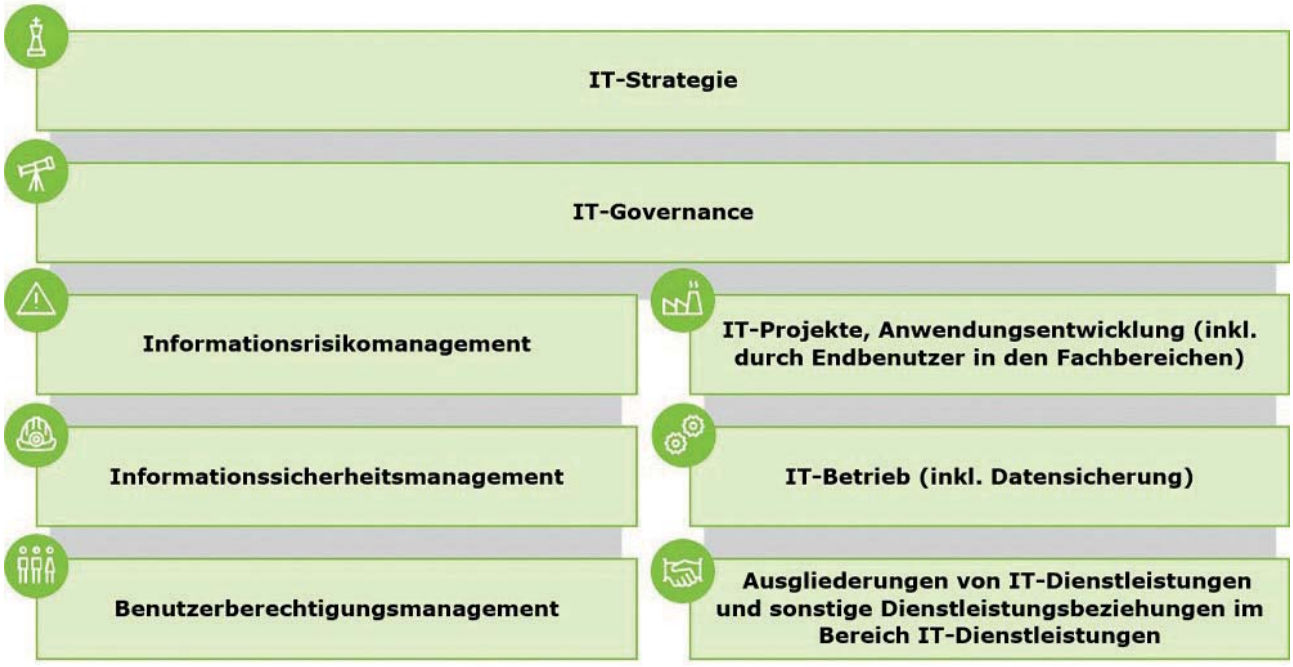
# Nächste Liste abarbeiten

Zu den bestehenden Anforderungen an die IT-Sicherheit der Versicherer ist die VAIT-Liste hinzugekommen. Steht nun der zu erwartende Aufwand bei der Umsetzung in einem angemessenen Verhältnis zum Aufsichtsziel der Bafin?

*Von Alexander Thoma und Philipp Widemann*

Mit dem am 13.03.2018 durch die Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) veröffentlichten Rundschreiben zu den Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) erfolgt die Auslegung der Vorschriften über die Geschäftsorganisation im Gesetz über die Beaufsichtigung der Versicherungsunternehmen (§ 23 ff. VAG) durch die BaFin. Die VAIT stellen eine Konkretisierung bzw. Auslegung bereits bestehender Vorschriften aus dem VAG bzw. aus den ebenfalls von der BaFin Anfang 2017 veröffentlichen Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) hinsichtlich der IT dar. Erfahrungen aus den bereits Ende 2017 veröffentlichten Bankaufsichtlichen Anforderungen an die IT (BAIT) zeigen, dass die konkretisierten Anforderungen der Bafin die Unternehmen durchaus vor „neue" Herausforderungen stellen. Da die Bafin nach Verabschiedung der VAIT (Mitte 2018) keine Übergangsfristen erlauben wird, müssen die Versicherungsunternehmen ihre IT-Organisation hinsichtlich der Anforderungen aus den VAIT auf den Prüfstand stellen und wenn nötig Maßnahmen ergreifen, um die gesetzten Erwartungen der Aufsicht zu erfüllen.Die Versicherungsaufsichtlichen Anforderungen an die IT enthalten Vorgaben zu den acht in der Grafik dargestellten Bereichen.

Wie bereits in den MaGo auf Basis des § 296 Abs. 1 VAG gefordert, haben sich die in den VAIT geforderten Anforderungen an dem unternehmensindividuellen Risikoprofil zu orientieren. Dieses Proportionalitätsprinzip zieht sich durch




**GDV warnt vor Überregulierung:** Die VAIT bestehen aus acht Themenblöcken mit insgesamt 70 Einzelanforderungen.

FOTO 1: © DELOITTE

alle acht Module und trägt dem sehr heterogenen Versicherungsmarkt in Deutschland Rechnung. Insbesondere die umfangreichen Dokumentationsanforderungen in den VAIT können durch das Proportionalitätsprinzip entsprechend gemildert werden.

Die VAIT fordern die Formulierung, Umsetzung und regelmäßige Überprüfung einer *IT-Strategie* in Abhängigkeit des Risikoprofils des Unternehmens. Gegenüber anderen einschlägigen Regelungen – wie beispielsweise der Stellungnahme zur Rechnungslegung des Fachausschusses für IT des IDW (IDW RS FAIT) oder den BSI-Standards schreiben die VAIT hier konkrete Mindestinhalte der IT-Strategie vor (siehe Rz. 2). Die bereits in der MaGo geforderte Abstimmung der Unternehmensstrategie mit dem Aufsichtsorgan wird in den VAIT auch auf die IT-Strategie bezogen und Änderungen der IT-Strategie sind im Unternehmen angemessen zu kommunizieren. Als Bestandteil der Geschäftsstrategie würde die IT-Strategie gemäß MaGo diese Anforderung nach Kommunikation mit dem Aufsichtsorgan erfüllen.

Die *IT-Governance* umfasst Regelungen zur IT-Aufbau- und IT-Ablauforganisation sowie Anforderungen an die IT-Systeme und die zugehörigen IT-Prozesse. Bei der Ausgestaltung der IT-Aufbau- und IT-Ablauforganisation sind Interessenskonflikte sowie durch Abwesenheit oder Ausscheiden von Mitarbeiter bedingte Störungen im Betriebsablauf vorzubeugen. Diese Anforderungen adressieren z.B. das der BaFin bekannte – und auch in der Projektpraxis von Deloitte immer wieder festgestellte Risiko bestehender Kopfmonopole in Bezug auf die Altsysteme der Versicherer. Erstmalig gefordert ist in den VAIT die Festlegung von qualitativen und quantitativen Kriterien zur Steuerung der für Betrieb und Weiterentwicklung der IT-Systeme zuständigen Bereiche (siehe Rz. 13), welche die IT in die Rolle eines internen Service-Dienstleisters rückt und ggf. die Definition von internen Service Level Agreements erforderlich macht.

Die Bereiche des *Informationsrisiko- und Informationssicherheitsmanagements* umfassen die Einrichtung eines Informationsrisikomanagementsystems zur Erreichung der in den BSI-Standards geforderten Informationssicherheit. Im Fokus des Informationsrisikomanagements und der zugehörigen Prozesse steht die Durchführung einer Risikoanalyse auf Basis der IT-Risikokriterien des BSI, deren Ergebnisse jährlich gegenüber der Geschäftsleitung zu kommunizieren sind. Die in den BSI definierten Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität) werden in den VAIT ebenfalls zu Grunde gelegt. Die Methodik zur Ermittlung dieser Schutzbedarfskategorien muss nachvollziehbar sein und konsistent angewendet werden. Ein neuer Sollmaßnahmenkatalog hat die unternehmensindividuellen Anforderungen zur Umsetzung der Schutzziele zu dokumentieren. Die Erstellung eines Sollmaßnahmenkatalogs ist eine von mehreren Dokumentationsanforderungen, die zu unerwünschten Aufwänden bei den Versicherern führen könnte.

Erstmalig gefordert wird der Überblick über Bestandteile, Abhängigkeiten und Schnittstellen des Informationsverbundes (Gesamtheit der an der Informationsverarbeitung beteiligten infrastrukturellen, organisatorischen, personellen und technischen Objekte) im Unternehmen (siehe Rz. 20), der auch die von den Fachbereichen entwickelten Anwendungen der individuellen Datenverarbeitung (IDV) miteinschließt. Die Vorgaben der VAIT bezüglich des Informationsmanagements basieren grundsätzlich auf den in den BSI-Standard bereits definierten Vorgaben zur Informationssicherheitsleitlinie, in der Ziele und Maßnahmen der Informationssicherheit definiert werden sowie der Rolle des Informationssicherheitsbeauftragten, welcher für die Umsetzung der Informationssicherheit verantwortlich ist. Auch im Bereich Informationssicherheitsmanagement werden weitere Dokumentationsanforderungen gestellt: auf Basis der Informationssicherheitsleitlinie sind Informationssicherheitsrichtlinien, sowie Informationssicherheitsprozesse zu definieren (siehe Rz. 27). Welche Inhalte sowie welchen Umfang die Dokumente haben müssen bleibt offen. Eine konsistente Orientierung am Risikoprofil wird auch hier den Maßstab bilden.

**VIEL DEFINIERT, WENIG PRAXISORIENTIERT**

Im Rahmen des *Berechtigungsmanagements* fordern die VAIT eine Ausgestaltung der den Benutzern eingeräumten Berechtigungen gemäß organisatorischer und fachlicher Vorgaben des Unternehmens durch Berechtigungskonzepte. Bestehende Vorgaben zum Identitäts- und Berechtigungsmanagement aus FAIT und den BSI-Standards werden durch die VAIT konkretisiert: das Berechtigungsmanagement hat nunmehr unter Einbezug des ermittelten Schutzbedarfs der jeweiligen IT-Systeme zu erfolgen (siehe Rz. 34). Präzisiert werden insbesondere die Vorgaben der FAIT zu den Teilprozessen des Berechtigungsmanagements Einrichtung, Änderung, Deaktivierung und Löschung von Berechtigungen. Im Rahmen der Rezertifizierung werden außerdem Vorgaben zum berechtigungstypenabhängigen Intervall der Kontrolle der vergebenen Berechtigungen definiert (siehe Rz. 38). Nicht personalisierte Berechtigungen oder technische Nutzer müssen zukünftig einer verantwortlichen natürlichen Person zuzuordnen sein. Hierdurch wird die bestehende IT-Sicherheitsanforderung Authentizität an alle IT-Systeme gestellt. Eine Überwachung der Verwendung von Berechtigungen, insbesondere für weitreichende oder privilegierte Benutzer wird nun explizit gefordert.

Im Bereich *IT-Projekte und Anwendungsentwicklung* der VAIT sind die regulatorischen Anforderungen im Rahmen

der Durchführung von wesentlichen Änderungen in den IT-Systemen eines Unternehmens geregelt, die in Form von IT-Projekten geplant und durchgeführt werden. Zum Anwendungsentwicklungsprozess selbst werden die in den FAIT genannten Anforderungen zur Einrichtung von IT-Systemen hinsichtlich des Testens der IT-Anwendung und der Dokumentation des Anwendungsentwicklungsprozesses präzisiert. Ein Versicherer muss erkennen können, ob eine Anwendung versehentlich geändert oder absichtlich manipuliert wurde (siehe Rz. 52).

Um diese Anforderung zu erfüllen, sollten die Versicherer ihre Kontrollen im Change- und Release-Managementprozess, sowie im Deployment auf den Prüfstand stellen. Für den Anwendungsentwicklungsprozess empfehlen die VAIT weiterhin konkrete Maßnahmen, wie z.B. die Einhaltung von Programmierrichtlinien zur Gewährleistung des Schutzbedarfs der jeweiligen IT-Anwendung, die auch für vom Fachbereich entwickelte IDV-Anwendungen gelten. Darüber hinaus müssen Versicherer Inhalte aus dem Berechtigungsmanagement und der Anwendungsentwicklung für IDV-Anwendungen in einer eigenen IDV-Richtlinie festlegen sowie ein zentrales Register der IDV-Anwendungen im Unternehmen pflegen. Die Umsetzung von IT-Projekten setzt eine Auswirkungsanalyse der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität voraus, bei der auch die Schlüsselfunktionen (unabhängiges Risikocontrolling, Compliance und versicherungsmathematische Funktion) einzubeziehen sind (siehe Rz. 42).

Der vorgeschriebene Einbezug von Schlüsselfunktionen erscheint sehr weitgehend und sicherlich aufwändig für die Unternehmen. Für die Steuerung einzelner IT-Projekte sind Vorgehensmodelle und zur projektübergreifenden Steuerung von Risiken wie z.B. Abhängigkeiten der Projekte untereinander eine Portfoliosicht einzurichten und zu überwachen (Portfoliomanagement).

**„Durch die neuen Anforderungen der VAIT rückt die IT immer mehr in die Rolle eines internen Servicedienstleisters mit festgelegten Service Level."**

Der Bereich *IT-Betrieb* hat die Anforderungen aus IT-Strategie und IT-Governance sowohl im Regelbetrieb als auch im Notbetrieb umzusetzen. Im Vergleich zu den Vorgaben der FAIT enthalten die VAIT eine Konkretisierung der Mindestinhalte, die im Rahmen der Inventarisierung der einzelnen IT-Systeme dokumentiert werden müssen (siehe Rz. 59). Änderungen an IT-Systemen sind in einem geregelten Changemanagement-Prozess zu beantragen, risikoorientiert zu bewerten und entsprechend zu priorisieren. Die VAIT definieren mit der Durchführung von Risikoanalysen, z.B. in Bezug auf die bestehenden Systeme, und Tests von Änderung, z.B. hinsichtlich möglicher Inkompatibilitäten, zusätzliche Kontrollanforderungen zur sicheren Umsetzung von IT-Änderungen. Darüber hinaus enthalten die VAIT Vorgaben zum Incident-Management wie z.B. die risikoorientierte Prio-

## VAIT IM VERGLEICH ZU DEN BANKENAUFSICHTLICHEN ANFORDERUNGEN (BAIT)

Die VAIT bündeln 70 Einzelanforderungen in den bereits beschriebenen acht Modulen und lehnen sich bei deren Strukturierung an die BAIT der Kreditinstitute an. Die VAIT stellen jedoch gegenüber den BAIT konkretere Anforderungen an die IT, da die übergeordnete Regulierung, v.a. die MaGo, im Vergleich zur MaRisk nur einen geringen Detaillierungsgrad zu IT-spezifischen Anforderungen aufweist. Gegenüber den BAIT enthalten die VAIT beispielsweise wesentlich konkretere Anforderungen in Bezug auf die Orientierung von IT-Governance am Risikoprofil des Unternehmens sowie hinsichtlich des Begriffs Informationsrisikomanagement. Jedoch bedeuten die konkreter formulierten Anforderungen nicht eine Verschärfung von Anforderungen für Versicherungen. Der deutlichste Unterschied ergibt sich für Versicherungen im Hinblick auf den Einbezug von IDV-Anwendungen in den Gültigkeitsbereich der VAIT. Außerdem ist ein breiterer Rahmen hinsichtlich Ausgliederungen, bspw. bei Unterstützungsleistungen im Bereich Softwareentwicklung festzustellen.

Im Wesentlichen stimmen die Inhalte der VAIT und der BAIT überein, die VAIT enthält lediglich zusätzliche Begriffsdefinitionen und ergänzende Anforderungen zu den einzelnen Themenfeldern, die als Konkretisierung der bestehenden Anforderungen dienen.

risierung oder ein prozessuales Vorgehen zur Ermittlung von Störungskorrelationen (siehe Rz. 63) sowie Vorgaben zur Datensicherung und Datenwiederherstellbarkeit, die zukünftig in einem Datensicherungskonzept geregelt werden müssen (siehe Rz. 64).

Die Anforderungen zu *Ausgliederung von IT-Leistungen* in den VAIT sind überwiegend bereits aus der MaGO und dem VAG bekannt. Der Geltungsbereich der Anforderungen erstreckt sich allerdings von der Ausgliederung von IT-Dienstleistungen bis hin zu kleinen Unterstützungsleistungen im Bereich Softwareentwicklung und v.a. auch auf Cloud-Dienstleistungen. Grundsätzlich muss vor Ausgliederung eine Risikoanalyse der mit der Ausgliederung verbundenen Risiken erfolgen. Die Risikoanalyse muss dabei regelmäßig in das Management der operationellen Risiken und damit in das Interne Kontroll-System der Versicherer eingebunden werden. Neu bzw. konkretisiert ist auch die Erfordernis ggf. Vertragsinhalte auf Basis der Ergebnisse der Risikoanalyse anzupassen.

**AUFZEIGEN, WER EIGENTÜMER WELCHER DATEN IST**

Die wesentlichen Herausforderungen, vor die die Versicherer bei der Umsetzung der VAIT gestellt werden, liegen vor allem im Informationsmanagement, dem sog. Enterprise Information Management, der Entwicklung und dem Betrieb von individueller Datenverarbeitung sowie in gestiegenen Anforderungen an die Dokumentation. Außerdem wird zunehmend prozessuale Transparenz gefordert, beispielsweise in der Anwendungsentwicklung und im Berechtigungsmanagement. Die mehrfach in den VAIT geforderte Vermeidung von Interessenskonflikten innerhalb der IT-Aufbau- und IT-Ablauforganisation sowie die geforderte Transparenz der Bestandteile des Informationsverbundes machen die Einführung von Data Governance unverzichtbar. Es muss klar sein, wer Eigentümer welcher Daten ist und welche Schutzbedarfsanforderungen für diese Informationen gelten. Die Unternehmen haben vollständige Transparenz der am Informationsverbund beteiligten Prozesse, Schnittstellen und Systeme herzustellen und müssen sich somit in die Lage versetzen, die bestehenden Abhängigkeiten zu erkennen und nachzuhalten. Nur dann kann auch nachhaltig Informationssicherheit gewährleistet werden.

Die bereits in den BSI-Standards definierten Schutzziele werden von den VAIT aufgegriffen und finden sich im Zuge einer starken Orientierung an den Schutzbedarfskategorien nun auch im Berechtigungsmanagement, der Anwendungsentwicklung und dem IT-Betrieb durch zusätzliche Anforderungen wie die Erstellung des Sollmaßnahmenkatalogs oder der Neuausrichtung der Berechtigungskonzepte wieder. Dieser Paradigmenwechsel weg von einer Funktionsorientierung wirkt sich auf Prozesse, Systeme und Datenflüsse aus.

Die Anforderungen zur Entwicklung und dem Betrieb der vom Fachbereich entwickelten Anwendungen, der IDV, stellen eine große Herausforderung für die Versicherer dar. Oft gibt es keinen zentralen Überblick und keine zentrale Steuerung der IDV-Anwendungen im Unternehmen, was die Erstellung des zentralen IDV-Registers und die in einer separaten IDV-Richtlinie zu regelnden Vorgaben zu Dokumentation, Schutzbedarfsfeststellung und Rezertifizierung zusätzlich erschwert. Die bereits in den MaGo geforderte Risikoanalyse muss in das Risikomanagement und das interne Kontrollsystem der Versicherer integriert werden. Unter anderem bei der Ausgliederung von IT-Leistungen und dem IT-Anwendungsentwicklungsprozess sind vorab Risikoanalysen durchzuführen, die im operationellen Risikomanagement berücksichtigt werden müssen. Diese Anpassung bzw. Erweiterung im Risikomanagement sollte methodisch keine größeren Schwierigkeiten bereiten, erhöht aber den operativen Aufwand im Auslagerungsprozess.

Themenübergreifend konkretisieren die VAIT Mindestinhalte und -anforderungen zu Berechtigungskonzepten sowie zur Dokumentation des Anwendungsentwicklungsprozesses und des IT-Betriebs, die mit einem erheblichen Dokumentationsaufwand verbunden sein werden. Herausfordernd für die Versicherer kann auch die geänderte Rolle der für Betrieb und Entwicklung der IT-Systeme zuständigen Bereiche sein. Durch die neuen Anforderungen der VAIT zur Steuerung und Überwachung dieser Bereiche sowie Anforderungen an den Umgang mit IT-Projekten und IT-Porfolios rückt die IT immer mehr in die Rolle eines internen Servicedienstleisters mit festgelegten Service Levels. So mancher IT-Bereich bei Versicherungsunternehmen wird jedoch noch nicht konsequent als Servicedienstleister gesteuert.

Fazit: Die in den VAIT gestellten Anforderungen an die Transparenz der IT, gesteigerte Dokumentationsanforderungen und Kontrollmaßnahmen in der IT-Umgebung stellen viele Versicherungsunternehmen vor eine große Herausforderung. Da für die Umsetzung der VAIT keine Übergangsfristen zu erwarten sind, ist es für die Versicherer empfehlenswert umgehend zu handeln und ihre IT entsprechend auf den Prüfstand zu stellen.


**Alexander Thoma**, Director im Risk Advisory. **Philipp Widemann**, Senior Manager im Risk Advisory, beide Deloitte.