Datum: 12.04.2019 | Kategorie: Investment Management

BaFin veröffentlicht Entwurf des Rundschreibens 07/2019 - Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)

Mit Datum vom 8. April 2019 hat die BaFin den Entwurf des Rundschreibens "Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)? zur Konsultation veröffentlicht. Die Konsultation endet am 15.05.2019.

Das Rundschreiben findet Anwendung auf alle Kapitalverwaltungsgesellschaften im Sinne des § 17 Kapitalanlagegesetzbuch (KAGB), soweit diese über eine Erlaubnis nach § 20 Abs. 1 KAGB verfügen. Das Rundschreiben findet insbesondere keine Anwendung auf Verwahrstellen, registrierte KVGen nach § 44 KAGB oder extern verwaltete Investmentgesellschaften.

Das Rundschreiben gibt dem Management einen flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausgestaltung der IT vor, insbesondere auch für das Management der IT-Ressourcen und für das IT-Risikomanagement. Die in den Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften (KAMaRisk) enthaltenden Anforderungen an die IT bleiben unberührt, werden jedoch durch das Rundschreiben konkretisiert. Dies betrifft folgende Bereiche:

a) IT-Strategie
b) IT-Governance
c) Informationsrisikomanagement
d) Informationssicherheitsmanagement
e) Benutzerberechtigungsmanagement
f) IT-Projekte, Anwendungsentwicklung (inkl. IDV)
g) IT-Betrieb (inkl. Datensicherung)
h) Auslagerung und sonstiger Fremdbezug von IT-Dienstleitungen

Inhaltlich sind insbesondere folgende Neuerungen durch die KAIT hervorzuheben:

Die KVG hat die Funktion des Informationssicherheitsbeauftragten einzurichten. Diese ist organisatorisch und prozessual unabhängig auszugestalten, d.h. unabhängig von Bereichen, die z. B. für den IT-Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind. Zu seinen Aufgaben gehören insbesondere die Realisierung von Informationssicherheitsmaßnahmen und deren Überwachung. Regelmäßig, mindestens vierteljährlich hat der Informationssicherheitsbeauftragte die Geschäftsleitung über den Status der Informationssicherheit zu berichten.

Für die von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen sind Programmierstandards festzulegen und einzuhalten. In einem zentralen Register sollen die Informationen zu den verwendeten IDV dokumentiert werden. In Abhängigkeit vom ermittelten Schutzbedarf sind die technischen Schutzmaßnahmen für diese Anwendungen festzulegen und umzusetzen.

Auslagerungen von IT-Dienstleistungen haben die Anforderungen nach Ziffer 10 der KAMaRisk zu erfüllen. Wegen der grundlegenden Bedeutung der IT für die KVG ist zukünftig auch für jeden sonstigen Fremdbezug von IT-Dienstleitungen (z. B. Bezug von Standard-Software, Support beim Betrieb dieser Systeme) vorab

eine Risikobewertung durchzuführen. Die aus der Risikobewertung zum sonstigen Fremdbezug von IT-Dienstleistungen abgeleiteten Maßnahmen sind angemessen in der Vertragsgestaltung zu berücksichtigen. Auch ist die Erbringung der vom Dienstleister geschuldeten Leistung entsprechend der Risikobewertung zu überwachen.

Quelle:
Konsultation 07/2019