

# Stellungnahme

## Novellierung des Rundschreibens Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

24. September 2021

Seite 1

Der Bitkom begrüßt, dass die BaFin das novellierte Rundschreiben zu den „Versicherungsaufsichtlichen Anforderungen an die IT“ (VAIT) zur Konsultation stellt. Im Zuge der digitalen Transformation der Versicherungsbranche kommen den VAIT eine immer größere Bedeutung zu. Die Novellierung ist daher in weiten Teilen gutzuheißen. Dennoch bedürfen einzelne Punkte einer näheren Betrachtung, zu welchen wir wie folgt Stellung nehmen möchten:

### 1 Anforderungen an die IT-Strategie (VAIT II.1)

Die vorgenommenen Anpassungen sehen wir als klarstellend und sinnvoll an. Der stärkere Fokus auf die Ziele der IT-Strategie führt bei Versicherungsunternehmen dazu, dass oftmals unklar ist, wie ausführlich solch hinreichend überprüfbare Ziele formuliert werden sollen. Ein deutlicher formulierter Grad der Detailtiefe würde zu einem geringeren Maß an Unsicherheit führen, was wir entsprechend als erstrebenswert ansehen. Ebenso würden konkretere Mindestinhalte zu mehr Sicherheit bei der Anwendung der VAIT führen.

Die in 1.2. (b) angeführten technischen Standards sollten auch ‚Business-Standards‘ beinhalten. Aufgrund der immer engeren Verzahnung von ‚IT‘ und ‚Business‘ ist die ehemals klassische Trennung nicht mehr zeitgemäß. Die zugrundeliegenden EIOPA-Leitlinien behandeln explizit die Abhängigkeit von Service-Providern und zwar im Allgemeinen (13 b) als auch – im Hinblick auf die Abhängigkeit zur Business Strategie – im Detail (13 a). Als aktuelles Beispiel wäre hier auch die Konsultation der EIOPA zum Themenkomplex ‚Open Insurance‘ zu nennen.

### 2 Anforderungen an die IT-Governance (VAIT II.2)

Das Kapitel zu den Anforderungen an die IT-Governance lässt eine konkrete Schwerpunktsetzung vermissen, sodass eine bewusste Strukturierung des Kapitels

Bitkom  
Bundesverband  
Informationswirtschaft,  
Telekommunikation  
und Neue Medien e.V.

Fabian Nadler  
Bereichsleiter Digital Insurance &  
InsurTech  
T +49 30 27576-164  
f.nadler@bitkom.org

Albrechtstraße 10  
10117 Berlin

Präsident  
Achim Berg

Hauptgeschäftsführer  
Dr. Bernhard Rohleder

## **Stellungnahme BaFin-Novellierung der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT)**

Seite 2|3

dann auch zu einer einfacheren Umsetzung führen würde. Auch ein deutlicher Verweis auf andere Kapitel der Verordnung wäre hilfreich.

### **3 Anforderungen an die operative Informationssicherheit (VAIT II.5)**

Dieses neue Kapitel weist lediglich eine knappe, schlagwortartige Aufzählung von Maßnahmen auf. Der Mehrwert des bloßen Verweises auf „gängige Standards“ ist daher als begrenzt einzuschätzen.

Die EIOPA-Leitlinien gehen unter den Punkten 42, 45 und 47 auch auf strategische und business-basierte Prozesse und Risiken beim operationalen Management ein. Diese zusätzliche Sicht findet sich in der jetzigen Form der VAIT Novellierung nicht einmal ansatzweise wieder. Dabei kann es durch diese Betrachtung zu veränderten und geschäftspolitisch anders priorisierten Aktivitäten und Maßnahmen kommen.

### **4 Anforderungen an das Identitäts- und Rechtemanagement (VAIT II.6)**

Das Kapitel umfasst einige sinnvolle und klarstellende Anpassungen. Die genannte Business Impact Analyse hat aber im Gegensatz zu den EIOPA-Leitlinien nur eine begrenzte Aussagekraft über die Berücksichtigung von Services und Service-Partnern, die auch außerhalb der Branche liegen können. Dem Kapitel liegt die implizite Annahme zugrunde, dass Prozesse nur innerhalb der Versicherungsbranche vorstattengehen. Dies ist aber im Hinblick auf die aktuellen Entwicklungen in dem Bereich als eher unrealistisch einzustufen.

### **5 Anforderungen an IT-Projekte und Anwendungsentwicklung (VAIT II.7)**

Das Kapitel spiegelt im Wesentlichen die relevanten Standards zu Konzeption und Durchführungen von IT-Projekten in verschiedenen Industrien, und verknüpft diese mit den spezifischeren weiteren Anforderungen der VAIT.

Lediglich bezüglich des sehr grundsätzlich formulierten Trennungsgebots von Produktionsumgebungen zu Entwicklungs-/Testumgebungen würden wir eine entweder

## Stellungnahme BaFin-Novellierung der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT)

Seite 3|3

differenziertere oder weniger finale Aussage anregen: Moderne Architekturen (insb. SCS und Microservice-Architekturen) und die vielgliedrige Wertschöpfungskette zu Prozessen und Daten zwischen unterschiedlichen Akteuren bedingen – nicht nur aber insbesondere – an den Schnittstellenfunktionalitäten (REST-APIs und andere) Tests in produktiven Szenarios. Gleiches gilt für Security-Tests, die sinnvollerweise regelmäßig Teil der Entwicklungstests sind, und die ebenfalls teilweise in den Produktivumgebungen stattfinden.

Das Trennungsgebot in der im Entwurf beschriebenen Form ist im Rahmen der heute genutzten Technologien und Architekturen unserer Ansicht nach in vielen Fällen obsolet.

### 6 Anforderungen an das IT-Notfallmanagement (VAIT II.10)

Das neue Kapitel zu den Anforderungen an das IT-Notfallmanagement überzeugt im Gegensatz zu anderen Kapiteln in den Augen des Bitkom durch eine gute Detailtiefe als auch Anwenderfreundlichkeit.

In 10.2. wird lediglich auf die Gefahr von Cyber-Angriffen von Systemen und Kommunikationsinfrastruktur hingewiesen, aber nicht auf die Business Service Funktionen, obwohl diese mitunter das größte Risiko für die Organisationen und deren Geschäftspartner darstellen.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.