FINBRIDGE

based on competence and commitment

++ COMING SOON ++

KAIT für KVGen

Am 08.04.2019 veröffentlichte die Bafin den Entwurf eines Rundschreibens "Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)". Damit führt die Bafin die Detaillierung und Verschärfung der Anforderungen an die IT-Governance für Kapitalverwaltungsgesellschaften (KVGen) nach dem Vorbild der Anforderungen an Banken "Bankaufsichtliche Anforderungen an die IT (BAIT)"und Versicherungsunternehmen "Versicherungsaufsichtliche Anforderungen an die IT (VAIT)"fort.

Ziele der KAIT

Zentrales Ziel der neuen Regulatorik ist, die IT-Sicherheit im Markt zu erhöhen und das IT-Risikobewusstsein in den KVGen zu schärfen. 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 KAIT gibt detaillierte Hinweise zur Auslegung der nationalen und europarechtlichen Vorschriften über die Geschäftsorganisation, soweit sie sich auf die technisch-organisatorische Ausstattung der KVGen beziehen (vgl. Abbildung 1):

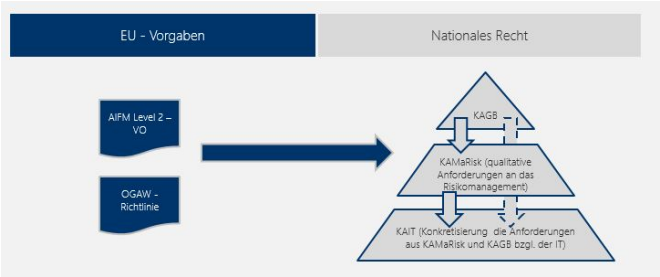

Abbildung 1: *Einbindung der KAIT im Aufsichtsrecht für KVGen.*

IT-Strategie Bezüglich der Anforderungen an die IT-Strategie aus den Mindestanforderungen an das Risikomanagement für KVGen (KaMaRisk) werden in der KAIT weitere Mindestinhalte definiert. So hat die IT-Strategie z.B. Aussagen zur IT-Aufbau und Ablauforganisation, IT-Prozessen, Informationssicherheit und dem Zielbild der IT-Architektur zu treffen (vgl. Abb.2). Des Weiteren sind messbare Kriterien zur Ermittlung und Überprüfung des Zielbildes festzulegen, sowie ein Genehmigungs- und Kommunikationsprozess einzuführen.

IT-Governance ist die Definition der Struktur zur Steuerung und Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der dazugehörigen IT-Prozesse unter adäquater Ressourcenausstattung und Qualifikation des Personals.

Abbildung 2: *Beispielhafte Übersicht der Themen, die gemäß KAIT in der IT-Strategie behandelt werden müssen.*

Hierbei sind die in der IT-Strategie definierten Regelungen zu IT-Aufbau und Ablauforganisation umzusetzen. Bei der Umsetzung ist zudem auf die Berücksichtigung der Schnittstelle zu den Verwahrstellen und wichtigen Auslagerungsunternehmen zu achten. Es ist auf eine angemessene Ressourcenausstattung der IT zur Erfüllung der Aufgaben zu achten, und Prozesse sind frei von Interessenskonflikten zu definieren. Kriterien für den Betrieb und Anwendungsentwicklung sind festzulegen und dadurch gemessene IT-Risiken sind adäquat zu überwachen und zu steuern. Ein Notfallmaßnahmenplan zur Fortführung der Geschäftstätigkeit ist einzurichten.

Informationsrisikomanagement Die Identifikations-, Bewertungs-, Überwachungs- und Steuerungsprozesse der KVG 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 Behandlung von Restrisiken zu umfassen. Das System zum Management von IT Risiken ist unter Mitwirkung aller Beteiligten (inklusive der Fachbereiche als Eigentümer der Information) und frei von Interessenskonflikten umzusetzen. Ein Überblick über die Bestandteile des Informationsverbunds, Abhängigkeiten und Schnittstellen ist aufzustellen. Eine Methodik zur Ermittlung der Schutzbedarfe mit Hinblick auf die Schutzziele ist zu

entwickeln und darauf basierend ein Referenzmaßnahmenkatalog zur Umsetzung dieser festzulegen. Eine Risikoanalyse hat zu erfolgen, akzeptierte Restrisiken sind in den operationalen Risikomanagementprozess zu überführen. Die Risikosituation ist regelmäßig der Geschäftsleitung zu berichten.

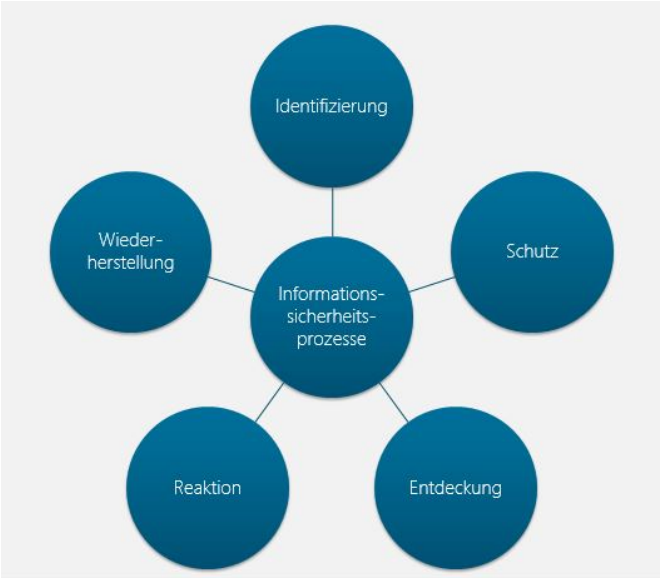

Abbildung 3: *Übersicht der Life Cycles der Informationssicherheitsprozesse gemäß KAIT.*

Informationssicherheitsmanagement Die Geschäftsleitung hat eine Informationssicherheitsleitlinie zu beschließen und angemessen zu kommunizieren. Auf Basis der Informationssicherheitsleitlinie sind konkrete Informationssicherheitsrichtlinien und Informationssicherheitsprozesse mit den Teilprozessen (Life Cycles) Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren (vgl. 3. Die Stelle eines Informationssicherheitsbeauftragten ist zu definieren und ins Organigramm aufzunehmen. Dieser Aufgabenbereich ist organisatorisch und prozessual unabhängig zu gestalten und muss mit umfassenden Kompetenzen ausgestattet werden, die die Wahrnehmung aller Belange der Informationssicherheit des Instituts und gegenüber Dritten erlauben. Der Informationssicherheitsbeauftragte hat der Geschäftsleitung regelmäßig, mindestens vierteljährlich, über den Status der Informationssicherheit sowie anlassbezogen zu berichten.

Benutzerberechtigungsmanagement Das Berechtigungskonzept bestimmt Umfang und Nutzungsbedingung der Zugriffsrechte, welche unter dem Sparsamkeitsprinzip (Need-to-know-Prinzip) zu vergeben sind. Der Berechtigungsmanagementprozess hat unter Einbindung der fachlich Verantwortlichen Stelle zu erfolgen. Technische User sind handelnden und verantwortlichen Personen zuzuordnen, bspw. für die Re-zertifizierung der Zugriffsrechte. Ein allgemeiner Re-Zertifizierungsprozess ist einzurichten und zu dokumentieren. Die Funktionstrennung für die verantwortliche Stelle für Nutzerberechtigungen und den berechtigten Nutzern/Organisationseinheiten ist einzuhalten.

IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen) Es ist ein Vorgehensmodell für die Anwendungsentwicklung festzulegen. Zudem sind Prozesse zu entwickeln die Vorgaben zum Anforderungsmanagement, Programmierrichtlinien, zur Qualitätssicherung, Test, Abnahme und Freigabe enthalten (vgl. Abb. 4). Die Anforderungen an IT-Systeme gelten auch für IDV Anwendungen entsprechend.

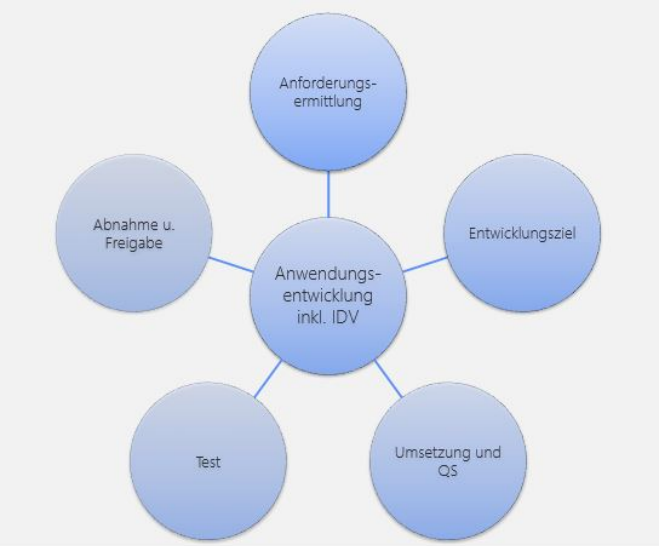

Abbildung 4: *Gemäß KAIT sind klare (Prozess-)Vorgaben zur Anwendungsentwicklung zu formulieren. Die Abbildung zeigt eine Übersicht der relevanten (Teil-)Aspekte.*

IT-Betrieb (inkl. Datensicherung) Ein Life Cycle Management über ein zentrales Register/ Inventar für die Steuerung und Verwaltung des Portfolios der IT-Systeme ist einzuführen. Änderungsanträge an IT-Systeme sind zu dokumentieren, risikoorientiert zu bewerten, zu priorisieren, zu genehmigen und geregelt umzusetzen (Change Management). Weiterhin sind Störungen, sowie deren Ursache und Lösung risikoorientiert zu bewerten, zu steuern und zu berichten. Ein Datensicherungskonzept unter Berücksichtigung der Anforderungen an die Verfügbarkeit, Lesbarkeit und Aktualität der Daten, abgeleitet aus den Geschäftsfortführungsplänen ist zu etablieren. Durchgeführte Datensicherungen sind regelmäßig auf die Nutzbarkeit zu prüfen.

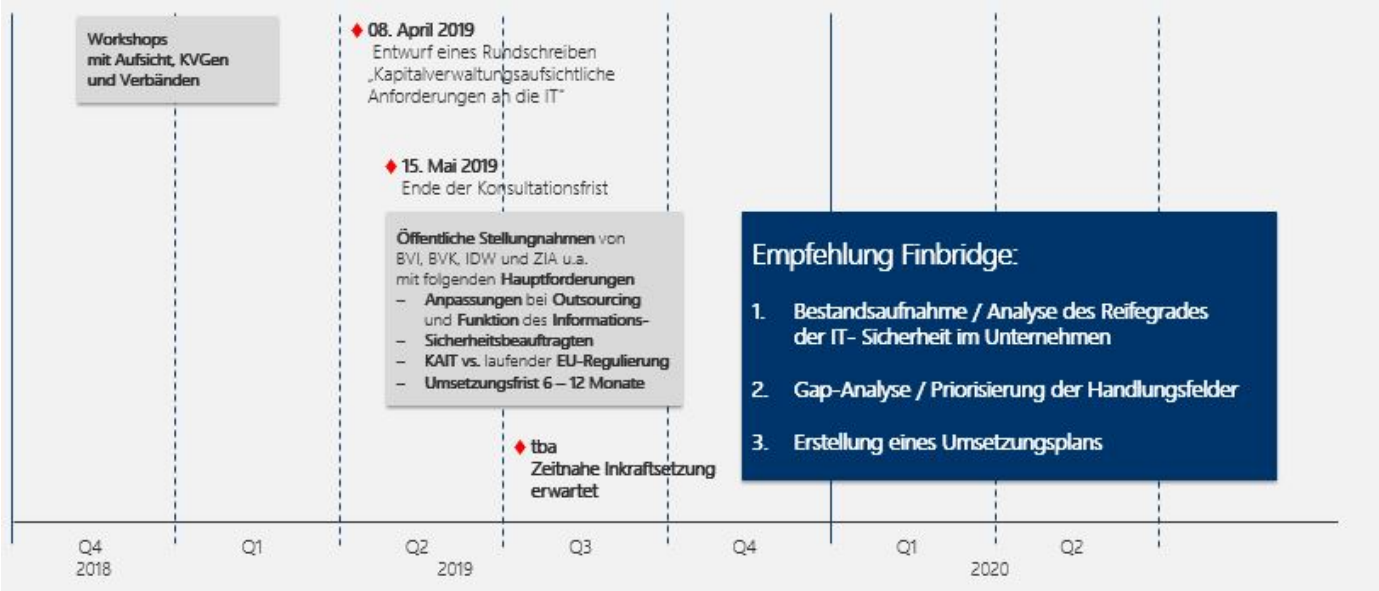

Abbildung 5: *Roadmap zu den Anforderungen der KAIT.*

Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
Die Regelungen für Auslagerungen und sonstigen Fremdbezug werden in BAIT II.8 näher spezifiziert im Hinblick auf die strategische Steuerung, Risikobewertung und Einbindung der relevanten Funktionen, ableitbare Maßnahmen der Risikobewertung bei der Vertragsgestaltung, regelmäßige und anlassbezogene Überprüfungen sowie die Überwachung der Leistungserbringung und Restrisiken.

Fazit

Das Rundschreiben formuliert sehr detaillierte Anforderungen an die IT-Prozesse und Funktionen der betroffenen KVGen, die regelmäßig durch Wirtschaftsprüfer und Aufsicht geprüft werden und, nach aktuellem Stand, nach Beendigung der Konsultationsphase ab sofort gelten, siehe auch Abb.5. Daher empfehlen wir dringend den zeitnahen Start einer Bestandsaufnahme der betroffenen Prozesse und Funktionen sowie die Ausarbeitung eines Umsetzungsplanes inklusive Priorisierung der Umsetzung der aufgedeckten Handlungsfelder.

Unser Angebot

Gerne begleiten wir Sie bei der Bestandaufnahme der relevanten Prozesse und Funktionen, der Erstellung eines detaillierten und priorisierten Umsetzungsplans (Roadmap) sowie der anschließenden Umsetzung der Maßnahmen zur zeitnahen Erfüllung der KAIT.

Durch Nutzung unseres etablierten Vorgehensmodells (vgl. Abbildung 6) sowie durch unsere langjährige Projekt- und Umsetzungserfahrung vergleichbarer regulatorischer Anforderungen ermöglichen wir eine effiziente und risikoorientierte Abarbeitung der identifizierten Handlungsfelder. Dazu zählen typischerweise:

- **IT-Strategie:** Ergänzung und Verfeinerung um Aussagen zu
  - Zielbild der IT-Architektur,
  - Notfallmanagement und Geschäftsfortführung,
  - IDV Anwendungen.
- **Informationssicherheitsbeauftragter:** Strategische Beratung bei der Definition des Aufgabenfeldes eines Informationssicherheitsbeauftragten und Analyse, Einführung und Etablierung geeigneter Prozesse in Bezug auf Informationssicherheit innerhalb der Organisation.
- **Überwachungs- und Steuerungsprozesse:** Überprüfung hinsichtlich der Best-Practise-Methoden (COBIT, ITIL, COSO).
- **Notfallkonzept:** Erstellung bzw. Validierung des Notfallkonzepts.
- **IT-Risiken:** Berücksichtigung von IT-Risiken und daraus resultierenden Schutzmaßnahmen in den Entscheidungsprozessen der KVG, Konzeption von Risikoanalysen, Erstellung eines

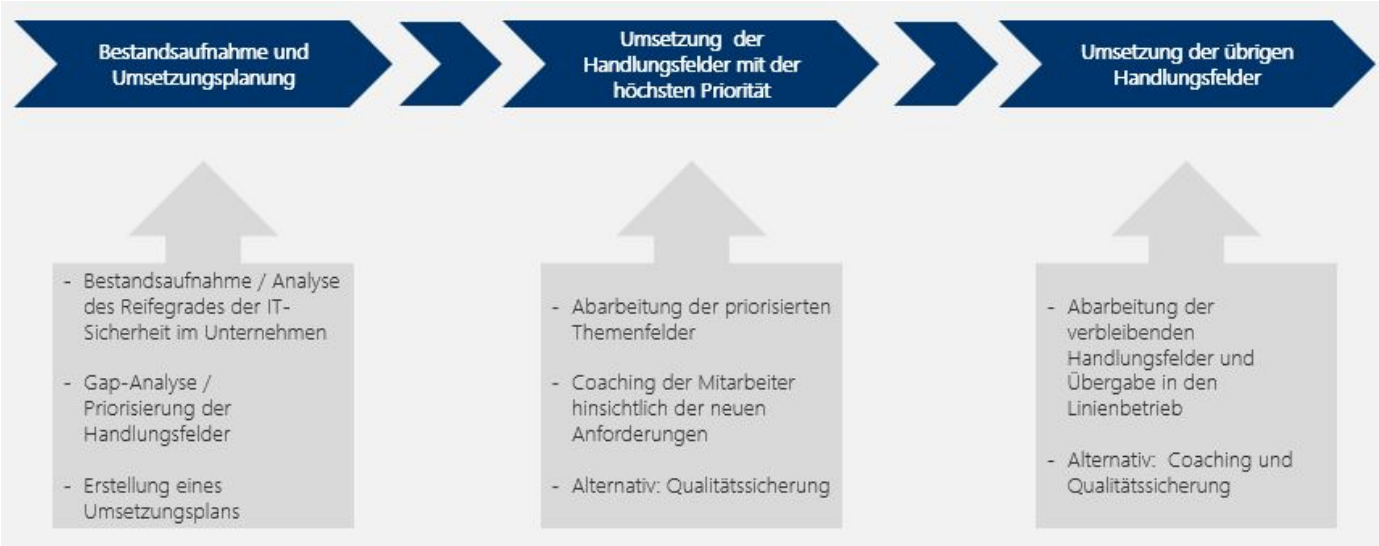

Abbildung 6: *Finbridge GmbH & Co. KG Vorgehensmodell zur Analyse und Umsetzung des Handlungsbedarfs aus der KAIT.*

Sollmaßnahmenkatalogs.

- **Informationssicherheitsleitlinie:** Erstellung bzw. Validierung und Definition von geeigneten Richtlinien und Prozessen.
- **IT-Berechtigungskonzepte:** Überprüfung der IT-Berechtigungskonzepte (Need To Know Prinzip) und Validierung der Rechtevergabeprozesse, Genehmigungs- und Kontrollprozesse und Unterstützung bei etwaigen Anpassungen an den IT-Systeme.
- **Vorgehensmodell für IT-Projekte:** Review des Vorgehensmodells für die Durchführung und Überwachung von IT-Projekten inkl. Testmanagement.
- **IDV Anwendungen:** Prüfung auf Schutzbedarf und Dokumentation (Zentrales Register).
- **Vertragsdatenbank für Outsourcing Verträge:** Aufbau einer entsprechenden Datenbank
- **Risikobewertung:** Durchführung einer Risikobewertung von ausgelagerten IT-Dienstleistungen.

Sprechen Sie uns gerne an!

Kontakt

FINBRIDGE
based on competence and commitment

Steffen Jahr
Senior Manager

Finbridge GmbH Co. KG
Louisenstraße 100
61348 Bad Homburg
www.finbridge.de

Telefon: +49 6172 499770
Telefax: +49 6172 49977-11
Mobil: +49 151 58 06 28 02
steffen.jahr@finbridge.de

FINBRIDGE
based on competence and commitment

David Lingler
Geschäftsführer

Finbridge GmbH Co. KG
Louisenstraße 100
61348 Bad Homburg
www.finbridge.de

Telefon: +49 6172 499770
Telefax: +49 6172 49977-11
Mobil: +49 175 52 42 930
david.lingler@finbridge.de