INSTITUT DER WIRTSCHAFTSPRÜFER

Institut der Wirtschaftsprüfer
in Deutschland e. V.

Wirtschaftsprüferhaus
Tersteegenstraße 14
40474 Düsseldorf
Postfach 32 05 80
40420 Düsseldorf

TELEFONZENTRALE:
+49 (0) 211 / 45 61 - 0

FAX GESCHÄFTSLEITUNG:
+49 (0) 211 / 4 54 10 97

INTERNET:
www.idw.de

E-MAIL:
info@idw.de

BANKVERBINDUNG:
Deutsche Bank AG Düsseldorf
IBAN: DE53 3007 0010 0748 0213 00
BIC: DEUTDEDDXXX
USt-ID Nummer: DE119353203

Bundesanstalt für Finanzdienstleistungsaufsicht
Referat WA 46
Marie-Curie-Straße 24-28
60439 Frankfurt am Main

Düsseldorf, 14. Mai 2019

[567/579]

via E-Mail: Konsultation-07-19@bafin.de

Stellungnahme im Rahmen der Konsultation 07/2019
Geschäftszeichen WA 46-FR 1903-2018/0001
Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)

Sehr geehrte Damen und Herren,

wir danken Ihnen für die Gelegenheit, aus Sicht des Berufsstands der Wirtschaftsprüfer zum Entwurf eines Rundschreibens der BaFin zu „Kapitalverwaltungsaufsichtlichen Anforderungen an die IT (KAIT)“ Stellung nehmen zu dürfen.

A. Allgemeine Anmerkungen (zu Abschnitt I. "Vorbemerkung" Tz. 1 und 2)

Unzweifelhaft ist der Einsatz von Informationstechnik (IT) von herausragender Bedeutung für die Geschäftstätigkeit der Kapitalverwaltungsgesellschaften (KVGen). In der Praxis kommt es dabei häufig auch zu Fremdbezug oder Auslagerungen der IT.

Der Entwurf des KAIT Rundschreibens (KAIT-E) führt aus, dass sich die Vorgaben an die Organisationspflichten, das Risikomanagement und die Auslagerung (neben § 36 KAGB) in erster Linie nach den Artikeln 38 bis 66 sowie 75 bis 82 der AIFM Level 2-VO bestimmen. Das Rundschreiben konkretisiere "Teile dieser Regelungen und ist daher erst in zweiter Linie zur Bestimmung der Mindestanforderungen an die aufsichtlichen Anforderungen an die IT der KVG heranzuziehen".

Gleichzeitig sollen durch das Rundschreiben Teile der KAMaRisk – die im Übrigen unberührt bleiben sollen – konkretisiert werden.

Diese beiden "Anwendungshinweise" für das neue Rundschreiben führen u.E. für die Prüfungspraxis zu einem Nebeneinander von Quellen mit Vorgaben für den Einsatz, Fremdbezug sowie Auslagerungslösungen von IT sowie u.a. auch aufgrund der Verweistechnik des KAGB zu ggf. schwierigen Abgrenzungsfragen. Zum Beispiel könnte für registrierte KVGen unklar sein, welche Anforderungen zu den allgemeinen Organisationsanforderungen i.S.d. § 28 Abs. 1 Nr. 1 KAGB und welche Anforderungen zu den Anforderungen an das Risikomanagement i.S.d. § 29 KAGB (vgl. dazu auch Abschnitt B. 2.) gehören.

Das Nebeneinander einer Vielzahl von Quellen mit Anforderungen an den Einsatz von IT erhöht u.E. für den Anwender die Gefahr einer mehrfachen Befassung mit inhaltlich gleichlautenden Anforderungen oder kann – im ungünstigsten Fall – ggf. auch zu widersprüchlichen Anforderungen bzw. Auslegungen auf europäischer gegenüber nationaler Ebene führen.

Vor dem Erlass der KAIT regen wir daher an, folgende Lösungsansätze zu erwägen:

1. Im Falle der Inanspruchnahme des Europäischen Passes und damit auch grenzüberschreitender Lösungen für den Einsatz von IT sollte einer europäischen Formulierung gemeinsamer Mindestanforderungen für KAIT auf Basis der Vorschriften der AIFM Level 2-VO der Vorzug gegeben werden.
2. Nationale Besonderheiten und Konkretisierungen sollten in die KAMaRisk (insbesondere in Abschnitt 8) integriert werden.

Ferner regen wir an, die beiden Empfehlungen zur IT des Joint Committee der ESAs an die Kommission[1], die am 10. April 2019 (d.h. nach Beginn der KAIT-Konsultation) veröffentlicht wurden, bei der endgültigen Formulierung der KAIT zu berücksichtigen. So könnte in den Vorbemerkungen neben dem Hinweis auf (bisher) gängige Standards z.B. auf eine mögliche Anwendung des (freiwilligen) Rahmenwerks EU-TIBER[2] als aktuelle Weiterentwicklung hingewiesen werden.

---

1 https://www.esma.europa.eu/press-news/esma-news/esas-publish-joint-advice-information-and-communication-technology-risk

2 https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

B. Anwendungsbereich (zu Vorbemerkung I. Tz. 3 und 4)

1. Allgemeiner Anwendungsbereich der KAIT

Der Anwendungsbereich der KAIT sollte u.E. parallel zum Anwendungsbereich der KAMaRisk ausgestaltet werden. So ergeben sich für OGAW die Anforderungen an die Ausgestaltung des Risikomanagements nicht aus der AIFM-Level 2-VO, sondern unmittelbar aus den §§ 28, 29 und 30 KAGB und werden in §§ 4-6 KAVerOV näher bestimmt (vgl. Abschnitt 1 Satz 1 KAMaRisk).

Darüber hinaus ist der Einsatz von IT nicht nur für die Kerndienstleistungen der kollektiven Vermögensverwaltung und des Risikomanagements in Bezug auf die kollektive Vermögensverwaltung von tragender Bedeutung, sondern z.B. auch für die Buchhaltung und Rechnungslegung sowie damit verbundene Aufzeichnungspflichten.

Der Hinweis am Ende der Tz. 3, wonach "Schnittstellen" zu der Verwahrstelle oder einem "Fondsadministrator" zu berücksichtigen sind, ist u.E. unklar. Während der Aufgabenkreis der Verwahrstelle gesetzlich festgelegt ist, bleibt unklar, was genau mit der Schnittstelle zu einem "Fondsadministrator" gemeint ist. Nach unserem Verständnis ist die Aufgabe eines "Fondsadministrators" jedenfalls in Zusammenhang mit der Buchhaltung und der Rechnungslegung für Sondervermögen originäre Aufgabe der KVG; der Fondsadministrator wäre also gleichzeitig ein Auslagerungsunternehmen und die KVG müsste in dieser Konstellation nicht nur die Schnittstelle zu dem Fondsadministrator berücksichtigen, sondern den Sachverhalt insgesamt als Auslagerung behandeln. Die KVG wäre somit auch dafür verantwortlich, dass der Auslagerungspartner die Einhaltung der KAIT gewährleistet.

Auch für Nebendienstleistungen mit Wertpapierdienstleistungsbezug regen wir an, den Anwendungsbereich parallel zu den KAMaRisk auszugestalten.

2. Anwendung der KAIT auf extern verwaltete Investmentgesellschaften

Eine Anwendung der KAIT für extern verwaltete Investmentgesellschaften ist gemäß Tz. 4 explizit nicht vorgesehen. Die Verantwortung für die Beachtung der KAIT wird der externen KVG zugewiesen.

Dabei wird u.E. die mögliche Ausstrahlungswirkung der KAIT auf die Buchhaltung und Rechnungslegung der Investmentgesellschaft nicht ausreichend berücksichtigt. Während die Verantwortung für die Rechnungslegung nach den gesellschaftsrechtlichen Regelungen bei der Geschäftsleitung der Investmentgesellschaft verbleibt, kann die Buchhaltung als "administrative Tätigkeit" der

kollektiven Vermögensverwaltung verstanden werden (§ 1 Abs. 19 Nr. 24 KAGB). Die "Schnittstelle" zwischen der externen KVG als Verwalter und der Investmentgesellschaft als Rechnungslegungspflichtigem sollte in den KAIT daher ebenfalls Berücksichtigung finden; z.B. dergestalt, dass die externe KVG die Investmentgesellschaft jedenfalls für die Konzeption (bzw. bei wesentlichen Änderungen) rechnungslegungsrelevanter IT-Lösungen einzubeziehen hat.

3. Anwendung der KAIT auf nach § 44 KAGB registrierte Kapitalverwaltungsgesellschaften (KVGen)

Die Aufzählung zu Beginn der Tz. 4 schließt registrierte KVGen unterschiedslos von der zwingenden Anwendung der KAIT aus.

Zur Vermeidung von Widersprüchen zum Anwendungsbereich gemäß Abschnitt 2 Tz. 1 der KAMaRisk sowie aus den nachfolgenden Gründen regen wir an, den Anwendungsbereich für registrierte KVGen parallel zu Abschnitt 2 Tz. 1 der KAMaRisk auszugestalten bzw. entsprechend klarzustellen:

a) Registrierte KVGen unter der Ausnahme des § 2 Abs. 5 KAGB:

Für registrierte KVGen unter der Ausnahme des § 2 Abs. 5 KAGB sind die Anforderungen des § 28 KAGB (Allgemeine Organisationspflichten) anwendbar.

Obwohl nach der Aufzählung in Tz. 4 registrierte KVGen (unterschiedslos) von der Anwendung der KAIT ausgeschlossen werden, weist Tz. 4 vorletzter Absatz für registrierte KVG unter der Ausnahme des § 2 Abs. 5 KAGB auf die Anwendung des § 28 KAGB (Allgemeine Organisationspflichten) hin. § 28 Abs. 1 Satz 2 Nr. 5 KAGB fordert hierbei ausdrücklich angemessene Kontroll- und Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung, die jetzt nach unserem Verständnis in den KAIT festgelegt werden sollen. Darüber hinaus wird auch klargestellt, dass die KAMaRisk (mit Ausnahme der Regelungen zur Auslagerung) für die KVGen unter der Ausnahme des § 2 Abs. 5 KAGB anwendbar ist. Da die KAIT u.a. die Organisationspflichten des § 28 KAGB und damit gleichzeitig auch die jeweiligen korrespondierenden Anforderungen der KAMaRisk konkretisieren, könnten sich hieraus Anwendungsfragen in der Praxis ergeben. Wir regen daher an, einen möglichen Widerspruch in Tz. 4 bezüglich der Anwendung der KAIT auf registrierte KVGen zu vermeiden.

b) Registrierte KVG unter der Ausnahme des § 2 Abs. 4 KAGB:

Für registrierte KVGen unter der Ausnahme des § 2 Abs. 4 KAGB finden für den Fall der Gewährung von Gelddarlehen u.a. die Vorschriften an das Risikomanagement nach § 29 Abs. 1, 2, 5 und 5a KAGB und § 30 Abs. 1 bis 4 KAGB

Anwendung. Nach § 29 Abs. 5a KAGB gelangen solche KVGen damit zumindest teilweise in den Anwendungsbereich der KAMaRisk. Da Einsatz oder Fremdbezug von IT im Zusammenhang mit der Anwendung des Abschnitts 5 der KAMaRisk von Bedeutung sind, ist es u.E. nicht sachgerecht, die Anwendung der KAIT für diese Aufgaben der KVG auszuschließen.

C. Anwendung des Proportionalitätsprinzips (zur Vorbemerkung I. Tz. 3)

Nach unserem Verständnis handelt es sich bei den KAIT um Mindestanforderungen, die – werden sie von einer KVG sachgerecht erfüllt – den aufsichtsrechtlichen Anforderungen Genüge tun. Von diesem Verständnis ausgehend, kann eine Fallkonstellation, in der von einer KVG darüber hinausgehende Vorkehrungen getroffen werden müssten, um die aufsichtsrechtlichen Mindestanforderungen zu erfüllen, nicht bestehen bzw. nach unserem Verständnis bei sachgerechtem Umgang mit den KAIT auch nicht gefordert werden.

Darüber hinaus könnte die Darstellung des Proportionalitätsprinzips in Tz. 3 KAIT-E dahingehend interpretiert werden, dass Unterschreitungen der Mindestanforderungen der KAIT unter Berücksichtigung der Größe, Komplexität und Risikopositionierung der KVG und damit – anders als im Falle der KAMaRisk – ebenfalls nicht möglich sind.

Wir regen daher an, das Proportionalitätsprinzip in Tz. 3 entsprechend den KAMaRisk zu formulieren.

D. Informationssicherheitsbeauftragter (zu Abschnitt 4. Tz. 29)

1. *Kombination des Informationssicherheitsbeauftragten mit dem Datenschutzbeauftragten*

Tz. 29 Abs. 1 KAIT-E sieht die Möglichkeit einer Personalunion von Informationssicherheitsbeauftragtem und Datenschutzbeauftragtem vor, sofern die datenschutzrechtlichen Anforderungen dem nicht entgegenstehen.

Damit kommt dem externen Prüfer auch die Aufgabe zu, jeweils individuell zu prüfen, ob die Anforderungen der EU-Datenschutzgrundverordnung sowie des Bundesdatenschutzgesetzes einer solchen Personalunion entgegenstehen. Die Funktion des Informationssicherheitsbeauftragten wird aufsichtsrechtlich durch die KAIT mit einem klar definierten Aufgabenkatalog unterlegt.

Die Vereinbarkeit der Vereinigung beider Funktionen in einer Person ist daher u.E. eine Frage, die generell abstrakt anhand der relevanten

Datenschutzvorschriften von der BaFin einheitlich beantwortet werden sollte. Dementsprechend sollte u.E. hierzu eine eindeutige Aussage in den KAIT getroffen werden.

Darüber hinaus weisen wir darauf hin, dass die Funktion des Informationssicherheitsbeauftragten und die Funktion des Datenschutzbeauftragten unterschiedliche Stoßrichtungen haben und sich insofern die Frage stellt, ob es durch die Kombination der beiden Funktionen in einer Person nicht zwangsläufig zu Interessenskonflikten kommt. Während die Funktion des Informationssicherheitsbeauftragten dem Schutz des Assets „Information“ dient, ist der Datenschutzsicherheitsbeauftragte in seiner Funktion dem Schutz des Betroffenen verpflichtet. Wir regen daher an, die Formulierung an die in den BAIT verwendete Formulierung anzupassen; dort heißt es: "Institute können die Funktion des Informationssicherheitsbeauftragten grundsätzlich mit anderen Funktionen im Institut kombinieren" (BAIT, Tz. 20). Darüber hinaus regen wir für den Fall, dass die Funktion des Informationssicherheitsbeauftragten mit anderen Funktionen im Unternehmen kombiniert wird, eine Klarstellung an, wonach die Abgrenzung zwischen beiden Funktionen klar definiert werden muss, um Interessenskonflikte zu vermeiden.

2. Externer Dritter als Informationssicherheitsbeauftragter

Anders als die BAIT und VAIT eröffnen die KAIT-E bestimmten KVGen die Möglichkeit, einen "fachlich qualifizierten" externen Dritten mit der Funktion des Informationssicherheitsbeauftragten zu betrauen. Abschnitt 4 Tz. 29 KAIT-E beschränkt diese Möglichkeit zunächst auf KVGen mit einer geringen Mitarbeiterzahl und ohne wesentlichen eigenen IT-Betrieb. Eine Definition, was unter geringer Mitarbeiterzahl bzw. wesentlichem IT-Betrieb zu verstehen ist, enthält Tz. 29 KAIT-E nicht.

Tz. 29 KAIT-E sieht ferner vor, dass für den Fall der Auslagerung des IT-Betriebs an einen externen IT-Dienstleister, die Funktion des Informationssicherheitsbeauftragten einem fachlich qualifizierten Dritten übertragen werden kann. Aufgrund der Differenzierung zwischen „externem IT-Dienstleister“ auf der einen Seite und „einem fachlich qualifizierten Dritten“ andererseits scheint eine Übertragung der Funktion auf einen Mitarbeiter des externen IT-Dienstleisters ausgeschlossen. In diesem Zusammenhang ist insb. die sachgerechte Funktionsausübung des Informationssicherheitsbeauftragten von Bedeutung.

Wir regen daher an, eine Formulierung entsprechend der VAIT (dort Abschnitt 4, Tz. 30) zu verwenden: "Bei Ausgliederung der Funktion des

Informationssicherheitsbeauftragten sind die hierfür jeweils geltenden Anforderungen zu erfüllen. Bei der Entscheidung für oder gegen die Ausgliederung hat das Unternehmen 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 Funktionsausübung des Informationssicherheitsbeauftragten gewährleistet werden kann."

3. Übergeordnetes Konzernunternehmen als Informationssicherheitsbeauftragter

Die BAIT sehen Erleichterungen für "verbundangehörige Unternehmen" (also Sparkassen oder Genossenschaften) mit einem gleichgerichteten Geschäftsmodell und gemeinsamen IT-Dienstleistern vor. Eine darüber hinausgehende Konzernausnahme kennen die BAIT nicht. Auch die VAIT kennen keine Konzernausnahme.

Die Regelung, in welchen Fällen der Informationssicherheitsbeauftragte außerhalb der KVG angesiedelt werden kann, ist derzeit im Entwurf der KAIT uneinheitlich geregelt. Ist der IT-Betrieb an einen externen Dienstleister ausgelagert, dann kann die Funktion des Informationssicherheitsbeauftragten an einen externen fachlich qualifizierten Informationssicherheitsbeauftragten ausgelagert werden. Wird der IT-Betrieb jedoch an ein anderes konzernangehöriges Unternehmen übertragen, dann besteht nach dem derzeitigen Wortlaut der KAIT-E lediglich die Möglichkeit, den Informationssicherheitsbeauftragten an ein übergeordnetes Konzernunternehmen – nicht aber an einen externen Dritten oder ein Schwesterunternehmen – auszulagern. Da es sich auch bei einem übergeordneten Konzernunternehmen aus Sicht der KVG um einen externen Dritten handelt, stellt sich die Frage, warum es einer gesonderten Regelung für die konzerninterne Auslagerung bedarf. Wir regen daher an, die Regelungen zu vereinheitlichen. Wir verweisen hierzu auf die o.a. in Anlehnung an die VAIT vorgeschlagene Formulierung.

4. Aufgaben des Informationssicherheitsbeauftragten

Die Beachtung der KAIT ist für alle Wertschöpfungsebenen relevant, d.h. auch für wesentliche Auslagerungen. Daher sollte der Informationssicherheitsbeauftragte die Informationssicherheitsprozesse nicht nur in der KVG und gegenüber IT-Dienstleistern überwachen, sondern auch in geeigneter Form in die Auswahl und Überwachung der Auslagerungsunternehmen einbezogen werden, sofern

das Auslagerungsunternehmen für die Erbringung der ausgelagerten Leistung in nicht unwesentlichem Umfang IT nutzt. Wir regen an, dies klarzustellen (z.B. in Tz 30 bzw. der dazugehörenden Erläuterung).

Hilfreich wäre in diesem Zusammenhang u.E. auch die Klärung der Frage, welche Abschnitte der KAIT bei Auslagerungsunternehmen zur Anwendung kommen sollen und dementsprechend durch den Informationssicherheitsbeauftragten – neben den Fachbereichen bzw. den für das Auslagerungscontrolling Verantwortlichen – zu überwachen sind; d.h. ob beispielsweise auch das Auslagerungsunternehmen über eine IT-Strategie verfügen soll oder ob die Anforderungen des Abschnitts 7 zu beachten sind.

E. IT-Projekte und Anwendungsentwicklung (zu Abschnitt 6, Tz. 41)

Im Hinblick auf IT-Projekte und Anwendungsentwicklungen führt Tz. 41 KAIT-E aus, dass wesentliche Veränderungen der IT auch im Hinblick auf die Auswirkungen auf das IKS zu beurteilen sind. Der umgekehrte Sachverhalt, dass Änderungen der Geschäftsaktivitäten, der Aufbau- oder Ablauforganisation zu Auswirkungen auf den IT-Einsatz und die IT-Struktur/IT Funktionalitäten führen, ist bisher weder in den KAMaRisk noch in KAIT-E adressiert.

Wir regen an, dieses Zusammenspiel von Geschäftstätigkeit, Organisation, IT und IKS in Anlehnung an die Formulierung der MaRisk AT Abschnitt 8.2 (vorzugsweise durch eine Ergänzung der KAMaRisk (z.B. in Abschnitt 4.3 "Internes Kontrollsystem"), alternativ durch eine Ergänzung der Tz. 41 KAIT-E) zu berücksichtigen und die KAMaRisk oder KAIT entsprechend zu ergänzen.

Gerne stehen wir Ihnen für weitere Erläuterungen zur Verfügung.

Mit freundlichen Grüßen

Prof. Dr. Naumann

Groove, WP StB
Fachreferent