BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

Konsultation 07/2019

Entwurf eines Rundschreibens

Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

Inhalt

I. Vorbemerkung

1 Der Einsatz von Informationstechnik (IT) in den Kapitalverwaltungsgesellschaften („KVGen"), auch unter Einbeziehung von IT-Dienstleistungen, die durch IT-Dienstleister bereitgestellt werden, hat eine zentrale Bedeutung für die Finanzwirtschaft und wird weiter an Bedeutung gewinnen. Dieses Rundschreiben gibt auf der Grundlage der §§ 28, 29 und 30 Kapitalanlagegesetzbuch (KAGB), §§ 4-6 Verordnung zur Konkretisierung der Verhaltensregeln und Organisationsregeln nach dem Kapitalanlagegesetzbuch (KAVerOV) und den Artikeln 38 bis 66 der Delegierten Verordnung (EU) Nr. 231/2013 der Kommission vom 19. Dezember 2012 zur Ergänzung der Richtlinie 2011/61/EU des Europäischen Parlamentes und des Rates („AIFM Level 2-VO") einen flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausstattung der KVGen - insbesondere für das Management der IT-Ressourcen und für das IT-Risikomanagement - vor. Es präzisiert ferner die Anforderungen des § 36 KAGB und der Artikel 75 bis 82 der AIFM Level 2-VO (Auslagerung) im Hinblick auf die Auslagerung von IT-Dienstleistungen und den sonstigen Fremdbezug von IT-Dienstleistungen. Da die Regelungen der AIFM Level 2-VO unmittelbar gelten, bestimmen sich die Vorgaben für die Organisationspflichten, das Risikomanagement und die Auslagerung in erster Linie nach den Artikeln 38 bis 66 sowie 75 bis 82 der AIFM Level 2-VO. Dieses Rundschreiben konkretisiert Teile dieser Regelungen und ist daher erst in zweiter Linie zur Bestimmung der Mindestanforderungen an die aufsichtlichen Anforderungen an die IT der KVG heranzuziehen.

2 Die in den Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften (KAMaRisk) enthaltenen Anforderungen an die IT bleiben unberührt und werden durch dieses Rundschreiben konkretisiert. Die Themenbereiche dieses Rundschreibens sind nach Regelungstiefe und -umfang nicht abschließender Natur. Die KVGen bleiben folglich auch insbesondere jenseits der Konkretisierungen in diesem Rundschreiben gemäß § 28 Abs. 1 Satz 2 Nr. 2 KAGB i. V. m. Ziffer 8.1 Tz. 3 KAMaRisk verpflichtet, bei der Ausgestaltung der IT-Systeme (Hardware- und Softwarekomponenten) und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Zu diesen zählen beispielsweise die IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik und der internationale Sicherheitsstandard ISO/IEC 270XX der International Organization for Standardization.

3 Die prinzipienorientierten Anforderungen dieses Rundschreibens ermöglichen die Umsetzung des Proportionalitätsprinzips (vgl. hierzu die Ausführungen in Ziffer 1 Tzn. 2 und 3 KAMaRisk). Der sachgerechte Umgang mit dem Proportionalitätsprinzip und den prinzipienorientierten Anforderungen erfordert auch, dass die KVGen im Einzelfall über die in diesem Rundschreiben formulierten Anforderungen hinaus weitergehende Vorkehrungen treffen, soweit dies zur Sicherstellung der Angemessenheit und Wirksamkeit der technisch-organisatorischen Ausstattung und des Risikomanagements, insbesondere im Hinblick auf die Größe, Komplexität, Internationalität oder Risikoexponierung der KVG erforderlich sein sollte. Hierbei sind insbesondere auch die Schnittstellen zu externen Systemen (z.B. von Verwahrstelle oder Fondsadministrator) angemessen zu berücksichtigen.

4 Dieses Rundschreiben ist anwendbar auf KVGen im Sinne des § 17 KAGB, soweit diese über eine Erlaubnis nach § 20 Abs. 1 KAGB verfügen.

Dieses Rundschreiben findet keine Anwendung auf

- registrierte KVGen nach § 44 KAGB,
- extern verwaltete Investmentgesellschaften,
- Zweigniederlassungen von EU-Verwaltungsgesellschaften nach §§ 51 und 54 KAGB,
- Verwahrstellen,
- Treuhänder und
- Bewerter.

Bei extern verwalteten Investmentgesellschaften trägt die verwaltende KVG die Verantwortung für die Einhaltung der Vorgaben dieses Rundschreibens.

Insbesondere für die nach §§ 2 Abs. 5, 44 KAGB registrierten KVGen bleiben im Hinblick auf die risikoadäquate technisch-organisatorische Ausstattung die Anforderungen nach § 28 KAGB sowie, soweit einschlägig, die KAMaRisk anwendbar.

Für die nach § 44 KAGB registrierten KVGen bleibt die Anwendung der KAIT, soweit angemessen und darstellbar, unbenommen.

5	Alle Geschäftsleiter[1] einer KVG sind für die ordnungsgemäße und wirksame Geschäftsorganisation gesamtverantwortlich. Soweit sich die Anforderungen dieses Rundschreibens auf die Geschäftsleitung beziehen, ist immer die gesamte Geschäftsleitung angesprochen.

[1] Soweit aus Gründen der Lesbarkeit auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen diese sich auf alle Geschlechter in gleicher Weise.

II. Anforderungen

1. IT-Strategie

1	Die IT-Strategie hat die Anforderungen nach Ziffer 4.2 der KAMaRisk zu erfüllen. Dies beinhaltet insbesondere, dass die Geschäftsleitung eine nachhaltige IT-Strategie festlegt, in der die Ziele sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden.	
2	Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente IT-Strategie festzulegen. Mindestinhalte der IT-Strategie sind: (a) Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation der KVG sowie der Auslagerungen von IT-Dienstleistungen, (b) Zuordnung der gängigen Standards, an denen sich die KVG orientiert, auf die Bereiche der IT, (c) Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation (d) Strategische Entwicklung der IT-Architektur, (e) Aussagen zum Notfallmanagement unter Berücksichtigung der IT-Belange, (f) Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten).	Zu a): Beschreibung der Rolle, der Positionierung und des Selbstverständnisses der IT im Hinblick auf Personaleinsatz und Budget der IT-Aufbau- und IT-Ablauforganisation sowie die Darstellung und strategische Einordnung der IT-Dienstleistungen. Aussagen zu Auslagerungen von IT-Dienstleistungen können auch in den strategischen Ausführungen zu Auslagerungen enthalten sein. Zu b): Auswahl der gängigen Standards und Umsetzung auf die IT-Prozesse der KVG sowie Darstellung des avisierten Implementierungsumfangs der jeweiligen Standards Zu c): Beschreibung der Bedeutung der Informationssicherheit in der KVG sowie der Einbettung der Informationssicherheit in die Fachbereiche und in das jeweilige Zusammenarbeitsmodell mit den IT-Dienstleistern Zu d): Darstellung des Zielbilds der IT-Architektur in Form eines Überblicks über die Anwendungslandschaft
3	Die in der IT-Strategie niedergelegten Ziele sind so zu formulieren, dass eine sinnvolle Überprüfung der Zielerreichung möglich ist.	
4	Die IT-Strategie ist bei Erstverabschiedung sowie bei Anpassungen dem Aufsichtsrat oder dem vergleichbaren Aufsichtsorgan der KVG zur Kenntnis zu geben und ggf. mit diesem zu erörtern.	

5	Die Inhalte sowie Änderungen der IT-Strategie sind innerhalb der KVG in geeigneter Weise zu kommunizieren.

2. IT-Governance

6	Die IT-Governance ist die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der dazugehörigen IT-Prozesse auf Basis der IT-Strategie. Hierfür maßgeblich sind insbesondere die Regelungen zur IT-Aufbau- und IT-Ablauforganisation (vgl. Ziffer 4.3 Tzn. 1, 4 und 5 KAMaRisk), zum Informationsrisiko- sowie Informationssicherheitsmanagement (vgl. Ziffer 4.3 Tzn. 6, 7, 9, 12 bis 15 KAMaRisk und Ziffer 8.1 Tzn. 1 und 3 KAMaRisk), zur quantitativ und qualitativ angemessenen Personalausstattung der IT sowie zum Umfang und zur Qualität der technisch-organisatorischen Ausstattung (vgl. Ziffer 8.1 Tz. 2 KAMaRisk). Regelungen für die IT-Aufbau- und IT-Ablauforganisation sind bei Veränderungen der Aktivitäten und Prozesse zeitnah anzupassen (vgl. Ziffer 6 Tzn. 1 und 2 KAMaRisk). Die Anforderungen an ein IT-Notfallmanagement richten sich auch nach Ziffer 8.2 KAMaRisk.	
7	Die Geschäftsleitung ist dafür verantwortlich, dass auf Basis der IT-Strategie die Regelungen zur IT-Aufbau- und IT-Ablauforganisation festgelegt und bei Veränderungen der Aktivitäten und Prozesse zeitnah angepasst werden. Es ist sicherzustellen, dass die Regelungen zur IT-Aufbau- und IT-Ablauforganisation wirksam umgesetzt werden. Das gilt auch bezüglich der Schnittstellen zu Verwahrstellen und wichtigen Auslagerungsunternehmen.	
8	Die KVG hat insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, den IT-Betrieb und die Anwendungsentwicklung quantitativ und qualitativ angemessen mit Personal auszustatten.	Hinsichtlich der Maßnahmen zur Erhaltung einer angemessenen qualitativen Personalausstattung werden insbesondere der Stand der Technik sowie die aktuelle und zukünftige Entwicklung der Bedrohungslage berücksichtigt.
9	Interessenkonflikte und unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation sind zu vermeiden.	Interessenkonflikten zwischen Aktivitäten, die beispielsweise im Zusammenhang mit der Anwendungsentwicklung und den Aufgaben des IT-Betriebs stehen, kann durch aufbau- oder ablauforganisatorische Maßnahmen bzw. durch eine adäquate Rollendefinition begegnet werden.
10	Zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche durch die Geschäftsleitung sind angemessene quantitative oder qualitative Kriterien festzulegen und deren Einhaltung ist zu überwachen.	Bei der Festlegung der Kriterien können z. B. die Qualität der Leistungserbringungen, die Verfügbarkeit, Wartbarkeit, Anpassbarkeit an neue Anforderungen, Sicherheit der IT-Systeme oder der dazugehörigen IT-Prozesse sowie deren Kosten berücksichtigt werden.

11	Für IT-Risiken sind angemessene Überwachungs- und Steuerungsprozesse einzurichten.	
12	Die KVG hat sicherzustellen, dass die IT-bezogenen Geschäftsaktivitäten auf der Grundlage von Arbeitsablaufbeschreibungen (Organisationsrichtlinien) betrieben werden. Der Detaillierungsgrad der Organisationsrichtlinien hängt von der Risikostruktur der KVG ab.	Hinsichtlich der Darstellung der Organisationsrichtlinien kommt es in erster Linie darauf an, dass diese sachgerecht und für die Mitarbeiter der KVG nachvollziehbar sind. Die konkrete Art der Darstellung bleibt der KVG überlassen. IT-bezogene Geschäftsaktivitäten sind alle Geschäftsaktivitäten, die durch IT umgesetzt oder unterstützt werden.
13	Alle Mitarbeiter müssen fortlaufend - abhängig von ihren Aufgaben, Kompetenzen und Verantwortlichkeiten - über die erforderlichen Kenntnisse und Erfahrungen auch im Bereich der IT verfügen.	Durch geeignete Maßnahmen ist zu gewährleisten, dass das Qualifikationsniveau der Mitarbeiter angemessen ist.
14	Die Abwesenheit oder das Ausscheiden von Mitarbeitern darf nicht zu nachhaltigen Störungen der Betriebsabläufe führen.	
15	Für den Fall einer Störung, eines Ausfalls oder der Zerstörung der IT-Systeme, einschließlich der Schnittstellen und / oder der Online-Anbindung sind geeignete Notfallmaßnahmen zu implementieren, die die angemessene Fortführung des Geschäftsbetriebs, die Handlungsfähigkeit der KVG und die Sicherung der Wahrnehmung der Interessen der Anleger gewährleisten. Die Funktionsfähigkeit der Notfallmaßnahmen ist regelmäßig zu testen.	

3. Informationsrisikomanagement

16	Die Informationsverarbeitung und -weitergabe in Geschäfts- und Serviceprozessen wird durch datenverarbeitende IT-Systeme und zugehörige IT-Prozesse unterstützt. Deren Umfang und Qualität ist insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie an der Risikosituation zu orientieren (vgl. Ziffer 8.1 Tz. 2 KAMaRisk). IT-Systeme und zugehörige IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen (vgl. Ziffer 8.1 Tz. 3 KAMaRisk). Die KVG hat die mit dem Management der Informationsrisiken verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege klar zu definieren und aufeinander abzustimmen (vgl. Ziffer 4.3. Tz 5 KAMaRisk). Hierfür hat die KVG angemessene Überwachungs- und Steuerungsprozesse einzurichten (vgl. Ziffer 4.3 Tzn. 7, 9 und 15 KAMaRisk) und diesbezügliche Berichtspflichten zu definieren (vgl. Ziffer 4.3 Tzn. 12 bis 14 sowie Ziffer 4.9 KAMaRisk).	
17	Die Identifikations-, Bewertungs-, Überwachungs- und Steuerungsprozesse haben insbesondere die Festlegung von IT-Risikokriterien, die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie die Festlegung von Maßnahmen zur Risikobehandlung der verbliebenen Restrisiken zu umfassen. Beim Bezug von Software sind die damit verbundenen Risiken angemessen zu bewerten und zu steuern.	
18	Die Bestandteile eines Systems zum Management der Informationsrisiken sind unter Mitwirkung aller maßgeblichen Stellen und Funktionen kompetenzgerecht und frei von Interessenkonflikten umzusetzen.	Zu den maßgeblichen Stellen gehören auch die Fachbereiche, die Eigentümer der Informationen sind.
19	Die KVG hat über einen aktuellen Überblick über die Bestandteile des festgelegten Informationsverbunds sowie deren Abhängigkeiten und Schnittstellen zu verfügen. Die KVG sollte sich hierbei insbesondere an den betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie an der Risikosituation orientieren.	Zu einem Informationsverbund gehören beispielsweise geschäftsrelevante Informationen, Geschäftsprozesse, IT-Systeme sowie Netz- und Gebäudeinfrastrukturen.
20	Die Methodik zur Ermittlung des Schutzbedarfs (insbesondere im Hinblick auf die Schutzziele „Integrität“, „Verfügbarkeit“, „Vertraulichkeit“ und „Authentizität“) hat die Konsistenz der resultierenden Schutzbedarfe nachvollziehbar sicherzustellen.	Schutzbedarfskategorien sind beispielhaft „niedrig“, „mittel“, „hoch“ und „sehr hoch“.

21	Die Anforderungen der KVG zur Umsetzung der Schutzziele in den Schutzbedarfskategorien sind festzulegen und in geeigneter Form zu dokumentieren (Sollmaßnahmenkatalog).	Der Sollmaßnahmenkatalog enthält lediglich die Anforderung, nicht jedoch deren konkrete Umsetzung.
22	Die Risikoanalyse auf Basis der festgelegten Risikokriterien hat auf Grundlage eines Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen zu erfolgen. Sonstige risikoreduzierende Maßnahmen aufgrund unvollständig umgesetzter Sollmaßnahmen sind wirksam zu koordinieren, zu dokumentieren, zu überwachen und zu steuern. Die Ergebnisse der Risikoanalyse sind durch den verantwortlichen Mitarbeiter zu genehmigen und in den Prozess des Managements der operationellen Risiken zu überführen.	Risikokriterien enthalten bspw. mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit. Die Risikoanalyse kann u. a. auch auf Grundlage eines Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen erfolgen.
23	Die Geschäftsleitung ist regelmäßig, mindestens jedoch vierteljährlich, insbesondere über die Ergebnisse der Risikoanalyse sowie Veränderungen an der Risikosituation zu unterrichten (Statusbericht).	Der Statusbericht enthält bspw. die Bewertung der Risikosituation im Vergleich zum Vorbericht (Deltareport).

4. Informationssicherheitsmanagement

24	Das Informationssicherheitsmanagement macht Vorgaben zur Informationssicherheit, definiert Prozesse und steuert deren Umsetzung (vgl. Ziffer 8.1 Tz. 3 KAMaRisk). Das Informationssicherheitsmanagement folgt einem fortlaufenden Prozess, der die Phasen Planung, Umsetzung, Erfolgskontrolle sowie Optimierung und Verbesserung umfasst. Die inhaltlichen Berichtspflichten des Informationssicherheitsbeauftragten an die Geschäftsleitung sowie den Aufsichtsrat sowie der Turnus der Berichterstattung orientieren sich an Ziffer 4.3 Tzn. 12 bis 14 und 17 sowie Ziffer 4.9 KAMaRisk.	
25	Die Geschäftsleitung hat eine Informationssicherheitsleitlinie zu beschließen und innerhalb der KVG angemessen zu kommunizieren. Die Informationssicherheitsleitlinie hat im Einklang mit den Strategien der KVG zu stehen.	In der Informationssicherheitsleitlinie werden die Ziele und der Geltungsbereich für die Informationssicherheit festgelegt und die wesentlichen organisatorischen Aspekte des Informationssicherheitsmanagements beschrieben. Regelmäßige Überprüfungen und Anpassungen an geänderte Bedingungen werden risikoorientiert vorgenommen. Veränderungen der Aufbau- und Ablauforganisation sowie der IT-Systeme einer KVG (Geschäftsprozesse, Fachaufgaben, organisatorische Gliederung) werden hierbei ebenso berücksichtigt wie Veränderungen der äußeren Rahmenbedingungen (z.B. gesetzliche Regelungen, regulatorische Anforderungen), der Bedrohungsszenarien oder der Sicherheitstechnologien.
26	Auf Basis der Informationssicherheitsleitlinie sind konkretisierende, den Stand der Technik berücksichtigende Informationssicherheitsrichtlinien und Informationssicherheitsprozesse mit den Teilprozessen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren.	Informationssicherheitsrichtlinien werden bspw. für die Bereiche Netzwerksicherheit, Kryptografie, Authentisierung und Protokollierung erstellt. Informationssicherheitsprozesse dienen in erster Linie zur Erreichung der vereinbarten Schutzziele. Dazu gehört u. a., Informationssicherheitsvorfällen vorzubeugen und diese zu identifizieren sowie die angemessene Reaktion und Kommunikation im weiteren Verlauf.
27	Die KVG hat die Funktion des Informationssicherheitsbeauftragten einzurichten. Diese Funktion umfasst die Verantwortung für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der KVG und gegenüber Dritten. Sie 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 Funktion des Informationssicherheitsbeauftragten umfasst insbesondere die nachfolgenden Aufgaben: ■ die Geschäftsleitung beim Festlegen und Anpassen der Informationssicherheitsleitlinie zu unterstützen und in allen Fragen der Informationssicherheit zu beraten; dies umfasst auch Hilfestellungen bei der Lösung von Zielkonflikten (z. B. Wirtschaftlichkeit kontra Informationssicherheit), ■ Erstellung von Informationssicherheitsrichtlinien und ggf. weiteren einschlägigen Regelungen sowie die Kontrolle ihrer Einhaltung,

		■ den Informationssicherheitsprozess in der KVG zu steuern und zu koordinieren sowie diesen gegenüber IT-Dienstleistern zu überwachen und bei allen damit zusammenhängenden Aufgaben mitzuwirken, ■ Beteiligung bei der Erstellung und Fortschreibung des Notfallkonzepts bzgl. der IT-Belange, ■ die Realisierung von Informationssicherheitsmaßnahmen zu initiieren und zu überwachen, ■ Beteiligung bei Projekten mit IT-Relevanz, ■ als Ansprechpartner für Fragen der Informationssicherheit innerhalb der KVG und für Dritte bereitzustehen, ■ Informationssicherheitsvorfälle zu untersuchen und diesbezüglich an die Geschäftsleitung zu berichten, ■ Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu koordinieren.
28	Die Funktion des Informationssicherheitsbeauftragten ist organisatorisch und prozessual unabhängig auszugestalten, um mögliche Interessenskonflikte zu vermeiden.	Zur Vermeidung möglicher Interessenkonflikte werden insbesondere folgende Maßnahmen beachtet: ■ Funktions- und Stellenbeschreibung für den Informationssicherheitsbeauftragten und seinen Vertreter, ■ Festlegung der erforderlichen Ressourcenausstattung für die Funktion des Informationssicherheitsbeauftragten, ■ ein der Funktion 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 Informationssicherheitsbeauftragten über alle bekannt gewordenen IT sicherheitsrelevanten Sachverhalte, die die KVG betreffen. ■ Die 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.

29	Jede KVG hat die Funktion des Informationssicherheitsbeauftragten grundsätzlich im eigenen Haus vorzuhalten.	KVGen können die Funktion 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 des Informationssicherheitsbeauftragten auf einen fachlich qualifizierten Dritten 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 ist in der KVG eine interne Ansprechperson für den Informationssicherheitsbeauftragten zu benennen. Die Möglichkeit, sich externer Unterstützung per Servicevertrag zu bedienen, bleibt unberührt.
30	Nach einem Informationssicherheitsvorfall sind die Auswirkungen auf die Informationssicherheit zu analysieren und angemessene Nachsorgemaßnahmen zu veranlassen.	Die Definition des Begriffes „Informationssicherheitsvorfall“ nach Art und Umfang basiert auf dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Systeme und den zugehörigen IT-Prozessen. Ein Informationssicherheitsvorfall kann auch dann vorliegen, wenn mindestens eines der Schutzziele („Verfügbarkeit“, „Integrität“, „Vertraulichkeit“, „Authentizität“) gemäß den Vorgaben des KVG-spezifischen Sollkonzepts der Informationssicherheit - über dem definierten Schwellenwert - verletzt ist. Der Begriff „Informationssicherheitsvorfall“ ist nachvollziehbar vom Begriff „Abweichung vom Regelbetrieb“ (im Sinne von „Störung im Tagesbetrieb“) abzugrenzen.
31	Der Informationssicherheitsbeauftragte hat der Geschäftsleitung regelmäßig, mindestens vierteljährlich, über den Status der Informationssicherheit sowie anlassbezogen zu berichten.	Der Statusbericht enthält beispielsweise die Bewertung der Informationssicherheitslage im Vergleich zum Vorbericht, Informationen zu Projekten zur Informationssicherheit, Informationssicherheitsvorfälle sowie Penetrationstest-Ergebnisse (Deltareport).

5. Benutzerberechtigungsmanagement

32	Ein Benutzerberechtigungsmanagement stellt sicher, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben der KVG entspricht. Das Benutzerberechtigungsmanagement hat die Anforderungen nach Ziffer 8.1 Tz 3 sowie Ziffer 4.5 Tz. 7 der KAMaRisk zu erfüllen.	
33	Berechtigungskonzepte legen den Umfang und die Nutzungsbedingungen der Berechtigungen für die IT-Systeme konsistent zum ermittelten Schutzbedarf sowie vollständig und nachvollziehbar ableitbar für alle von einem IT-System bereitgestellten Berechtigungen fest. 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.	Eine mögliche Nutzungsbedingung ist die Befristung der eingeräumten Berechtigungen. Berechtigungen können sowohl für personalisierte, für nicht personalisierte als auch für technische Benutzer vorliegen.
34	Nicht personalisierte Berechtigungen müssen jederzeit zweifelsfrei einer handelnden Person (möglichst automatisiert) zuzuordnen sein. Abweichungen in begründeten Ausnahmefällen und die hieraus resultierenden Risiken sind zu genehmigen und zu dokumentieren.	Nicht personalisierte Berechtigungen sind nicht an einen spezifischen Mitarbeiter gebunden und können von mehreren Mitarbeitern verwendet werden (Bspw. „Admin“-User).
35	Jeder technische Benutzer muss einer verantwortlichen Person zugeordnet sein, die im Rahmen der Rezertifizierung einzubinden ist. Die eingerichteten technischen Benutzer müssen in einem Zentralverzeichnis verwaltet werden.	Technische Benutzer sind Nutzer, die von IT-Systemen verwendet werden, um sich gegenüber Dritten zu identifizieren oder eigenständige IT-Routinen auszuführen. Sie werden beispielsweise in der Maschine-zu-Maschine Kommunikation verwendet.
36	Die Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen für Benutzer haben durch Genehmigungs- und Kontrollprozesse sicherzustellen, dass die Vorgaben des Berechtigungskonzepts eingehalten werden. Dabei ist die fachlich verantwortliche Stelle angemessen einzubinden, so dass sie ihrer fachlichen Verantwortung nachkommen kann.	Die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen umfassen jeweils die Umsetzung des Berechtigungsantrags im Zielsystem.

37	Bei der Überprüfung, ob die eingeräumten Berechtigungen weiterhin benötigt werden und ob diese den Vorgaben des Berechtigungskonzepts entsprechen (Rezertifizierung), sind die für die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen zuständigen Kontrollinstanzen mit einzubeziehen.	Fällt im Rahmen der Rezertifizierung auf, dass außerhalb des vorgeschriebenen Verfahrens Berechtigungen eingeräumt wurden, so werden diese gemäß der Regelverfahren zur Einrichtung, Änderung und Löschung von Berechtigungen entzogen. Dies gilt auch für die nicht personalisierten und technischen Benutzer.
38	Die Einrichtung, Änderung, Deaktivierung sowie Löschung von Berechtigungen und die Rezertifizierung sind nachvollziehbar und auswertbar zu dokumentieren.	
39	Die KVG hat nach Maßgabe des Schutzbedarfs und der Soll-Anforderungen Prozesse zur Protokollierung und Überwachung einzurichten, die überprüfbar machen, dass die Berechtigungen nur wie vorgesehen eingesetzt werden.	Die übergeordnete Verantwortung für die Prozesse zur Protokollierung und Überwachung von Berechtigungen wird einer Stelle zugeordnet, die unabhängig vom berechtigten Benutzer oder dessen Organisationseinheit ist. Aufgrund weitreichender Eingriffsmöglichkeiten privilegierter Benutzer wird die KVG insbesondere für deren Aktivitäten angemessene Prozesse zur Protokollierung und Überwachung einrichten.
40	Durch begleitende technisch-organisatorische Maßnahmen ist einer Umgehung der Vorgaben der Berechtigungskonzepte vorzubeugen.	Technisch-organisatorische Maßnahmen hierzu sind beispielsweise: ■ Auswahl angemessener Authentifizierungsverfahren, ■ Implementierung einer Richtlinie zur Wahl sicherer Passwörter, ■ automatischer passwortgesicherter Bildschirmschoner, ■ Verschlüsselung von Daten, ■ eine manipulationssichere Implementierung der Protokollierung, ■ Maßnahmen zur Sensibilisierung der Mitarbeiter.

6. IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen)

41 Wesentliche Veränderungen in den IT-Systemen im Rahmen von IT-Projekten, deren Auswirkung auf die IT-Aufbau- und IT-Ablauforganisation sowie die dazugehörigen IT-Prozesse sind vorab im Rahmen einer Analyse des Risikogehalts zu bewerten. Dabei hat die KVG insbesondere auch die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität sowie auf das Portfolio- und das Risikomanagement zu analysieren. In diese Analysen sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten zu beteiligen. Im Hinblick auf den erstmaligen Einsatz sowie wesentliche Veränderungen von IT-Systemen sind die Anforderungen der Ziffer 8.1 Tzn. 4 und 5 KAMaRisk zu erfüllen.

42 Die IT-Systeme sind vor ihrer Übernahme in den produktiven Betrieb zu testen und von den fachlich sowie auch von den technisch zuständigen Mitarbeitern abzunehmen. Produktions- und Testumgebung sind dabei grundsätzlich voneinander zu trennen. Diese Anforderungen gelten grundsätzlich auch bei wesentlichen Veränderungen der IT-Systeme.

Es ist ein Regelprozess der Entwicklung, des Testens, der Freigabe und der Implementierung in die Produktionsprozesse zu etablieren.

Soweit Änderungen an IT-Systemen automatisiert von Dritten durchgeführt werden und nicht vor Inbetriebnahme von der KVG getestet werden können, überzeugt sich die KVG regelmäßig davon, dass bei diesem Dritten die notwendigen Tests vorab durchgeführt werden.

43 Die organisatorischen Grundlagen von IT-Projekten (inkl. Qualitätssicherungsmaßnahmen) und die Kriterien für deren Anwendung sind zu regeln.

IT-Projekte sind Projekte, die mit Anpassungen der IT-Systeme einhergehen. Der Ausgangspunkt kann sowohl im Fachbereich als auch im IT-Bereich liegen.

44 IT-Projekte sind angemessen zu steuern, insbesondere unter Berücksichtigung der Risiken im Hinblick auf die Dauer, den Ressourcenverbrauch und die Qualität von IT-Projekten. Hierfür sind Vorgehensmodelle festzulegen, deren Einhaltung zu überwachen ist.

Beispielsweise kann die Entscheidung über den Übergang zwischen den Projektphasen von eindeutigen Qualitätskriterien des jeweiligen Vorgehensmodells abhängen.

45 Das Portfolio der IT-Projekte ist angemessen zu überwachen und zu steuern. Dabei ist zu berücksichtigen, dass auch aus Abhängigkeiten verschiedener Projekte voneinander Risiken resultieren können.

Die Portfoliosicht ermöglicht einen Überblick über die IT-Projekte mit den entsprechenden Projektdaten, Ressourcen, Risiken und Abhängigkeiten.

46 Wesentliche IT-Projekte und IT-Projektrisiken sind der Geschäftsleitung regelmäßig und anlassbezogen zu berichten. Wesentliche Projektrisiken sind im Risikomanagement zu berücksichtigen.

---

47 Für die Anwendungsentwicklung sind angemessene Prozesse festzulegen, die Vorgaben zur Anforderungsermittlung, zum Entwicklungsziel, zur (technischen) Umsetzung (einschließlich Programmierrichtlinien), zur Qualitätssicherung, sowie zu Test, Abnahme und Freigabe enthalten.

Anwendungsentwicklung umfasst beispielsweise die Entwicklung von Software zur Unterstützung fachlicher Prozesse oder die von Endbenutzern in den Fachbereichen selbst entwickelten Anwendungen (z. B. Individuelle Datenverarbeitung - IDV).

Die Ausgestaltung der Prozesse erfolgt risikoorientiert.

48 Anforderungen an die Funktionalität der Anwendung müssen ebenso erhoben, bewertet und dokumentiert werden wie nichtfunktionale Anforderungen.

Die Verantwortung für die Erhebung und Bewertung dieser fachlichen Anforderungen liegt in den zuständigen Fachbereichen.

Anforderungsdokumente sind beispielsweise:

- Fachkonzept (Lastenheft),
- User Story,
- Product Backlog,
- Technisches Fachkonzept (Pflichtenheft).

Nichtfunktionale Anforderungen an IT-Systeme sind beispielsweise:

- Ergebnisse der Schutzbedarfsfeststellung,
- Zugriffsregelungen,
- Ergonomie,
- Wartbarkeit,
- Antwortzeiten,
- Resilienz.

---

49 Im Rahmen der Anwendungsentwicklung sind nach Maßgabe des Schutzbedarfs angemessene Vorkehrungen im Hinblick darauf zu treffen, dass nach Produktivsetzung der Anwendung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten nachvollziehbar sichergestellt werden.

Geeignete Vorkehrungen können sein:

- Prüfung der Eingabedaten,
- Systemzugangskontrolle,
- Nutzer-Authentifizierung,
- Transaktionsautorisierung,
- Protokollierung der Systemaktivität,
- Prüfpfade (Audit Logs),
- Verfolgung von sicherheitsrelevanten Ereignissen,
- Behandlung von Ausnahmen.

50	Im Rahmen der Anwendungsentwicklung müssen Vorkehrungen getroffen werden, die erkennen lassen, ob eine Anwendung versehentlich geändert oder absichtlich manipuliert wurde.	Eine geeignete Vorkehrung unter Berücksichtigung des Schutzbedarfs kann die Überprüfung des Quellcodes im Rahmen der Anwendungsentwicklung sein. Die Überprüfung des Quellcodes ist eine methodische Untersuchung zur Identifizierung von Risiken.
51	Sowohl die von Dritten für die KVG entwickelte als auch die in der KVG selbst entwickelte Anwendung sowie deren Entwicklung sind übersichtlich und für sachkundige Dritte nachvollziehbar zu dokumentieren.	Die Dokumentation der Anwendung und deren Entwicklung umfasst mindestens folgende Inhalte: ■ Was wurde entwickelt?, ■ Anwenderdokumentation, ■ Technische und prozessuale Systemdokumentation, ■ Betriebsdokumentation. Zur Nachvollziehbarkeit der Anwendungsentwicklung trägt beispielsweise eine Versionierung des Quellcodes und der Anforderungsdokumente bei.
52	Es ist eine Methodik für das Testen von Anwendungen vor ihrem erstmaligen Einsatz und nach wesentlichen Änderungen zu definieren und einzuführen. Die Tests haben in ihrem Umfang die Funktionalität der Anwendung, die Sicherheitskontrollen und die Systemleistung unter verschiedenen Stressbelastungsszenarien einzubeziehen. Sofern bei einer Anwendung die Systemleistung von Bedeutung ist, ist auch diese unter verschiedenen, sachgerechten Stressbelastungsszenarien zu testen. Die Durchführung von fachlichen Abnahmetests verantwortet der für die Anwendung zuständige Fachbereich. Testumgebungen zur Durchführung der Abnahmetests haben in für den Test wesentlichen Aspekten der Produktionsumgebung zu entsprechen. Testaktivitäten und Testergebnisse sind zu dokumentieren.	Dies umfasst einschlägige Expertise sowie eine angemessen ausgestaltete Unabhängigkeit von den Anwendungsentwicklern. Eine Testdokumentation enthält mindestens folgende Punkte: ■ Testfallbeschreibung ■ Dokumentation der zugrunde gelegten Parametrisierung des Testfalls ■ Testdaten ■ erwartetes Testergebnis ■ erzieltes Testergebnis ■ aus den Tests abgeleiteten Maßnahmen.
53	Nach Produktivsetzung der Anwendung sind mögliche Abweichungen vom Regelbetrieb zu überwachen, deren Ursachen zu untersuchen und ggf. Maßnahmen zur Nachbesserung zu veranlassen.	Nach der Produktivsetzung bedarf es einer temporär erhöhten Überwachung. Hinweise auf erhebliche Mängel können z. B. Häufungen der Abweichungen vom Regelbetrieb sein.
54	Ein angemessenes Verfahren für die Klassifizierung / Kategorisierung (Schutzbedarfsklasse) und den Umgang mit den von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen ist festzulegen.	Die Einhaltung von Programmierstandards wird auch für die von Endbenutzern in den Fachbereichen entwickelten Anwendungen (z. B. IDV-Anwendung) sichergestellt. Jede dieser Anwendungen wird einer Schutzbedarfsklasse zugeordnet.

		Übersteigt der ermittelte Schutzbedarf die technische Schutzmöglichkeit dieser Anwendungen, werden Schutzmaßnahmen in Abhängigkeit der Ergebnisse der Schutzbedarfsklassifizierung ergriffen.
55	Die Vorgaben zur Identifizierung aller von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen, zur Dokumentation, zu den Programmierrichtlinien und zur Methodik des Testens, zur Schutzbedarfsfeststellung und zum Rezertifizierungsprozess der Berechtigungen sind zu regeln (z. B. in einer IDV-Richtlinie). Die Anforderungen unter II. Rn. 17 und 42 sind auch beim Einsatz von durch die Fachbereiche selbst entwickelten Anwendungen (Individuelle Datenverarbeitung - „IDV“) entsprechend der Kritikalität der unterstützten Geschäftsprozesse und der Bedeutung der Anwendungen für diese Prozesse zu beachten. Die Festlegung von Maßnahmen zur Sicherstellung der Datensicherheit hat sich am Schutzbedarf der verarbeiteten Daten zu orientieren.	Für einen Überblick und zur Vermeidung von Redundanzen wird ein zentrales Register dieser Anwendungen geführt und es werden mindestens folgende Informationen erhoben: ■ Name und Zweck der Anwendung ■ Versionierung, Datumsangabe ■ Fremd- oder Eigenentwicklung ■ Fachverantwortliche(r) Mitarbeiter ■ Technisch verantwortliche(r) Mitarbeiter ■ Technologie ■ Ergebnis der Risikoklassifizierung/Schutzbedarfseinstufung und ggf. die daraus abgeleiteten Schutzmaßnahmen.

7. IT-Betrieb (inkl. Datensicherung)

56 Der IT-Betrieb hat die Erfüllung der Anforderungen, die sich aus der Umsetzung der Geschäftsstrategie, aus den Vorgaben der Ziffer 8.1 Tz. 1 KAMaRisk sowie aus den IT-unterstützten Geschäftsprozessen ergeben, umzusetzen (vgl. Ziffer 4.3 Tz. 17 sowie Ziffer 8.1 Tzn. 2 und 3 KAMaRisk).

57 Die Komponenten der IT-Systeme sowie deren Beziehungen zueinander sind in geeigneter Weise zu verwalten, und die hierzu erfassten Bestandsangaben regelmäßig sowie anlassbezogen zu aktualisieren.

Zu den Bestandsangaben zählen insbesondere:

- Bestand und Verwendungszweck der Komponenten der IT-Systeme mit den relevanten Konfigurationsangaben,
- Standort der Komponenten der IT-Systeme,
- Aufstellung der relevanten Angaben zu Gewährleistungen und sonstigen Supportverträgen (ggf. Verlinkung),
- Angaben zum Ablaufdatum des Supportzeitraums der Komponenten der IT-Systeme,
- Akzeptierter Zeitraum der Nichtverfügbarkeit der IT-Systeme sowie der maximal tolerierbare Datenverlust.

58 Das Portfolio aus IT-Systemen ist angemessen zu steuern. Hierbei werden auch die Risiken aus veralteten IT-Systemen berücksichtigt (Lebens-Zyklus Management).

59 Die Prozesse zur Änderung von IT-Systemen sind abhängig von Art, Umfang, Komplexität und Risikogehalt auszugestalten und umzusetzen. Dies gilt ebenso für Neu- bzw. Ersatzbeschaffungen von IT-Systemen sowie für sicherheitsrelevante Nachbesserungen (Sicherheitspatches).

Beispiele für Änderungen sind:

- Funktionserweiterungen oder Fehlerbehebungen von Software-Komponenten,
- Datenmigrationen,
- Änderungen an Konfigurationseinstellungen von IT-Systemen,
- Austausch von Hardware-Komponenten (Server, Router etc.),
- Einsatz neuer Hardware-Komponenten,
- Umzug der IT-Systeme zu einem anderen Standort.

60	Anträge zur Änderung von IT-Systemen sind in geordneter Art und Weise aufzunehmen, zu dokumentieren, unter Berücksichtigung möglicher Umsetzungsrisiken zu bewerten, zu priorisieren, zu genehmigen sowie koordiniert und sicher umzusetzen.	Der sicheren Umsetzung der Änderungen in den produktiven Betrieb dienen beispielsweise: ■ Risikoanalyse in Bezug auf die bestehenden IT-Systeme (insbesondere auch das Netzwerk und die vor- und nachgelagerten IT-Systeme), auch im Hinblick auf mögliche Sicherheits- oder Kompatibilitätsprobleme, als Bestandteil der Änderungsanforderung, ■ Tests von Änderungen vor Produktivsetzung auf mögliche Inkompatibilitäten der Änderungen sowie mögliche sicherheitskritische Aspekte bei maßgeblichen bestehenden IT-Systemen, ■ Tests von Patches vor Produktivsetzung unter Berücksichtigung ihrer Kritikalität (z. B. bei Sicherheits- oder Notfallpatches), ■ Datensicherungen der betroffenen IT-Systeme, ■ Rückabwicklungspläne, um eine frühere Version des IT-Systems wiederherstellen zu können, wenn während oder nach der Produktivsetzung ein Problem auftritt, ■ alternative Wiederherstellungsoptionen, um dem Fehlschlagen primärer Rückabwicklungspläne begegnen zu können. Für risikoarme Konfigurationsänderungen/Parametereinstellungen (z. B. Änderungen am Layout von Anwendungen, Austausch von defekten Hardwarekomponenten, Zuschaltung von Prozessoren) können abweichende prozessuale Vorgaben/Kontrollen definiert werden (z. B. Vier-Augen-Prinzip, Dokumentation der Änderungen oder der nachgelagerten Kontrolle).
61	Die Meldungen über ungeplante Abweichungen vom Regelbetrieb (Störungen) und deren Ursachen sind in geeigneter Weise zu erfassen, zu bewerten, insbesondere hinsichtlich möglicherweise resultierender Risiken zu priorisieren und entsprechend festgelegter Kriterien zu eskalieren. Bearbeitung, Ursachenanalyse und Lösungsfindung inkl. Nachverfolgung sind zu dokumentieren. Ein geordneter Prozess zur Analyse möglicher Korrelationen von Störungen und deren Ursachen muss vorhanden sein. Der Bearbeitungsstand offener Meldungen über Störungen, wie auch die Angemessenheit der Bewertung und Priorisierung, ist zu überwachen und zu steuern. Die KVG hat geeignete Kriterien für die Information der Geschäftsleitung über Störungen festzulegen.	Die Identifikation der Risiken kann beispielsweise anhand des Aufzeigens der Verletzung der Schutzziele erfolgen. Die Ursachenanalyse erfolgt auch dann, wenn mehrere IT-Systeme zur Störungs- und Ursachenerfassung sowie -bearbeitung eingesetzt werden.

62 Die Vorgaben für die Verfahren zur Datensicherung (ohne die langfristige Datenarchivierung) sind schriftlich in einem Datensicherungskonzept zu regeln. Die im Datensicherungskonzept dargestellten Anforderungen an die Verfügbarkeit, Lesbarkeit und Aktualität der Kunden- und Geschäftsdaten sowie an die für deren Verarbeitung notwendigen IT-Systeme sind aus den Anforderungen der Geschäftsprozesse und den Geschäftsfortführungsplänen (Business Continuity Plan) abzuleiten. Die Verfahren zur Wiederherstellbarkeit im erforderlichen Zeitraum und zur Lesbarkeit von Datensicherungen sind regelmäßig, mindestens jährlich, im Rahmen einer Stichprobe sowie anlassbezogen zu testen.

Die Anforderungen an die Ausgestaltung und Lagerung der Datensicherungen sowie an die durchzuführenden Tests ergeben sich aus diesbezüglichen Risikoanalysen. Hinsichtlich der Standorte für die Lagerung der Datensicherungen können eine oder mehrere weitere Lokationen erforderlich sein.

8. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

63 IT-Dienstleistungen umfassen alle Ausprägungen des Bezugs von IT; dazu zählen insbesondere die Bereitstellung von IT-Systemen, Projekte/Gewerke oder Personalgestellung. Hierzu zählen auch IT-Dienstleistungen, die der KVG durch ein Dienstleistungsunternehmen über ein Netz bereitgestellt werden (z. B. Rechenleistung, Speicherplatz, Plattformen oder Software) und deren Angebot, Nutzung und Abrechnung ggfs. dynamisch und an den Bedarf angepasst über definierte technische Schnittstellen sowie Protokolle erfolgen (Cloud-Dienstleistungen). Die Auslagerungen der IT-Dienstleistungen haben die Anforderungen nach Ziffer 10 der KAMaRisk und des BaFin-FAQ zu Auslagerung gemäß § 36 KAGB zu erfüllen. Die KVG hat auch beim sonstigen Fremdbezug von IT-Dienstleistungen die allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß §§ 28 bis 30 KAGB zu beachten (vgl. Ziffer 10 Tz. 1 - Erläuterungen - KAMaRisk). Bei jedem Bezug von Software sind die damit verbundenen Risiken angemessen zu bewerten (vgl. Ziffer 4.3 Tzn. 7, 9 und 15 KAMaRisk).

64 Eine Auslagerung liegt vor, wenn ein anderes Unternehmen mit der Wahrnehmung von Aufgaben beauftragt wird (Auslagerungsunternehmen), die ansonsten von der KVG selbst erbracht würden.

Von der Auslagerung von IT-Dienstleistungen ist der sonstige Fremdbezug von IT-Dienstleistungen abzugrenzen.

Der isolierte Bezug von handelsüblicher Standard-Software, d.h. von Software ohne unternehmensspezifische Anpassungen, (einschließlich automatischer Updates und Patches) und die auf diese bezogene Inanspruchnahme von Software-Anbietern für Ad-Hoc-Hilfe beim Betrieb dieser Systeme (vgl. Erwägungsgrund 82 der Delegierten Verordnung EU 231/2013) ist in der Regel als sonstiger Fremdbezug einzustufen. Die Personalgestellung zu Gunsten der KVG ist in der Regel als sonstiger Fremdbezug einzustufen, wenn die Tätigkeit auf den Systemen der KVG und nach deren Weisung und unter ihrer Kontrolle erfolgt.

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

- die Anpassung der Software an die Erfordernisse der KVG (Parametrisierung bzw. Customising),
- die entwicklungstechnische Erstellung von Programmen oder Programmteilen und die Umsetzung von Änderungswünschen (Programmierung),
- das Testen, die Freigabe und die Implementierung der Software in die Produktionsprozesse beim erstmaligen Einsatz und bei wesentlichen Veränderungen, insbesondere von programmtechnischen Vorgaben,
- Fehlerbehebungen gemäß der Anforderungs-/Fehlerbeschreibung des Auftraggebers oder Herstellers,
- sonstige Unterstützungsleistungen (wie z.B. der Betrieb und die Wartung von IT-Systemen durch Dritte),

		sofern diese längerfristig angelegt sind oder erhebliche oder kritische Auswirkungen auf die Portfolioverwaltung, das Risikomanagement oder sonstige geschäftskritische Prozesse haben oder haben können. Im Übrigen ist es nicht ohne weiteres möglich, starre, praxisgerechte Kriterien für eine Abgrenzung zwischen Auslagerung und sonstigem Fremdbezug zu definieren. Die KVGen sind daher gehalten, bei der Beauftragung eines Dritten die Abgrenzung insbesondere unter Berücksichtigung der Bedeutung des Auftrags und der hierdurch entstehenden Risiken für die Portfolioverwaltung, das Risikomanagement und die sonstigen geschäftskritischen Prozesse selbst vorzunehmen. Ergänzender Hinweis: Für die Auslagerung auf Cloud-Anbieter ist ergänzend das BaFin-Merkblatt „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter“ zur berücksichtigen.
65	Wegen der grundlegenden Bedeutung der IT für die KVG ist auch für jeden sonstigen Fremdbezug von IT-Dienstleistungen vorab eine Risikobewertung durchzuführen.	Art und Umfang einer Risikobewertung kann die KVG unter Proportionalitätsgesichtspunkten nach Maßgabe ihres allgemeinen Risikomanagements flexibel festlegen. Für gleichartige Formen des sonstigen Fremdbezugs von IT-Dienstleistungen kann auf bestehende Risikobewertungen zurückgegriffen werden. Die für Informationssicherheit und Notfallmanagement verantwortlichen Funktionen der KVG werden eingebunden.
66	Der sonstige Fremdbezug von IT-Dienstleistungen ist im Einklang mit den Strategien unter Berücksichtigung der Risikobewertung der KVG zu steuern. Die Erbringung der vom Dienstleister geschuldeten Leistung ist entsprechend der Risikobewertung zu überwachen.	Hierfür wird eine vollständige, strukturierte Vertragsübersicht vorgehalten. Die Steuerung kann auf der Basis dieser Vertragsübersicht durch Bündelung von Verträgen des sonstigen Fremdbezugs von IT-Dienstleistungen (Vertragsportfolio) erfolgen. Bestehende Steuerungsmechanismen können hierzu genutzt werden.
67	Die aus der Risikobewertung zum sonstigen Fremdbezug von IT-Dienstleistungen abgeleiteten Maßnahmen sind angemessen in der Vertragsgestaltung zu berücksichtigen. Die Ergebnisse der Risikobewertung sind in angemessener Art und Weise im Managementprozess des operationellen Risikos, vor allem im Bereich der Gesamtrisikobewertung des operationellen Risikos, zu berücksichtigen.	Dies beinhaltet beispielsweise Vereinbarungen zum Informationsrisikomanagement, zum Informationssicherheitsmanagement und zum Notfallmanagement, die im Regelfall den Zielvorgaben der KVG entsprechen. Bei Relevanz wird auch die Möglichkeit eines Ausfalls eines IT-Dienstleisters berücksichtigt und eine diesbezügliche Exit- bzw. Alternativ-Strategie entwickelt und dokumentiert.

		Als erforderlich erkannte Maßnahmen sind auch im Fall der Einbindung von Subunternehmen zu berücksichtigen.
68	Die Risikobewertungen in Bezug auf den sonstigen Fremdbezug von IT-Dienstleistungen sind regelmäßig und anlassbezogen zu überprüfen und ggf. inkl. der Vertragsinhalte anzupassen.	