plenum

finanzinstitute

die kait: anforderungen an die it-compliance

aktuelle handlungsbedarfe für kapitalverwaltungsgesellschaften

regulierung der IT nun auch in den KVGen

Nach der Veröffentlichung der BAIT (Banken) in 2017 und der VAIT (Versicherungen) in 2018 ist nun auch der Einsatz von IT in Kapitalverwaltungsgesellschaften in den Fokus der Bafin geraten. Mit den KAIT hat die Aufsicht zum 01. Oktober 2019 ein verbindliches Regelwerk über die Anforderungen an die IT von Kapitalverwaltungsgesellschaften veröffentlicht. Vor allem für kleinere Gesellschaften stellen diese Anforderungen eine erhebliche Herausforderung dar.

spezifische risiken der KVG-IT

Die Banken und Versicherungen wurden bereits reglementiert, nun folgen die Kapitalverwaltungsgesellschaften.

Aus Sicht der Aufsicht verarbeiten Kapitalverwaltungsgesellschaften analog zu Banken sensible Daten ihrer Kunden und stellen in ihrer Gesamtheit eine kritische Infrastruktur dar.

Konsequenterweise wendet die Bafin daher für die i.d.R. kleineren, unabhängigen KVGen nun die gleichen Maßstäbe wie für die Kreditinstitute und Versicherungskonzerne an.

Situation bei den KVGen

Insbesondere die KVGen, die Captives von Banken und Versicherungen sind, haben – erzwungen über die Regulierung des Konzerns – bereits weite Teile der KAIT in Umsetzung.

Die Mehrzahl der KVGen jedoch hatte die Anforderungen an die IT bislang nicht im Fokus, zumal bei vielen Häusern weder die Ressourcen noch die Mittel vorhanden sind, um die notwendigen Maßnahmen umzusetzen.

Parallel sind jedoch gerade für kleinere Häuser die Cyberrisiken weiter angestiegen. Denn gerade kleinere KVGen sind heute über das Internet mit zahlreichen Marktpartnern und Kunden vernetzt und sind damit aus verschiedenen Richtungen ständigen Bedrohungen ausgesetzt.

KAIT sind bereits wirksam

Da die KAIT lediglich die Regelungen des KAGB, der KAVerOV und der AIFM-VO sowie der KAMaRisk konkretisieren (vgl. Abb. 1), räumt die BaFin – wie bereits bei Einführung der BAIT und VAIT – den KVGen keine Übergangsfrist ein.

Ab 01.10.2019 wird ihre Beachtung vorausgesetzt.

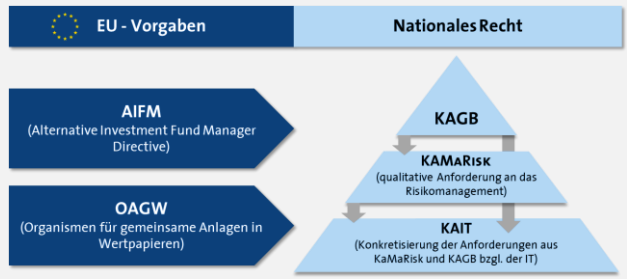

Abb. 1: EU-Vorgaben und nationales Recht

gleiche anforderungen für alle

Ziel der KAIT ist, eine verbindliche, einheitliche und zu Kreditinstituten vergleichbare Auslegung der Anforderungen aus KAGB und KAMaRisk für die IT-Organisation in Kapitalverwaltungsgesellschaften zu erreichen.

Die Bafin setzt bei der Formulierung der KAIT auf etablierte und anerkannte Standards. So werden zu verschiedenen Regelungsbereichen der IT-Sicherheit die IT-Grundschutzkataloge des BSI und die ISO/IEC 270XX Normenreihe herangezogen.

Für die Anforderungen an die Governance der IT wiederum setzen die KAIT auf den Frameworks CobIT und ITIL auf.

Die Aufsicht erwartet, dass durch Anwendung dieser Standards ein für jede Kapitalverwaltungsgesellschaft gestaltbarer Rahmen geschaffen wird, der die konkrete Umsetzung erleichtert – und gleichzeitig das Prüfungshandeln vereinheitlichen und damit vereinfachen wird.

Ob KVGen bei der Umsetzung von Maßnahmen Vereinfachungen vornehmen dürfen, wird sich v.a. an der Komplexität des Unternehmens und seiner IT orientieren (Proportionalitätsprinzip).

die acht themenfelder der KAIT

Die KAIT bündelt die fast 70 Einzelanforderungen in acht Themenfeldern und lehnt sich in deren Strukturierung eng an die BAIT der Kreditinstitute an.

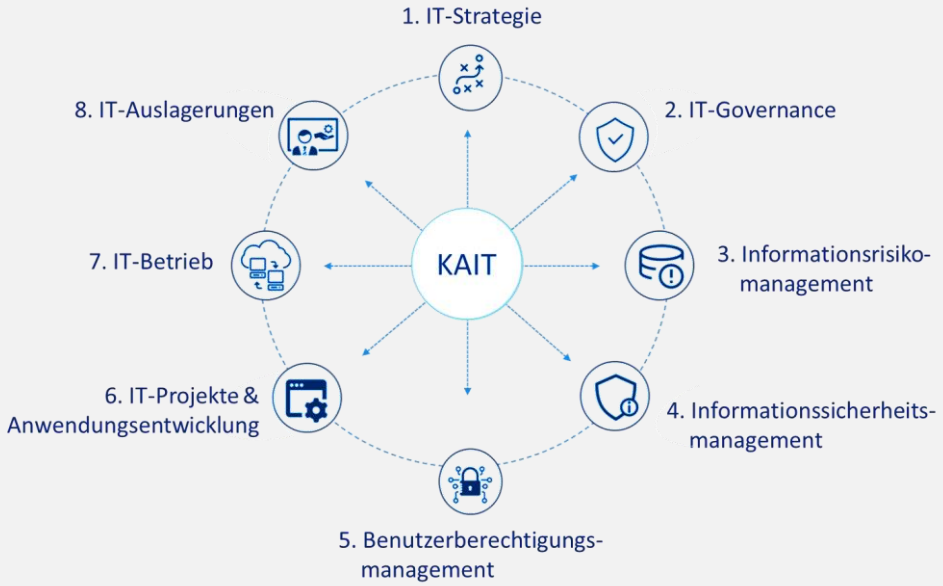

Abb. 2: Themenfelder der KAIT

1. it strategie

Formulierung einer detaillierten, konkreten und an der Geschäftsstrategie orientierten IT-Strategie, die u.a. Organisations- und IT-Risiko-Fragestellungen adressiert.

2. it governance

Mechanismen zur wirksamen Umsetzung und Steuerung der IT-Strategie durch eine Organisation, die frei von Interessenkonflikten gestaltet ist.

3. informationsrisikomanagement

Nutzung von Prozessen zur Erkennung und Steuerung von Risiken für die Schutzziele der Informationssicherheit.

4. informations-sicherheitsmanagement

Etablierung eines Systems zur Herstellung und Aufrechterhaltung eines angestrebten Sicherheits-niveaus.

5. benutzer-berechtigungsmanagement

Verfahren zur Einrichtung, Änderung und Entfernung von Berechtigungen unter Wahrung von Minimal- und Funktions-trennungsprinzip.

6. it projekte & anwendungsentwicklung

Regelungen zur Bereitstellung von Änderungen an IT-Systemen, von der Anforderungs-definition bis zur Produktivstellung (inkl. Individuelle Datenverarbeitung).

7. it betrieb

Sicherstellung eines sicheren IT-Betriebs und kontrollierter Änderungen der IT-Systeme – unter Zuhilfenahme eines aktuellen Asset-Registers.

8. auslagerungen

Steuerung insbesondere der Risiken von IT-Auslage-rungen und sonstigem Fremdbezug. Sowie Aufrecht-erhaltung der erforderlichen IT-Kenntnisse zur Steuerung des jeweiligen Dienstleisters.

unterschiedliche handlungsbedarfe

Inwiefern Ihr Haus einen konkreten Handlungsbedarf aufweist, können Sie in einem ersten Schritt mit unserem KAIT Self Assessment ermitteln: Falls Sie eine der Fragen nicht eindeutig mit „Ja“ beantworten können, ist eine tiefer gehende Analyse angeraten.

kait self assesssment – auszug aus dem anforderungskatalog

Ausgewählte Fragestellungen der KAITs	ja	tlw.	Nein	?
IT-Strategie				
Wird Ihre IT-Strategie fortlaufend an die Geschäftsstrategie angepasst, mit Performance Indikatoren überwacht und durch Maßnahmen umgesetzt?	○	○	○	○
Enthält Ihre IT-Strategie Aussagen u.a. zu Informationssicherheit, Auslagerungen, Notfallmanagement und individueller Datenverarbeitung?	○	○	○	○
Haben sie eine Business Continuity Strategie etabliert?	○	○	○	○
IT-Governance				
Beachtet Ihre Aufbau- und Ablauforganisation das Funktionstrennungsgebot?	○	○	○	○
Sind u.a. IT-Sicherheit, IT-Risiko, IT-Betrieb und Anwendungsentwicklung quantitativ und qualitativ ausreichend personell besetzt?	○	○	○	○
Haben sie ein funktionsfähiges Notfallmanagement zur Fortführung des Geschäftsbetriebs etabliert?	○	○	○	○
Informationsrisikomanagement				
Ist ein integriertes, die Fachbereiche umfassendes Informationsrisikomanagement etabliert, das in das Risikoreporting eingebunden ist?	○	○	○	○
Verfügen Sie über einen aktuellen und vollständigen Überblick über die Bestandteile des Informationsverbundes, dessen Abhängigkeiten und Schnittstellen?	○	○	○	○
Haben sie IT-Risiken identifiziert, welche sie überwachen und anhand von Risikokriterien steuern?	○	○	○	○
Informationssicherheitsmanagement				
Sind die Informationssicherheitsleitlinie konkretisierende, aktuelle Informationssicherheitsrichtlinien und -prozesse definiert und wird deren Einhaltung kontrolliert?	○	○	○	○
Verfügt Ihr Institut über einen organisatorisch unabhängigen Informationssicherheitsbeauftragten, der regelmäßig direkt an die Geschäftsleitung berichtet?	○	○	○	○
Ist ihr Informationssicherheitsbeauftragter in die Erstellung und Fortschreibung des IT-Notfallkonzepts mit eingebunden?	○	○	○	○
Benutzerberechtigungsmanagement				
Berücksichtigt Ihr Benutzerberechtigungsmanagement das Prinzip der Funktionstrennung und den Sparsamkeitsgrundsatz?	○	○	○	○
Sind aufbauend auf diesen Prinzipien Berechtigungskonzepte für alle IT-Systeme definiert und wird Ihre Beachtung unabhängig überprüft?	○	○	○	○
Werden Ihre technischen Benutzer zur Maschine-zu-Maschine-Kommunikation in einem Zentralverzeichnis verwaltet?	○	○	○	○
IT-Projekte & Anwendungsentwicklung				
Werden die Vorgaben der Anwendungsentwicklung in Ihrem Institut an den Schutzbedarf der Anwendungen bzw. der verarbeiteten Daten angepasst?	○	○	○	○
Gilt dies auch für dezentral in den Fachbereichen auf Basis von bspw. Office-Produkten erstellte Anwendungen, sog. Individuelle Datenverarbeitung (IDV)?	○	○	○	○
Ist ein Regelprozess der Entwicklung, des Testens, der Freigabe und der Implementierung in die Produktionsprozesse etabliert?	○	○	○	○
IT-Betrieb				
Sind die Komponenten aller IT-Systeme sowie deren Beziehungen untereinander erfasst und werden diese Informationen aktuell gehalten?	○	○	○	○
Werden Datensicherungen gemäß der Geschäftsfortführungspläne vorgenommen und werden diese Sicherungen auf Wiederherstellbarkeit und Lesbarkeit geprüft?	○	○	○	○
Sind die Standardprozesse zur Betriebssteuerung wie Incident-, Problem-, Configuration- und Change-Management etabliert?	○	○	○	○
IT-Auslagerungen				
Werden Risikobewertungen für Auslagerungen und „Sonstigen Fremdbezug“ durchführt und werden diese Risiken überwacht und gesteuert?	○	○	○	○
Überwachen und steuern sie sämtliche Verträge zu Fremdbezug und Auslagerungen in einem zentralen Verzeichnis?	○	○	○	○
Integrieren Sie in dieses Verfahren auch den Fremdbezug von Clouddiensten, auch wenn dieser dezentral seitens der Fachbereiche erfolgt?	○	○	○	○

unser angebot: der KAIT quick check

plenum führt seit vielen Jahren sehr erfolgreich regulatorische Projekte für die IT von Kreditinstituten und konzerngebundene KVGen durch. Die hier gewonnenen Erkenntnisse über die Prüfungspraxis der Aufsicht kombinieren wir für Sie zu einem „KAIT Quick Check“, der Ihnen in kurzer Zeit Ihre individuellen Handlungsbedarfe aufzeigt.

Als Partner der IT betrachten wir die IT und ihre Risiken hierbei „end-to-end“ entlang der Leistungsprozesse und gehen den Risikoursachen sorgfältig auf den Grund. Denn unser Auftrag endet nicht damit, die IT „durchzuprüfen”, sondern beginnt damit erst.

Mit einem kompakten und ressourcenschonenden Vorgehen bieten wir Ihnen eine Standortbestimmung innerhalb weniger Wochen. Neben den Schwachstellen Ihrer IT aus Sicht der KAIT zeigen wir Ihnen hierin auf, mit welchen Sofortmaßnahmen Sie Ihre Compliance kurzfristig steigern können.

Der wichtigste Mehrwert in unserem Vorgehen liegt jedoch darin, dass wir auf Basis unserer mehr als 25 Jahre Erfahrung mit Ihnen zukunftsorientierte Maßnahmen erarbeiten, die für eine angemessene & nachhaltige Compliance sorgen – damit Sie sich wieder voll auf Ihr Kerngeschäft konzentrieren können.

plenum AG
Management Consulting

THE SQUAIRE WEST 15 | Am Flughafen | D-60549 Frankfurt am Main
Telefon: +49 69 6435524-0 | Fax: +49 69 6435524-60 | Internet: www.plenum.de