Stellungnahme

des Gesamtverbandes der Deutschen Versicherungswirtschaft

zu dem Entwurf der BaFin

„Versicherungsaufsichtliche Anforderungen an die IT (VAIT)“ vom 15. März 2018

Konsultation 04-2018

Geschäftszeichen: VA 36-I 2802-2018/0001

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5452 / 5455
Fax: +49 30 2020-6452 / 6455

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39
ID-Nummer 6437280268-55

Ansprechpartner:
Patrik Maeyer
Leiter Betriebstechnik, Digitalisierung und IT

Christine Jansen
Betriebstechnik, Digitalisierung und IT

E-Mail: p.maeyer@gdv.de/
c.jansen@gdv.de

www.gdv.de

Zusammenfassung

Die IT-Sicherheit ist ein wesentlicher Grundpfeiler des Geschäftsmodells von Versicherungsunternehmen in Deutschland. Mit den Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) plant die BaFin, neue Vorgaben zu schaffen, die jedoch nicht zwingend die IT-Sicherheit erhöhen und lediglich weitere bürokratische Hemmnisse für die Unternehmen manifestieren.

Dies ist nicht zuletzt darauf zurückzuführen, dass neben den bereits existierenden **Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo)** ohne ersichtlichen Grund weitere aufsichtsbehördliche Vorgaben für einen speziellen Bereich innerhalb der Unternehmen geschaffen werden. Ein solches Vorgehen ist grundsätzlich abzulehnen. Denn es trägt zu einer Unübersichtlichkeit und Inkongruenz der aufsichtsbehördlichen Äußerungen zur Geschäftsorganisation von Versicherungsunternehmen bei.

Jedenfalls muss sowohl unter Wettbewerbs- als auch unter Kostenaspekten der zu **erwartende Aufwand für die Umsetzung der VAIT** in Unternehmen in einem angemessenen Verhältnis zum Aufsichtsziel stehen. IT-Sicherheitsanforderungen und damit in Zusammenhang stehende Pflichten gegenüber der BaFin dürfen nicht zu einer **Überforderung der Unternehmen** führen. Aus Sicht der deutschen Versicherungswirtschaft sind daher folgende Nachbesserungen in den VAIT notwendig:

- **Vermeidung von Doppelregulierung und redundanten Berichtspflichten** beispielsweise zum IT-Sicherheitsgesetz. Hierzu ist eine stärkere Verzahnung der Behörden und Vorschriften notwendig.
- **Konsequente Anwendung des Proportionalitätsprinzips** mit dem Ziel, den Verwaltungsaufwand für die Unternehmen mit nachweislich einfachem Risikoprofil gering zu halten. Die VAIT müssen flexibel umsetzbar sein und auch ausdrücklich die Nichtanwendung von einzelnen Anforderungen vorsehen.
- **Kritikalität, Wesentlichkeit und Versicherungsbezug** als Maßstab für die VAIT heranziehen. Es sollten nur Informationen erfasst werden, die maßgeblich für die Bewertung tatsächlicher IT-Risiken für die Versicherungswirtschaft sind.
- **Ressortteilige Arbeitsweise der Geschäftsleitung beibehalten.** Eine Einbindung der gesamten Geschäftsleitung bei allen IT-Fragen sehen wir als zu weitreichend an.
- **Praxisnahe Lösungen für Individuelle Datenverarbeitung (IDV)** ermöglichen. Nicht jede IDV-Anwendung stellt ein IT-Sicherheitsrisiko dar und sollte daher auch nicht als solches behandelt werden.
- **Vorschriften für IT-Ausgliederungen im Einklang mit Unternehmenspraxis und bestehenden Rechtsvorschriften gestalten**. Anforderungen an Ausgliederungen dürfen im Bereich der IT nicht weitreichender sein als gesetzlich vorgesehen.

Den Unternehmen sollte der notwendige Handlungsspielraum erhalten bleiben, ihre IT nach risiko- und geschäftsbezogenen Kriterien individuell passgenau zu organisieren.

1. Allgemeine Anmerkungen

Der Einsatz von Informationstechnik (IT) hat eine zentrale Bedeutung für Versicherungsunternehmen in Deutschland. Die Unternehmen sind sich dessen bewusst und arbeiten kontinuierlich an einer Optimierung ihrer IT-Systeme. Die IT-Sicherheit ist ein wesentlicher Grundpfeiler ihres Geschäftsmodells, da nur so die Datensicherheit der Kundendaten gewährleistet werden kann.

1.1. VAIT gehen weit über bestehende Regulierung hinaus

Die nunmehr geplanten Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) konkretisieren laut den Vorbemerkungen der BaFin lediglich die Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo). Daraus sollte folgen, dass die VAIT keine Anforderungen enthalten, die über bereits bestehende gesetzliche und aufsichtsbehördliche Festlegungen, insbesondere in den MaGo, hinausgehen. Allerdings werden mit den VAIT weitreichende und teilweise überschießende Anforderungen formuliert, für die sich keine Grundlage in den verbindlichen gesetzlichen Vorgaben finden.

Während die MaGo beispielsweise in Tz. 47 ff. die Dokumentation von schriftlichen Leitlinien erwarten, enthält der Konsultationsentwurf der VAIT eine Fülle von zusätzlichen Dokumentationsvorgaben – von der IT-Strategie mit Mindestinhalten (Tz. 4) über Regelungen zur IT-Aufbau- und IT-Ablauforganisation (Tz. 7), Arbeitsablaufbeschreibungen (Tz. 16), Sollmaßnahmenkatalog (Tz. 22), Statusberichte (Tz. 24, 32), schriftliche Informationssicherheitsleitlinie (Tz. 25), Informationssicherheitsrichtlinien (Tz. 26), Notfallkonzept Tz. 28), Benutzerberechtigungsmanagement (Tz. 33), Anwendungsdokumentation (Tz. 53), IDV-Richtlinie und zentrales Register (Tz. 57) und Datensicherungskonzept (Tz. 64). Dabei ist zu bedenken, dass sich Dokumentationsvorgaben stets an den Risiken und der Relevanz für das Unternehmen messen lassen müssen. Unternehmen müssen weiterhin entsprechende Gestaltungsspielräume haben.

Zusätzliche Überprüfungen und entsprechende interne oder externe Berichtsanforderungen sollten vermieden werden. Die IT bildet einen Bestandteil der Geschäftsorganisation, über die die Unternehmen schon heute sowohl regelmäßig intern (§ 23 Abs. 2 VAG, § 30 VAG) als auch an die Aufsichtsbehörden (im Rahmen des RSR) und an die Öffentlichkeit (im Rahmen des SFCR) berichten müssen. Ebenso werden die relevanten IT-Prozesse auch im Rahmen der jährlichen Jahresabschussprüfungen und der Prüfungen der Solvabilitätsübersichten gemäß § 35 Abs. 2 VAG durch

den Wirtschaftsprüfer überprüft. Risiken im Zusammenhang mit der IT sind als Bestandteil des operationellen Risikos (Tz. 161 MaGo) in den entsprechenden Risikoberichten (insbesondere ORSA-Bericht) erfasst. Wesentliche Schadenereignisse sind sowohl der Geschäftsleitung als auch unverzüglich der unabhängigen Risikocontrollingfunktion (URCF) zu berichten (Tz. 168 MaGo). Zusätzliche vierteljährliche Statusmeldungen (Tz. 24, 32), Störungsmeldungen (Tz. 61) oder sonstige Berichtsformate sind vor diesem Hintergrund nicht angemessen.

1.2. Doppelregulierung und redundante Berichtspflichten vermeiden

Gerade das Thema IT-Sicherheit ist bezüglich der behördlichen Zuständigkeit und gesetzlichen Vorgaben ganzheitlich zu betrachten, um Doppelregulierung und redundante Meldepflichten zu vermeiden. Nur so kann sowohl auf Behörden- als auch auf Unternehmensseite ein sinnvoller Ressourceneinsatz sichergestellt werden.

Nicht zuletzt durch das umfangreiche Regelwerk von Solvency II sehen sich die Unternehmen einer hohen Regulierungsdichte ausgesetzt. Zudem ist im Juli 2015 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheits-gesetz, IT-SiG) in Kraft getreten. Die betroffenen Unternehmen müssen eine Reihe von Pflichten erfüllen, wenn sie unter das IT-Sicherheitsgesetz fallen. Insgesamt haben Unternehmen damit regelmäßig mehrere europäische und nationale Regulierungsebenen zu beachten. Unterschiedliche Regelungen zum selben Sachverhalt stellen für Unternehmen ein Problem dar, insbesondere, wenn jede Behörde hierfür eine eigene Prüfung verlangt. Generell sollten Daten, die bei staatlichen Stellen bereits aufgrund einer verbindlichen regulatorischen Vorgabe erhoben werden, nicht ein zweites Mal angefordert werden.

Die VAIT nutzen an unterschiedlichen Stellen Begriffe, die in den MaGo nicht enthalten sind und teilweise aus unterschiedlichen IT-Standards entlehnt sind. Im Einzelnen sind Unklarheiten in der Interpretation der VAIT i.V.m. den MaGo und Widersprüche in den Begrifflichkeiten zu erkennen (vgl. Kommentare zum Informationsrisikomanagement, Berechtigungsmanagement, IT-Ausgliederungen und sonstigem Fremdbezug). Deshalb sollte auf Basis des finalen Rundschreiben-Textes eine inhaltliche und formale Konsistenzprüfung erfolgen. Zumindest sollten die Begrifflichkeiten der MaGo 1:1 in die VAIT übernommen werden.

1.3. Proportionalitätsprinzip in der Aufsichtspraxis stärken

Der Versicherungsmarkt in Deutschland zeichnet sich durch starke Heterogenität aus. Neben den großen, international tätigen Versicherungsgruppen gibt es zahlreiche kleine und mittelständische Unternehmen mit einfachem Geschäftsmodell, die häufig regional verankert sind. Das Ziel sollte es sein, den Verwaltungsaufwand für die Unternehmen mit nachweislich unterdurchschnittlichem Risikoprofil gering zu halten. Hierzu sollten keine neuen Vorgaben ohne nachweislichen Mehrwert für die Aufsicht und für Unternehmen eingeführt werden.

Die VAIT müssen nach dem gesetzlich zwingend vorgegebenen Proportionalitätsprinzip daher flexibel umsetzbar sein und auch die Nichtanwendung von einzelnen Anforderungen ermöglichen. Der Einschätzung, „wie" die Anforderungen der VAIT umgesetzt werden, muss eine Prüfung vorgeschaltet sein, „ob" diese Anforderungen für das Unternehmen aus Risikogesichtspunkten angemessen und notwendig sind. Denn die aufsichtsrechtlichen Anforderungen für Unternehmen können im Einzelfall so hoch sein, dass allein deren Nichtanwendung dem Proportionalitätsgrundsatz genügt. Dies gilt insbesondere für Unternehmen mit einfachem Risikoprofil. Als Beispiele sind zu nennen:

- Es kann sich die IT-Strategie als Bestandteil der Geschäfts- und Risikostrategie ergeben, ohne in einem separaten Dokument erneut ausführlich dokumentiert worden zu sein.

- Die Notwendigkeit und der Umfang etwaiger Richtlinien (etwa zur IT-Sicherheit oder IDV-Entwicklung) müssen stets die Betroffenheit der Unternehmen berücksichtigen. Sofern etwa der Einsatz von IDV-Anwendungen keine oder nur eine untergeordnete Rolle spielt und nicht für geschäftsrelevante Entscheidungen oder Ergebnisse (z. B. Solvency II) genutzt wird, sollte es möglich sein, auf die weitreichenden Anforderungen wie z. B. Dokumentation im Rahmen einer solchen Richtlinie zu verzichten.

- Der Entwurf der VAIT sieht vor, nicht nur bei Ausgliederungen, sondern bei jeder IT-Dienstleistung eine Risikoanalyse durchzuführen. Jede IT-Dienstleistung ist unter Berücksichtigung der Risikoanalyse zu steuern, permanent zu überwachen und ggf. anzupassen. Da dies in den Unternehmen zu einem erheblichen Mehraufwand führen würde, der nicht durch einen angemessenen Erkenntnisgewinn gerechtfertigt wird, sollte es möglich sein, auf die Risikoanalyse bei IT-Dienstleistungen verzichten zu können.

1.4. Kritikalität, Wesentlichkeit und Versicherungsbezug als Maßstab heranziehen

Wir teilen die Auffassung der BaFin, dass die Frage, welche konkreten Strukturen und Maßnahmen einem bestimmten Risikoprofil angemessen sind, nur im jeweiligen Kontext (unter Berücksichtigung u. a. der Kritikalität) beantwortet werden können. Allerdings bedarf es aus unserer Sicht einer weiteren Konkretisierung im Hinblick auf die „Wesentlichkeit“ und den „Versicherungsbezug“. Denn diese sind neben der Kritikalität maßgeblich für die Bewertung tatsächlicher IT-Risiken in den Unternehmen. Für IT-Systeme und Prozesse, die keinen wesentlichen Einfluss auf das Geschäft oder die Risikolage des Unternehmens haben, darf es keine Berichtspflichten geben.

1.5. Ressortteilige Arbeitsweise der Geschäftsleitung beibehalten

Die VAIT (Tz. 11) sehen vor, dass soweit sich die Anforderungen auf die Geschäftsleitung beziehen, immer die gesamte Geschäftsleitung gemeint ist. Diese kann der Konsultationsfassung zufolge ihre Verantwortung nicht delegieren, auch nicht auf einen oder mehrere Geschäftsleiter. Beispielsweise muss die Geschäftsleitung für die Umsetzung der IT-Strategie Sorge tragen. Aus Sicht der deutschen Versicherungswirtschaft ist diese Anforderung zu weitreichend und nicht praktikabel. Sie birgt hingegen die Gefahr einer Überlastung des Vorstandes. Die Beteiligung des IT-Vorstands sollte daher bei spezifischen IT-Fragen ausreichen. Dies entspräche der bisher praktizierten ressortbezogenen Arbeitsweise in den Vorständen. Auch in den MaGo ist ein entsprechender Grundsatz verankert. Die Einbindung der gesamten Geschäftsleitung sollte auf originäre Leitungsaufgaben beschränkt bleiben.

1.6. Vorschriften für IT-Ausgliederungen im Einklang mit Unternehmenspraxis und bestehenden Rechtsvorschriften gestalten

Besonders kritisch sehen wir die Anforderungen an Ausgliederungen. Gerade die Zusammenarbeit mit IT-Dienstleistern nimmt in Zeiten der Digitalisierung und Globalisierung stetig zu und ist für die effiziente Aufgabenerfüllung der Versicherungsunternehmen notwendig. Allerdings sind die im VAIT-Entwurf formulierten Anforderungen an Ausgliederungen zu detailliert und damit bürokratischer als notwendig. Darüber hinaus können aktive Überwachungs- und Kontrollrechte – anders als im Entwurf der VAIT gefordert – grundsätzlich nur bei dem primären Vertragspartner ausgeübt werden. Wir halten daher entsprechende Nachbesserungen im achten Modul der VAIT für zwingend erforderlich.

1.7. Übergangsfrist für die Umsetzung notwendig

Im Hinblick auf die notwendige Anpassung unternehmensinterner Abläufe und Prozesse ist es erforderlich, eine ausreichende Übergangsfrist für die Implementierung der Vorgaben der VAIT vorzusehen. Die umfassende Prüfung und möglicherweise daraus resultierende notwendige Anpassung von IT-Prozessen erfordert Zeit und nimmt erhebliche Ressourcen innerhalb der Unternehmen in Anspruch. Die deutsche Versicherungswirtschaft hält daher eine Übergangsfrist von mindestens 12 Monaten für erforderlich.

2. Anmerkungen zu den einzelnen Textziffern der Anforderungen

2.1. IT-Strategie

Tz. 1
Hinsichtlich der beschriebenen Aufgabe der Geschäftsleitung, eine IT-Strategie festzulegen, sollte der Zusatz „nachhaltige“ gestrichen werden. Gemäß den MaGo ist keine Nachhaltigkeit der Geschäftsstrategie gefordert, alle ergänzenden Strategien müssen konsistent dazu formuliert sein.

Tz. 2
Wir gehen davon aus, dass die IT-Strategie nicht zwingend in einem separaten Dokument neben der Geschäftsstrategie darzustellen ist. Die IT-Strategie sollte vielmehr als Bestandteil der Geschäftsstrategie angesehen werden. Sie sollte daher nur Mindestinhalte vorsehen, zu denen strategische Aussagen zur IT getroffen werden können.

2.2. IT-Governance

Tz. 9
Der Begriff „Informationsrisikomanagement“ sollte in der Aufzählung zur angemessenen Personalausstattung gestrichen werden, da das Informationsrisikomanagement im Sinne des 3. Moduls der VAIT keine personell vorzuhaltende (Schlüssel-)Funktion darstellt, sondern lediglich Methoden und Verfahren beschreibt.

2.3. Informationsrisikomanagement

Einzelne Risiken der Informationstechnologie können in Zusammenhang mit Risiken anderer Bereiche stehen, z. B. Personal-, Prozess- und Rechtsrisiken. Schon heute fließen IT-Risiken als Teil des operationellen Risikos und nicht als eigenständige Kategorie in die Risikosteuerungsprozesse der Unternehmen insgesamt ein. Mit dem Begriff „Informationsrisikomanagement“ sollte daher keinesfalls eine separate Risikodisziplin etabliert werden.

Tz. 18
Der Begriff „Restrisiken“ ist missverständlich und sollte gestrichen werden. Er impliziert, dass jegliche Risiken – also auch sehr unwahrscheinliche oder solche mit geringem Schadenpotenzial – aktiv gesteuert werden müssen. Dies widerspricht dem Grundgedanken von Solvency II, wonach vor allem wesentliche Risiken zu steuern sind. Zudem wäre der damit verbundene Aufwand in vielen Fällen völlig unverhältnismäßig zum Erkenntnisgewinn hinsichtlich der Risikolage des Unternehmens. Die Ergebnisse der Risikoanalyse in Bezug auf IT-Risiken sind daher lediglich im Rahmen der operationellen Risiken als Teil der operationellen Risiken des Unternehmens zu berücksichtigen.

2.4. Informationssicherheitsmanagement

Materiell wird in den VAIT die Stellung des Informationssicherheitsbeauftragten im Unternehmen konkretisiert und erweitert. Dieser soll künftig unabhängig von der operativen IT organisiert sein.

Tz. 28
Nach dem Konsultationsentwurf der VAIT soll der Informationssicherheitsbeauftragte angemessenen bei Projekten mit IT-Relevanz beteiligt werden. Je nach Einzelfall soll eine angemessene Beteiligung von der Information des Informationssicherheitsbeauftragten über das IT-Projekt bis hin zu seiner aktiven Mitwirkung daran reichen. Eine solch weitreichende Beteiligung des Informationssicherheitsbeauftragten erscheint uferlos, da grundsätzlich alle Projekte im heutigen Versicherungsgeschäft eine IT-Relevanz aufweisen. Stattdessen sollte der Informationssicherheitsbeauftragte nur bei wesentlich sicherheitsrelevanten IT-Projekten, die die Sicherheit der Daten und den Geschäftsbetrieb potenziell beeinträchtigen können, angemessen beteiligt werden.

Die Funktion des Informationssicherheitsbeauftragten sollte uneingeschränkt durch einen Geschäftsleiter wahrgenommen werden können.

Insbesondere kleine und mittlere Unternehmen haben oftmals keine wesentliche eigenbetriebene IT. Daher verbleiben bei diesen Unternehmen nur wenige Aufgaben im Zusammenhang mit dem Betrieb und der Weiterentwicklung der IT im eigenen Hause. Hierbei sollten risikomindernde organisatorische Maßnahmen als ausreichend angesehen werden, um Interessenkonflikten vorzubeugen. Soweit die anderen genannten Anforderungen zur Gewährleistung der Unabhängigkeit sichergestellt sind, sollte auch eine Ansiedlung der Funktion innerhalb einer Organisationsabteilung mit operativen IT-Aufgaben erfolgen können. Eine solche Lösung bietet im Hinblick auf die fachliche Qualifikation und informatorische Einbindung des Informationssicherheitsbeauftragten Vorteile im Vergleich zu einer abgekoppelten Stabsstelle.

Tz. 21

In der Teilziffer 21 der VAIT wird gefordert, dass die Methodik zur Ermittlung des Schutzbedarfs (insbesondere im Hinblick auf die Schutzziele „Integrität“, „Verfügbarkeit“, „Vertraulichkeit“ und „Authentizität“) die Konsistenz der resultierenden Schutzbedarfe nachvollziehbar sicherzustellen hat. Das Schutzziel Authentizität ist jedoch weder im BSI-Grundschutz noch in der ISO-Norm (IT-Schutzziele) verankert. Es sollte daher auch nicht in den VAIT gefordert werden. Authentizität kann allenfalls ein weiterer Faktor wie auch z. B. Zurechenbarkeit und Verlässlichkeit sein. Mit Blick auf eine konsequente Anwendung des Proportionalitätsprinzips gehen wir davon aus, dass eine Schutzbedarfsfeststellung für Unternehmen geringem Risikoprofil mit der Durchführung regelmäßiger Risikoanalysen abgedeckt ist.

Tz. 24 und 32

Die in den Teilziffern 24 und 32 geforderte vierteljährliche Berichterstattungspflicht sollte auf eine flexible regelmäßige Berichterstattungspflicht – kombiniert mit einer ad-hoc-Berichterstattung bei deutlichen Änderungen der Risikosituation – geändert werden. Die MaGo treffen selbst keine Aussage zum Turnus der Berichterstattung an die Geschäftsleitung zur Informationssicherheit. Als vergleichbare Anforderung kann jedoch der Maßstab der Berichterstattung der Compliance-Funktion, des zentralen Auslagerungsmanagements oder der Risikocontrolling-Funktion zum OpRisk-Reporting herangezogen werden, wo eine mindestens jährliche Berichterstattung an die Geschäftsleitung vorgesehen ist. Eine solche Regelung wäre für auch für das Informationsrisikomanagement risikoadäquat und ausreichend.

2.5. Benutzerberechtigungsmanagement

Berechtigungskonzepte legen im Rahmen des Benutzerberechtigungsmanagements den Umfang und die Nutzungsbedingungen der Berechtigungen für die IT-Systeme konsistent zum ermittelten Schutzbedarf sowie für alle von einem IT-System bereitgestellten Berechtigungen fest. Berechtigungskonzepte sollen sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt.

Tz. 34
In der Teilziffer 34 wird gefordert, dass nicht personalisierte Berechtigungen jederzeit und zweifelsfrei einer handelnden Person zuzuordnen sein müssen. Ist dies nicht möglich, sollte eine Zuordnung zu einer verantwortlichen Person möglich sein. In der Versicherungspraxis ist dies vor allem bei technischen User-Accounts wichtig. Der Passus sollte dementsprechend ergänzt werden.

Tz. 40
Grundsätzlich halten wir eine am Schutzbedarf ausgerichtete Protokollierung für sachgerecht. Die Anforderung, Prozesse zur Protokollierung einzurichten, die eine Überprüfung von IT-Berechtigungen hinsichtlich des „vorgesehenem Einsatzes“ sicherstellen, ist in der Praxis jedoch nicht umsetzbar. Eine Protokollierung kann lediglich einen möglichen Missbrauch dokumentieren. Es sollte deutlich gemacht werden, dass Unternehmen nach Maßgabe des Schutzbedarfs und der Soll-Anforderungen Prozesse zur Protokollierung einzurichten haben, die sicherstellen, dass die IT-Berechtigungen nur wie vorgesehen eingesetzt werden.

2.6. IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen)

Die Dokumentation der Anwendungsentwicklung muss auch agilen Vorgehensmodellen, die in der Praxis immer größere Bedeutung erlangen, Rechnung tragen.

Tz. 42
Der Begriff „IT-Projekte“ sollte konkretisiert werden. Es sollte klargestellt werden, ob darunter nur eigenständige Projekte, die nur auf IT-Anwendungsentwicklungen abzielen, verstanden werden oder auch andere Projekte, die Anpassungen in der IT oder Einführungen von Software zur Folge haben, dazu zählen.

Die zwingende Einbindung der unabhängigen Risikokontroll-, Compliance- und Versicherungsmathematischen Funktion ist nicht notwendig. Die Einbindung der Schlüsselfunktionen bei wesentlichen Veränderungen in den IT-Systemen sollte dahingehend eingeschränkt werden, dass eine Einbindung unter Risikoaspekten und nur dann zwingend erfolgen muss, wenn die Aufgabenbereiche der jeweiligen Funktion durch die Veränderungen betroffen sind. Beispielsweise ist eine Beteiligung der Versicherungsmathematischen Funktion bei allen wesentlichen Veränderungen nicht zielführend und führt zu unnötig komplexen Prozessen.

Tz. 47
Wesentliche IT-Projekte und IT-Projektrisiken sind gemäß der Teilziffer 47 der VAIT der Geschäftsleitung regelmäßig und anlassbezogen zu berichten. Sofern ein Vorstandsmitglied in einem entsprechenden Lenkungsausschuss vertreten ist, ist dies in der Regel darstellbar.
Allerdings kommt es in der Unternehmenspraxis häufig vor, dass die Überwachungsaufgabe an einen leitenden Angestellten delegiert wird. Aus unserer Sicht sollte es genügen, die Geschäftsleitung als Eskalationsinstanz vorzusehen.

Tz. 53
Die VAIT sehen vor, dass sowohl die von Dritten für das Unternehmen entwickelte als auch die im Unternehmen selbst entwickelte Anwendung übersichtlich und für sachkundige Dritte nachvollziehbar zu dokumentieren sind. Aus unserer Sicht sollten lediglich die von den Fachbereichen selbst entwickelten Anwendungen entsprechend der Kritikalität der unterstützten Geschäftsprozesse und der Bedeutung der Anwendungen für diese Prozesse dokumentiert werden.

Tz. 54
Bei den Anforderungen an die Testverfahren ist nach dem Grundsatz der Proportionalität abhängig von Art, Einsatzzweck, Komplexität und Schutzbedarf der Anwendung zu differenzieren. Insbesondere trifft dies auf Anwendungen zu, für welche die einzelnen Unternehmen vereinfachte Tests sowie Programm- und Einsatzfreigabeverfahren durchführen können. Ein Test der Systemleistung unter verschiedenen Stressbelastungsszenarien ist nicht bei jeder Anwendung (einschl. IDV) notwendig.

Tz. 56 und 57
Zur Bestimmung von IDV-Anwendungen gehen wir davon aus, dass z. B. Excel-Spreadsheets o. ä. Anwendungen zur einmaligen und gelegentlichen Nutzung, nicht unter die Anforderungen der Teilziffern 56 und 57 fallen.

Tz. 57
Der Entwurf der VAIT sieht in der Teilziffer 57 die zwingende Führung eines Registers zur Identifizierung aller von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen, zur Dokumentation, zu den Programmierrichtlinien und zur Methodik des Testens dieser Anwendungen, zur Schutzbedarfsfeststellung und zum Rezertifizierungsprozess vor. Dies stellt aus unserer Sicht einen unverhältnismäßigen bürokratischen Aufwand dar, der nicht durch einen angemessenen Erkenntnisgewinn gerechtfertigt wird. Die entsprechende Anforderung sollte daher gestrichen werden.

2.7. IT-Betrieb (inkl. Datensicherung)

Bei Unternehmen mit ausgegliedertem IT-Betrieb erfolgt die Erfüllung der Anforderungen überwiegend durch die IT-Dienstleister auf Basis von Verträgen und zugehörigen Service-Level-Agreements (SLA).

Tz. 59
Wir bitten um Klarstellung, dass Bestandsangaben auch in mehreren Tools verwaltet werden können und nicht ein zentrales Inventartool notwendig ist, was einen mehrfachen Pflegeaufwand mit sich bringen würde.

2.8. Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen

Verschärfend zu den gesetzlichen Vorgaben hat die BaFin in dem Entwurf des VAIT-Rundschreibens (Teilziffern 65-70) weitere Anforderungen formuliert. Beispielsweise muss nach den MaGo eine Risikoanalyse, die jede Ausgliederung erfordert, nur erneut durchgeführt werden, sofern sich wesentliche Änderungen des Risikoprofils in Bezug auf den Ausgliederungssachverhalt ergeben. Hingegen fordern die VAIT in Teilziffer 69 eine regelmäßige Überprüfung. Es sollte daher für das 8. Modul klargestellt werden, dass für die Zuordnung bzw. Auslegung der Anforderungen die Bestimmungen der MaGo gelten, soweit das jeweilige Versicherungsunternehmen den Vorgaben der MaGo unterliegt.

Insbesondere die zwingende Vorlage des Ausgliederungsvertrags sowie der Verträge für sämtliche Subdelegationen sehen wir als unverhältnismäßiges Hemmnis an. Bei großen Versicherungsunternehmen kann sich die Zahl der Ausgliederungen und Subdelegationen auf mehrere Tausend belaufen. Hier kann es nach unserer Überzeugung nicht sinnvoll sein, diese bis in die letzte Ebene zu erfassen.

Da gerade für IT-Ausgliederungen in zahlreichen Fällen zugleich eine datenschutzrechtliche Prüfung stattfindet, bei der ebenfalls die technisch-organisatorischen Maßnahmen der Daten- und IT-Sicherheit eine Rolle spielen, sollte hier ein Gleichklang erreicht werden, statt eine zusätzliche und über die bestehenden Verpflichtungen hinausgehende Regulatorik einzuführen.

Das Prinzip, wonach der jeweilige Auftraggeber für die Einhaltung der rechtlichen Vorgaben im Hinblick auf die Sicherheit der Datenverarbeitung verantwortlich ist, darf nicht konterkariert werden. Die Verantwortlichkeit der ausgliedernden Stelle durch die Auswahl eines zuverlässigen Dienstleisters beinhaltet auch, dass der Auftraggeber sicher sein kann, dass auch bei Inanspruchnahme von Dienstleistern seitens des Auftragnehmers dieser die notwendige und vertraglich vereinbarte Sorgfalt walten lässt.

Dieses bewährte Prinzip wird aus unserer Sicht beispielsweise im 8. Modul unterlaufen, da es impliziert, dass der Auftraggeber bei IT-Ausgliederungen auch die Subunternehmer seines Dienstleisters zu verantworten hätte. In diesen Fällen der Subdelegation ist es für das ausgliedernde Versicherungsunternehmen in vielen Fällen nur über den Dienstleister möglich, die Subdienstleister zu kontrollieren. Es sollte daher in den VAIT klargestellt werden, dass aktive Überwachungs- und Kontrollrechte nur bei dem primären Vertragspartner ausgeübt werden müssen. Primäre Vertragspartner haben demnach gegenüber dem ausgliedernden Unternehmen aufzuzeigen, wie sie ihre Verantwortung bei Subunternehmern umsetzen. Dabei gehen wir davon aus, dass regelmäßig Nachweise durch Zertifikate (ISO27001, BSI-Grundschutz) und Auditberichte (TÜV etc.) als Wahrnehmung der Kontrollrechte ausreichen.

Überzogene Regelungen bei Sub-Delegationen können u. a. die Cloud-Nutzung für Versicherungsunternehmen verhindern bzw. erheblich erschweren. Dies führt zu massiven Wettbewerbsnachteilen im internationalen Umfeld und im Verhältnis zu anderen Branchen. Hinzuweisen ist insofern auch auf den FinTech-Aktionsplan der Europäischen Kommission, der gerade darauf abzielt, technologiegestützte Innovationen im Finanzsektor zu implementieren. Marktgängige Innovationen können jedoch nach den geplanten Vorgaben der VAIT im schlimmsten Fall nicht eingesetzt werden. Überwachungs- und Kontrollrechte bei Subunternehmern sind im geforderten Maß in vielen Fällen praktisch nicht durchsetzbar.

2.9. Isolierter Bezug von Hard- und/oder Software

Es sollte in der Teilziffer 70 klargestellt werden, dass hierunter nicht Standardverträge zum Bezug von Software und Hardware fallen. Ein isolierter Bezug ist nicht vom Ausgliederungsbegriff des § 7 Nr. 2 VAG erfasst, da keine Dienstleistung in Anspruch genommen wird. Eine Risikobewertung sollte daher nur anlassbezogen, allenfalls bei gesetzlichen Änderungen, wiederholt werden müssen. Eine regelmäßige Risikobewertung ohne konkreten Anlass ist nicht erforderlich.

Berlin, den 19. April 2018