebst Notfallmaßnahmen bzgl. IT-bezogener Geschäftsaktivitäten
- Arbeitsanweisungen an Mitarbeiter
- Festlegung bzw. Überprüfung/Anpassung von Kriterien zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche
- Festlegung bzw. Überprüfung/Anpassung der Prozesse für ein Informationsrisikomanagement nebst besonderer Berichtspflichten
- Beschließen einer Informationssicherheitsleitlinie nebst konkretisierender Informationssicherheitsrichtlinien und Informationssicherheitsprozesse
- Einrichtung einer [*unabhängigen*] Funktion eines Informationssicherheitsbeauftragten nebst neue Berichtspflichten
- Interne Schulungsmaßnahmen
- Einbindung von IT-Risiken und wesentlichen IT-Projektrisiken ins Risikomanagement
- Überprüfung/Anpassung der Prozesse nebst Berichterstattung für IT-Projekte

- Festlegung bzw. Überprüfung/Anpassung des Benutzerberechtigungsmanagements (insbesondere Berechtigungskonzepte, Zentralverzeichnis)
- Überprüfung/Anpassung der Prozesse zur Anwendungsentwicklung nebst IDV (insbesondere Schutzbedarfsklassifizierung, zentrales Anwendungsregister)
- Überprüfung/Anpassung der Prozesse zum IT-Betrieb (Bestandsangaben, Änderungen, Datensicherungskonzepte) nebst Umgang mit Störungen und Berichtspflichten
- Konzept zur Abgrenzung Auslagerung vs. Fremdbezug von IT-Dienstleistungen, Risikobewertung für Fremdbezug von Dienstleistungen, Überprüfung/Anpassung bestehender Verträge

Der ebenfalls zur Konsultation gestellte **Erfüllungsaufwand** zeigt daher nur einen Ausschnitt dessen, was Kapitalverwaltungsgesellschaften einmalig und wiederkehrend umsetzen müssen. Ergänzend zu den vorstehenden Punkten vermissen wir sowohl beim einmaligen als auch bei dem wiederkehrenden Erfüllungsaufwand insbesondere folgende Positionen:

- **Prozesse zum Informationsrisikomanagement**. Dies ist ein nicht zu unterschätzendes Thema, das Prozessdefinitionen, Dokumentationen und Schnittstellen von und zu den operationellen Risiken nach sich zieht. Dies gilt auch für die Anforderungen an nachvollziehbare Verfahren der Schutzbedarfsfeststellung, Sicherheitskonzeption und daraus abgeleitete Risikoanalysen inklusive der Behandlung selbiger Aufwandstreiber. Da das gesamte Thema IT-Risikomanagement nicht isoliert von den Fachbereichen gesehen werden und betrieben werden darf, zieht dies ebenfalls weiteren Erfüllungsaufwand nach sich.

- Es ist bereits jetzt absehbar, dass der im Abschnitt II 6 des KAIT-E unter „**IT-Projekte, Anwendungsentwicklung**“ im Klammerzusatz genannte Punkt zu den durch Endbenutzer in den Fachbereichen selbst entwickelten Anwendungen (z. B. individuelle Datenverarbeitung – IDV) zu einem erheblichen Aufwandsposten wird. Hier rechnen wir sowohl mit vielen Erstaufwänden (z. B. initiale Regelungen und Sollvorgaben der IDV) als auch mit wiederkehrenden Aufwänden bei der Prüfung der Umsetzung von Vorgaben und der regelmäßigen Rezertifizierung der erfassten Anwendungen und deren Einstufung (hier bezogen auf den Schutzbedarf usw.).

- Unklar ist auch, ob und inwieweit die im Entwurf der KAIT geforderten besonderen Regelungen zur Risikobewertung bei Auslagerungen und des sonstigen Fremdbezugs von IT-Dienstleistungen auch für **Bestandsverträge** oder erst für Neuverträge gelten. Nach **Abschnitt II 8 Tz. 67 KAIT-E** sind die aus der Risikobewertung abgebildeten Maßnahmen in den vertraglichen Vereinbarungen zum Informationsrisikomanagement, zum Informationssicherheitsmanagement und zum Notfallmanagement zu berücksichtigen. Gleichzeitig fordert **Abschnitt II 2 Tz. 7 KAIT-E**, dass die Regelungen zur IT-Aufbau- und IT-Ablauforganisation auch bezüglich der Schnittstellen zu wichtigen Auslagerungsunternehmen umgesetzt werden müssen. Soweit auch die bestehenden Verträge überprüft und ggf. nach vorheriger Vertragsverhandlung angepasst werden müssen, ist dies ebenfalls ein erheblicher Aufwand, den Kapitalverwaltungsgesellschaften nicht innerhalb kürzester Zeit leisten können. Selbst die EBA, die in ihren Leitlinien zur Auslagerung von kritischen und wesentlichen Funktionen besondere Regelungen für Auslagerungen von IT-Dienstleistungen festlegt, hat hier den Umsetzungsaufwand erkannt und eine allgemeine Umsetzungsfrist sowie eine Übergangsfrist bis zum 31. Dezember 2021 für Bestandsverträge bei den betroffenen Instituten festgelegt.

Darüber hinaus können wir nicht nachvollziehen, auf welcher Basis die BaFin den Erfüllungsaufwand geschätzt hat. Das **Standardkostenmodell**, auf das die BaFin verweist, wird nicht näher erläutert. Allerdings bezweifeln wir, dass die BaFin den jeweils angegebenen zeitlichen Erfüllungsaufwand angemessen geschätzt hat. Beispielhaft sind zu nennen:

- Der einmalige Erfüllungsaufwand für die Erstellung von Organisationsrichtlinien für die IT-bezogenen Geschäftsaktivitäten ist mit 495 Minuten (was 8,25 Stunden entspricht) viel zu niedrig. Hier müssen die Kapitalverwaltungsgesellschaften viele Schnittstellen zu bestehenden Richtlinien anpassen, da die IT nicht isoliert bearbeitet werden kann. Je nach Geschäftsorganisation, Größe, Art um Umfang der Kapitalverwaltungsgesellschaft ist dies kaum an einem Tag zu bewältigen.

- Auch die Einrichtung einer Funktion eines [*unabhängigen*] Informationssicherheitsbeauftragten erscheint mit einmalig 60 Stunden und einem durchschnittlichen Erfüllungsaufwand von etwa 3.200 Euro pro Gesellschaft unmöglich (hier: angegebener wiederkehrender Gesamterfüllungsaufwand von 439.670,68 Euro geteilt durch angegebene Fallzahl von 137), wenn eine Kapitalverwaltungsgesellschaft hierfür zunächst eine Stelle schaffen, Bewerbungsgespräche führen und einen geeigneten Mitarbeiter finden muss. Gleiches gilt für die laufende Unterhaltung dieser Stelle, deren zugewiesenen Aufgaben gemäß dem Entwurf der KAIT wohl kaum in 442 Minuten (7,3 Stunden) und mit einem durchschnittlichen Erfüllungsaufwand von etwa 478 Euro pro Gesellschaft (hier: angegebener wiederkehrender Gesamterfüllungsaufwand von 65.544,66 Euro geteilt durch angegebene Fallzahl von 137) erfüllbar ist. Hier dürfte allein die vorgesehene vierteljährliche Berichterstattung den geschätzten Rahmen sprengen.

Angesichts der selbst von der BaFin geschätzten nicht unerheblichen Positionen im Millionen-Euro-Bereich für den Erfüllungsaufwand der Wirtschaft ist äußerst fraglich, wie die Anforderungen des Rundschreibens ohne Übergangsfrist angemessen umgesetzt werden sollen. Wir halten daher eine **Umsetzungsfrist von mindestens zwölf Monaten** für zwingend erforderlich.

****