Jens Kock
Chartered Accountant (CA)
Certified Information Systems Auditor (CISA)
Krummacker 1a
24558 Henstedt-Ulzburg
Jkock.ca@gmail.com
30. März 2018

An die
Bundesanstalt für Finanzdienstleistungsaufsicht
Per E-Mail an konsultation-04-18@bafin.de

GESCHÄFTSZEICHEN: VA 36-I 2802-2018/0001
STELLUNGNAHME IM RAHMEN DER KONSULTATION 04-2018

Sehr geehrte Damen und Herren,

ich möchte den Entwurf des Rundschreibens „Versicherungsaufsichtliche Anforderungen an die IT (VAIT)“ wie folgt kommentieren:

Abschnitt 2, IT-Governance, enthält detaillierte Angaben, die die IT-Aufbau und -Ablauforganisation betreffen. Es ist m.E. jedoch auch erforderlich, Anforderungen an die Geschäftsleitung selbst zu stellen, da auch auf dieser Ebene ein Mindestmaß an Verständnis für die Risiken aus dem Betrieb von komplexen IT Systemen unentbehrlich ist. Das bedeutet:

- Die Geschäftsleitung hat darauf zu achten, dass sie als Organ über IT-Kompetenz verfügt, die dem Risikoprofil des Unternehmens entsprechend angemessen ist;
- Jedes Organ der Geschäftsleitung (z.B. Vorstand, Aufsichtsrat) sollte über ein entsprechendes Mindestmaß an IT-Kompetenz verfügen.

Des Weiteren sollte das Rundschreiben m.E. die Verantwortung der Geschäftsleitung noch klarer ausführen:

- Implementierung von IT Governance Best Practices im Sinne des Rundschreibens;
- Aufbau eines IT Governance Frameworks;
- Einschätzen und Überwachen aller IT Risiken einschließlich IT Sicherheit;
- Begrenzen der IT Risiken gemäß der Risikotoleranz des Unternehmens;
- Effektives Management von IT-Vermögenswerten, Bewertung und Überwachung von IT-Investitionen und -ausgaben;
- Verantwortung dafür, dass IT-Projekte ihre Ziele erreichen und die dafür getätigten Investitionen gerechtfertigt sind;
- Verantwortung dafür, dass die IT ihren Zweck im Sinne der Unternehmens- und IT-Strategie erfüllt; and
- Letztendlich verantwortlich für die Kontrolle über Information und Daten des Unternehmens.

Der Umfang der Tätigkeiten, die seitens der Geschäftsführung nötig sind, um dieser Verantwortung gerecht zu werden, hängt von der Kritikalität der IT für das Unternehmen ab, als auch vom Risikoprofil des Unternehmens. Ggf. lässt sich die Verantwortung an ein Mitglied der Geschäftsführung – z.B. einen Chief Information Officer, CIO oder einen Chief Technical Officer, CTO – oder an ein Gremium – z.B. ein IT-Strategie-Komitee – delegieren.

Mit freundlichen Grüßen

Jens Kock, CISA, CA