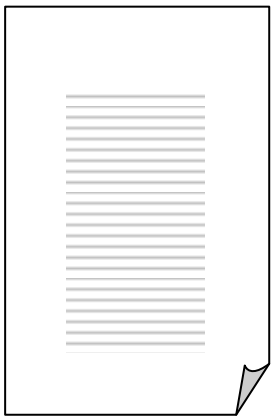
P R E S S E A U S S C H N I T T
P R E S S C O V E R A G E

Kunde/Client:

finanz informatik technologie service

Projekt/Project:	Fachbericht VAIT
Publikation/Medium:	www.datacenter-insider.de
Ausgabe/Issue:	05.07.2019
Page Impressions/Visits:	1,6 Mio. / 1,0 Mio.



FI-TS-PrA-www.datacenter-insider.de_20190705

Das Umsetzen von Regulatorik

Assekuranz kann von Banken lernen, was wichtig ist

05.07.19 | Autor / Redakteur: Christian Thiel* / Ulrike Ostler

Die Versicherungsbranche muss die „Versicherungsaufsichtlichen Anforderungen an die IT“ (VAIT) umsetzen. Doch die Regeln ähneln „Bankenaufsichtlichen Anforderungen an die IT“ (BAIT). Wie wäre es also mit einem Berater, der sich hier auskennt? (Bild: Ulises Baga on Unsplash)

Während Banken darin geübt sind, regulatorische Vorgaben und spezifizierte Prüfungsanforderungen von Aufsichtsbehörden zu erfüllen, stehen Versicherungen am Anfang des Weges. Ein Beispiel sind die „Versicherungsaufsichtlichen Anforderungen an die IT“ (VAIT). Bei deren Implementierung können Assekuranzen von Banken lernen, worauf die Aufsicht in Prüfungssituationen Wert legt.

Der Nachhall der Wirtschaftskrise 2008 ist in den meisten Branchen längst verstummt. Anders ist es bei Banken und Versicherungen: Sie arbeiten weiterhin intensiv daran, regulatorische Vorgaben und spezifizierte Prüfungsanforderungen der Aufsichtsbehörde zu erfüllen.

Die Umsetzung steht 2019 bei Versicherern ganz oben auf der Agenda: Solvency II, Datenschutz, EU-Vermittlerrichtlinie und VAIT - diese Regelwerke führen das Ranking der regulatorischen Vorgaben für Versicherungen zurzeit an.

Unter drei Aspekten ist das Erfüllen dieser Vorgaben herausfordernd. Sie sind mit einem hohen Personalaufwand, Kosten sowie kurzen Erfüllungsfristen verbunden. Letzteres gilt insbesondere für die VAIT.

Verlässlichkeit der IT

Mit dieser Vorgabe hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) einen Kurswechsel in der Versicherungsbranche eingeläutet. Die Prüfer haben bestehende Anforderungen konkretisiert und überprüfen in jeder Assekuranz deren Einhaltung – und zwar ohne Ausnahme.

Einen Vorteil haben Versicherer hierbei: Die VAIT machen Anforderungen nun greifbarer und sind zudem aus der Bankenbranche bereits wohlbekannt. Angesichts der steigenden Bedeutung der IT ist das Handeln der Aufsicht darauf ausgerichtet, Standards für den verlässlichen Betrieb von IT-Systemen durchzusetzen.

Erfahrung der Banken gibt Orientierung

An der VAIT führt kein Weg vorbei. Allerdings können Versicherungen eine hilfreiche Abkürzung einschlagen. Denn Banken und deren IT-Dienstleister stehen schon länger im Blickpunkt der Aufsicht und haben entsprechende Erfahrungen gesammelt. So haben die Institute schon die „Bankenaufsichtlichen Anforderungen an die IT" (BAIT) umgesetzt.

Dieses Regelwerk ist mit der VAIT vergleichbar. Beide sind gleich aufgebaut und haben ähnliche Ziele. Versicherungen können also die Erfahrungen der Banken für sich nutzen und sich so leichter auf Prüfungssituationen einstellen. Insgesamt sind in der VAIT acht Themenfelder erkennbar. Die Prüfer achten insbesondere darauf, dass Versicherer die Prüfungsthemen durchgängig, vollständig und nachhaltig behandeln.

1. IT-Strategie

Die BaFin legt Wert darauf, dass die IT-Strategie der Gesamtstrategie des Versicherungsunternehmens folgt und konsistent ist. Wesentliche Aspekte dabei sind die Aufbau- und Ablauforganisation, die Weiterentwicklung der IT-Architektur sowie Zuständigkeiten der Informationssicherheit.

2. IT-Governance

Im Mittelpunkt der IT-Governance stehen die Steuerung und Überwachung des IT-Betriebs und die Weiterentwicklung der IT-Systeme. Zudem setzen die Prüfer voraus, dass dies auf Basis entsprechender IT-Prozesse erfolgt, die sich an gängigen Standards orientieren.

3. Informationsrisiko-Management

Beim Umgang mit IT-Risiken erwartet die Aufsicht, dass Versicherungen ein entsprechendes Rahmenwerk definieren und unter anderem eine Methodik zur Ermittlung des Schutzbedarfs und Anforderungen zur Umsetzung der Schutzziele festlegen: „Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität" (VIVA).

4. Informationssicherheits-Management

Der Blick der Prüfer richtet sich auf konsistente Leitlinien und konkretisierende Richtlinien als Grundlage für die Informationssicherheit. Nach Auffassung der BaFin stehen diese stets im Einklang mit der Unternehmensstrategie.

Eine zentrale Rolle in diesem Prüfungsfeld nimmt der Informationssicherheitsbeauftragte ein. Er ist frühzeitig bei allen Informationssicherheitsvorfällen einzubinden und berichtet unmittelbar an die Geschäftsführung oder den Vor-stand. Zu seinem Verantwortungsbereich gehört es auch, Sicherheitsrichtlinien zu definieren und diese aktuell zu halten.

5. Benutzerberechtigungs-Management

Die Aufsicht setzt Vollständigkeit, Durchgängigkeit und Konsistenz bei diesem Thema voraus. Die Versicherung muss folgende Fragen beantworten: Wer hat Zugriff auf welche Daten und entsprechen diese Berechtigungen auch den fachlichen und organisatorischen Erfordernissen? An welcher Stelle sind die Rollen der Nutzer definiert? Die Prüfungserfahrungen im Bankensektor haben bei der Zuweisung von Rollen und Nutzerrechten Handlungsbedarf gezeigt.

6. IT-Projekte und Anwendungsentwicklung

In diesem Bereich müssen Versicherungen sicherstellen, dass Änderungen, Tests und die Produktivsetzung von Anwendungen nachvollziehbar und durchgehend dokumentiert sind. Gleichzeitig setzt die BaFin eine klare Trennung zwischen Test- und Produktionssystemen voraus. Zudem müssen IT-Projekte angemessen gesteuert werden und es ist eine Transparenz über das Gesamtport-folio von IT-Projekten und deren Risiken herzustellen.

7. IT-Betrieb

Wesentliche Inhalte dieser Anforderung sind der Überblick über die IT-Komponenten und deren Beziehungen zueinander (Configuration Management System) sowie das Business Continuity Management. Bei Letzterem müssen Versicherungen beim Ausfall eines Rechenzentrums dafür Sorge tragen, dass keine Daten verloren gehen. Aus Sicht der Aufsicht sind redundante Rechenzentren das Mittel der Wahl.

Das Problem: Der eigentlich notwendige Aufbau eines zweiten Rechenzentrums ist für Versicherungen unter wirt-schaftlichen Gesichtspunkten oftmals kaum umsetzbar. Vor diesem Hintergrund denken viele Assekuranzen über die Auslagerung ihres IT-Betriebs nach.

8. Ausgliederungen

Im Falle eines ausgegliederten IT-Betriebs richtet die BaFin ihren Blick auf alle beteiligten IT-Dienstleister. Zum einen sind vor Beauftragung Risiko-Analysen durchzuführen, zum anderen sind sie ebenso gefordert, die VAIT umzusetzen.

Zeit zum Handeln

Ein zentraler Punkt in VAIT-Umsetzungsprojekten ist eine weitreichende Analyse der gewachsenen IT-Strukturen wie die Erfahrungen der Prüfungen im Bankbereich zeigen. An dieser Stelle besteht nicht nur dringender Handlungsbedarf, sondern auch großes Potenzial, um die Effizienz zu erhöhen.

Angesichts der schwierigen Bedingungen am Kapitalmarkt sowie fehlendem Nachwuchs für den IT-Bereich denken Verantwortliche vermehrt dar-über nach, ihren IT-Betrieb auszulagern. Im Mittelpunkt der Überlegungen steht die Frage nach einem geeigneten IT-Dienstleister. Denn Versicherer stellen nicht nur bei aufsichtsrechtlichen Vorgaben hohe Anforderungen, sondern auch bei anderen Inhalten wie etwa dem Schutz personenbezogener Kundendaten.

Die Auswahl möglicher IT-Provider ist dabei überschaubar. Angesichts der hohen regulatorischen Hürden haben sich branchenunabhängige IT-Dienstleister aus dem Markt zurückgezogen. Infrage kommen daher Provider, die Branchenkenntnisse vorweisen können und in der Finanz- und Versicherungswirtschaft eine nachvollziehbare Strategie verfolgen wie etwa Finanz Informatik Technologie Service.

Dazu zählen auch Erfahrungen im Umgang mit der Regulatorik, insbesondere den BAIT sowie mit Prüfverfahren. Mit diesem Wissen sind sie in einer guten Ausgangsituation, um Versicherungen bei der Umsetzung der VAIT zur Seite zu stehen.

Was Provider leisten können

Wenn sich Versicherungen für die Zusammenarbeit mit einem branchenversierten IT-Dienstleister entscheiden, erhalten sie Zugriff auf IT-Services, die den hohen Anforderungen von Versicherungen gerecht werden. Gleichzeitig erfüllen sie auch die Vorgaben der Aufsicht. Ein Beispiel: Mit einem Identity-and-Access-Management-System (IAM) lassen sich Benutzer und deren Zugriffsrechte steuern sowie regelmäßig kontrollieren.

Ein weiteres Tool ist eine Security-Information-and-Event-Management-Plattform, kurz SIEM. Hier lassen sich Log-Daten zentral und revisionssicher speichern und archivieren, so dass auch nachträgliche Auswertungen möglich sind. Damit gelingt es, Auffälligkeiten wie etwa unberechtigte Zugriffe frühzeitig aufzudecken.

Für versierte IT-Dienstleister gehört der Rechenzentrumsbetrieb an räumlich getrennten Standorten zum Selbstverständnis. So kommen sie dem Wunsch der Aufsicht beim Thema Business Continuity nach.

Mit Schwenktests oder Schwachstellen-Scans kümmern sie sich regelmäßig um die Sicherheit der sensiblen Kundendaten. Aber nicht nur bei Services profitieren Versicherungen vom Know-how der IT-Provider. So geben diese auch Hilfestellung bei der Ausrichtung des IT-Betriebes und ebnen den Weg in die Cloud. Denn nur eine regulationskonforme Lösung kann aus Sicht der Prüfer Bestand haben.

* Dr. Christian Thiel ist Generalbevollmächtigter bei Finanz Informatik Technologie Service (FI-TS). Er verantwortet seit 2015 das Produkt- und Innovations-Management sowie die Beratung und das technische Lösungsdesign. Zudem ist er Experte für aufsichtsrechtliche Anforderungen an die IT in der Finanz- und Versicherungsbranche.