VAIT

VAIT – Versicherungsaufsichtliche Anforderungen an die IT

Eine effiziente und risikoorientierte Umsetzung neuer regulatorischer Anforderungen und deren effektive Nutzung auch zur Optimierung der Unternehmensführung und -überwachung sind heute wichtiger denn je.

Management Summary

Mitte 2018 veröffentlichte die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT), welche unmittelbar in Kraft traten.

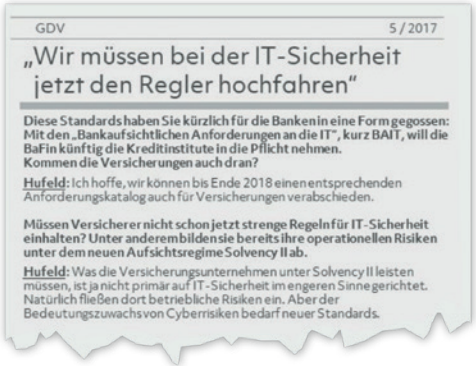
Im Fokus der BaFin steht hierbei, eine verbindliche Grundlage für das Management der IT zu schaffen. Gängige Standards und der jeweilige Stand der Technik sind hierbei angemessen zu berücksichtigen.

Steigende Regulierung erfordert ein zunehmend risikoorientiertes Compliance-Management.

Die aktive Steuerung der IT-Risiken eines Versicherers ist ein entscheidender Entwicklungsschritt – weg von einer reinen Erfüllung aufsichtsrechtlicher Pflichtenkataloge.

Ausgangssituation

In einem Interview zwischen dem Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) und dem Bafin-Präsidenten Felix Hufeld vom Mai 2017 zeichnete sich bereits damals die wachsende Bedeutung an die IT deutscher Versicherer in Form von verschärften Regulierungen ab.


GDV 5 / 2017

„Wir müssen bei der IT-Sicherheit jetzt den Regler hochfahren"

Diese Standards haben Sie kürzlich für die Banken in eine Form gegossen: Mit den „Bankaufsichtlichen Anforderungen an die IT", kurz BAIT, will die BaFin künftig die Kreditinstitute in die Pflicht nehmen. Kommen die Versicherungen auch dran?

Hufeld: Ich hoffe, wir können bis Ende 2018 einen entsprechenden Anforderungskatalog auch für Versicherungen verabschieden.

Müssen Versicherer nicht schon jetzt strenge Regeln für IT-Sicherheit einhalten? Unter anderem bilden sie bereits ihre operationellen Risiken unter dem neuen Aufsichtsregime Solvency II ab.

Hufeld: Was die Versicherungsunternehmen unter Solvency II leisten müssen, ist ja nicht primär auf IT-Sicherheit im engeren Sinne gerichtet. Natürlich fließen dort betriebliche Risiken ein. Aber der Bedeutungszuwachs von Cyberrisiken bedarf neuer Standards.

VAIT

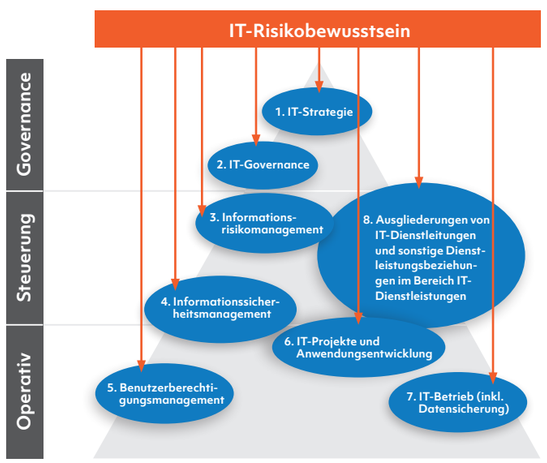
Das Rundschreiben legt die IT-bezogenen Anforderungen des Versicherungsaufsichtsgesetzes (VAG) und der aufsichtsrechtlichen Mindestanforderungen an die Geschäftsorganisation von Versicherungen (MaGo) verbindlich aus.

Betroffen sind alle Erst- und Rückversicherungsunternehmen, sowie Pensionsfonds, die der Aufsicht der BaFin unterliegen. Hiervon ausgenommen sind Versicherungszweckgesellschaften im Sinne des § 168 VAG oder die Sicherungsfonds gemäß § 223 VAG.

Bereits heute nutzt eine Vielzahl von Versicherungsunternehmen gängige Standards, wie z.B. COBIT zur Steuerung ihrer IT sowie den IT-Grundschutz des Bundesamt für Sicherheit in der Informationstechnik (BSI) für das Management der Informationssicherheit und Informationsrisiken.

Zentrales Ziel der BaFin ist es, eine verbindliche Grundlage für das Management der IT zu schaffen und das IT-Risikobewusstsein in den Unternehmen und gegenüber deren IT-Dienstleistern zu schärfen. Dabei sind die Anforderungen der VAIT nicht abschließend zu betrachten. Die BaFin fordert weiterhin die Versicherer auf, sich an den gängigen Standards sowie dem jeweiligen Stand der Technik auszurichten.

Grundlage und Schärfung des Risikobewusstseins

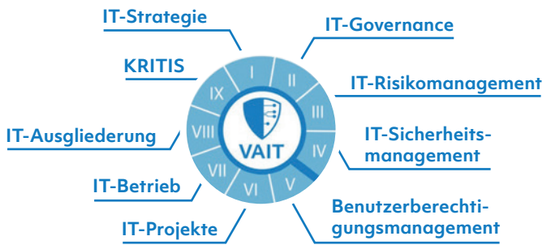


Analyse

Unternehmen haben die Aufgabe, den bisherigen Stand der IT gegen die neu ausformulierten Anforderungen der BaFin zu legen und GAPs zu erkennen und zu schließen.

Vorgesehen ist die Etablierung einer ganzheitlichen IT- Governance-Struktur zur Steuerung, Überwachung und Weiterentwicklung der IT auf Basis der IT-Strategie, welche aus der Geschäftsstrategie abgeleitet wurde.

Anforderungen unterteilen sich in neun Module



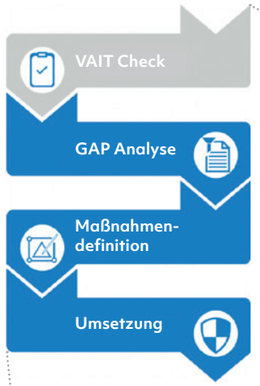
Durch die VAIT müssen Versicherer mit zusätzlichem Dokumentationsaufwand rechnen.

Die bereits bestehenden Dokumentationspflichten aus MaGo und Solvency II werden auf die IT ausgeweitet. Beispielsweise sind ab sofort Leitlinien, Konzepte sowie Register für die Informationssicherheit, Datensicherung und Ausgliederung vorzuhalten. Außerdem ist ein vollständiges Anwendungsregister (inklusive IDV) zu erstellen, welches u.a. die Schutzbedarfe aufzeigt.

Im Rahmen des Informationssicherheitsmanagements fordert die VAIT die Einrichtung der Funktion eines Informationssicherheitsbeauftragten. Diese überwachende Funktion umfasst die Wahrnehmung aller Belange der IT-Sicherheit innerhalb des Unternehmens und gegenüber Dritten.

Weiterhin sind künftig alle wesentlichen Veränderungen an den IT-Systemen im Rahmen von IT-Projekten, deren Auswirkung auf die IT-Aufbau- und IT Ablauforganisation sowie die dazugehörigen IT-Prozesse vorab im Rahmen einer Auswirkungsanalyse zu bewerten.

Auch vor der Ausgliederung von IT-Dienstleistungen ist eine Risikoanalyse durchzuführen. Bereits bestehende Verträge müssen hinsichtlich der Risikosituation überprüft und ggf. angepasst werden.



Lösung

Vom VAIT-Check bis zur Umsetzung: Gerne unterstützen wir Sie mit der notwendigen Methodik und maßgeschneiderten Ansätzen:

- IST-Analyse und Identifizierung möglicher Handlungsfelder in Form eines ersten Workshops mit den relevanten Ansprechpartnern zur Einschätzung der Situation
- Gegebenenfalls unter Heranziehung des aktuellen IT-Prüfungsberichts Ihres Wirtschaftsprüfers
- Risikoorientierte Priorisierung der GAPs. Planung von Workshops je Themenbereich, Ausarbeitung der „Pain-Points“ und Priorisierung der offenen Punkte
- Fokus auf kritische Handlungsfelder
- Maßnahmendefinition unter Abgleich bereits laufender Projekte
- Umsetzung der definierten Maßnahmen mit Blick eines Auditors und Revisors

Welchen Erfüllungsgrad der Anforderungen weist Ihr Unternehmen aktuell auf?

Rn.	Themenblock	Ja	Teilweise	Nein	Risikostatus
1	**IT Strategie** Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente IT-Strategie festzulegen, in der die Ziele sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden. Die IT-Strategie ist durch die Geschäftsleitung regelmäßig und anlassbezogen zu überprüfen und erforderlichenfalls anzupassen. Die Geschäftsleitung muss für die Umsetzung der IT-Strategie Sorge tragen.	✓			
6	**IT-Governance** Die IT-Governance im Sinne dieses Rundschreibens 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 Vorgaben zur IT-Aufbau- und IT-Ablauforganisation, zum Informationsrisiko- sowie Informationssicherheitsmanagement, zur quantitativ und qualitativ angemessenen Personalausstattung der IT sowie zum Umfang und zur Qualität der technisch-organisatorischen Ausstattung. Die Regelungen für die IT-Aufbau- und IT-Ablauforganisation sind bei Veränderungen der Aktivitäten und Prozesse zeitnah anzupassen.	✓			
17	**Informationsmanagement** Das Unternehmen hat im Rahmen des Risikomanagements die mit dem Management der Informationsrisiken verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege zu definieren und aufeinander abzustimmen. Das Unternehmen hat angemessene Identifikations-, Bewertungs-, Überwachungs- und Steuerungsprozesse einzurichten und diesbezügliche Berichtspflichten zu definieren.			✗	
25	**Informationssicherheitsmanagement** Das Unternehmen hat ein Benutzerberechtigungsmanagement einzurichten, welches sicherstellt, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Unternehmens entspricht. Bei der Ausgestaltung des Benutzerberechtigungsmanagements sind die Anforderungen an die Ausgestaltung der Prozesse (siehe II. Rn. 7 und 15) entsprechend zu berücksichtigen.		?		
33	**Benutzerberechtigungsmanagement** Das Unternehmen hat ein Benutzerberechtigungsmanagement einzurichten, welches sicherstellt, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Unternehmens entspricht. Bei der Ausgestaltung des Benutzerberechtigungsmanagements sind die Anforderungen an die Ausgestaltung der Prozesse (siehe II. Rn. 7 und 15) entsprechend berücksichtigen.	✓			
42	**IT-Projekte und Anwendungsentwicklung** 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 Auswirkungsanalyse zu bewerten. Dabei hat das Unternehmen insbesondere die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren. In diese Analysen sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten zu beteiligen. Im Rahmen ihrer Aufgaben sind auch die unabhängige Risikocontrollingfunktion, die Compliance-Funktion und die versicherungsthematische Funktion zu beteiligen, sofern das Unternehmen die jeweiligen Funktionen von Gesetzes wegen einzurichten hat.			✗	
58	**IT-Betrieb** Der IT-Betrieb hat die Erfüllung der Anforderungen, die sich aus der Umsetzung der Geschäftsstrategie sowie aus den IT-unterstützten Geschäftsprozessen ergeben (vgl. II. Rn. 14 und 15), umzusetzen.		?		
65	**Ausgliederung** Bei Ausgliederungen von IT-Dienstleistungen – unabhängig davon, ob es sich hierbei um die Hauptdienstleistung oder um eine ergänzende Nebendienstleistung zu einer anderen Hauptdienstleistung handelt – sind die hierfür jeweils geltenden Anforderungen zu erfüllen; insbesondere ist vorab eine Risikoanalyse durchzuführen. Dies gilt auch für Ausgliederungen von solchen IT-Dienstleistungen, die dem Unternehmen durch ein Dienstleistungsunternehmen über ein Netz bereitgestellt werden (z.B. Rechenleistung, Speicherplatz, Plattformen oder Software) und deren Angebot, Nutzung und Abrechnung dynamisch an den Bedarf angepasst über definierte technische Schnittstellen sowie Protokolle erfolgen (Cloud-Dienstleistungen).	✓			

ppi

VAIT

Theorie & Praxis aus einer Hand!

Unser Geschäftsfeld Versicherungen begleitet Sie auf diesem Wege fachlich und technisch. Wir bieten Ihnen Expertenwissen aus der Erstellung von eigenen Produkten für den Versicherungs- und Bankensektor.

Ob Ableitung einer IT-Strategie, IT-Governance, Business Continuity Management (BCM), IKS, Incident-, Change- oder Releasemanagement sowie Analyse und Neuausrichtung Ihres Berechtigungsvergabeprozesses:

Wir von PPI verfügen über das Know-how und die Umsetzungserfahrung!

Unsere Expertise für Sie

Durch unsere Eigenentwicklung cysmo© verfügen unsere Berater zusätzlich über die Expertise bei der Analyse der Angreifbarkeit der IT-Struktur eines Unternehmens und unterstützen Sie so bei der Einschätzung von Cyber-Risiken.

cysmo© bewertet die Sicherheit der von außen sichtbaren IT-Infrastruktur eines Unternehmens. Somit können Sie sowohl Ihr Unternehmen als auch externe Unternehmen, wie z. B. Dienstleister, bewerten.

Unser Fokus

- Praxistauglichkeit
- Einhaltung regulatorischer Anforderungen
- Ausrichtung an gängigen Standards

Unser maßgeschneidertes Angebot für Sie

- Lernen Sie uns und unser Vorgehen in einem umfassenden, unverbindlichen Workshop kennen.
- Idealerweise nehmen Ihre Ansprechpartner für die entsprechenden Themenbereiche teil.

Gibt es kritische Handlungsfelder?

- Erste Einschätzung möglicher offener Themengebiete
- PPI unterstützt Sie bei der Einschätzung möglicher Risiken, sowie bei der daraus resultierenden Maßnahmenplanung und deren Umsetzung.
- Wir übernehmen Ergebnisverantwortung.

Bei Fragen und für weitere Informationen:

Sebastian Scholz
Partner
T +49 40 227433-1725
M +49 151 62836107
sebastian.scholz@ppi.de

PPI AG
Moorfuhrtweg 13
22301 Hamburg
Germany

Tim Glenewinkel
Managing Consultant
T +49 40 227433-1745
M +49 151 17601697
tim.glenewinkel@ppi.de

PPI AG
Moorfuhrtweg 13
22301 Hamburg
Germany