Dr. Jan Hendrik Sohl / Michael Kötting

Versicherungsaufsichtliche Anforderungen an die IT: Einordnung und Umsetzungshinweise

Konkretisierung bisheriger Regelungen

Der Einsatz von Informationstechnologie nimmt in der Versicherungswirtschaft seit jeher einen hohen Stellenwert ein. Diese große Bedeutung würdigt nun auch die BaFin, indem sie im November 2017 einen ersten Entwurf der versicherungsaufsichtlichen Anforderungen an die IT (VAIT) veröffentlicht hat. Die VAIT stellen dabei eine sinnvolle Konkretisierung und Ergänzung bisheriger Regelungen dar, wie insbesondere der Anfang 2017 veröffentlichten Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo). So geht die aktuelle Fassung der MaGo unter dem Aspekt des Risikomanagements zwar explizit auf IT-Risiken ein, verzichtet jedoch auf weiterführende Details und Umsetzungshinweise. Diese Lücke möchte die BaFin nun mit der Verabschiedung der finalen Version der VAIT schließen. Die finale Version ist dabei Mitte 2018 zu erwarten.

Die VAIT legen die aus dem Versicherungsaufsichtsgesetz (VAG) und den MaGo resultierenden Anforderungen an die Geschäftsorganisation eines Versicherers verbindlich aus und gewährleisten auf diesem Wege eine konsistente Anwendung innerhalb der Versicherungswirtschaft. Bei den Anforderungen der VAIT bedient sich die BaFin eines flexiblen und praxisnahen Rahmens. So zielen vor allem die Anforderungen hinsichtlich des Managements der IT-Ressourcen, des Informationsrisikomanagements und des Informationssicherheitsmanagements auf gängige Standards ab.

Die BaFin betont dabei jedoch, dass die Anforderungen der VAIT nicht grundsätzlich abschließender Natur sind, sondern dass die Unternehmen im Rahmen der Ausgestaltung ihrer IT-Systeme und der dazugehörigen IT-Prozesse stets auf den Einsatz aktueller Standards zu achten haben. Exemplarisch können hier die IT-Grundschutzkataloge des BSI, der internationale Sicherheitsstandard ISO/IEC 2700X oder auch das IT-Governance-Framework COBIT genannt werden.

Wesentliche Anforderungen der VAIT

Die Inhalte der VAIT sind in acht übergeordnete Themenfelder mit insgesamt 68 Ziffern gegliedert (siehe Abbildung 1). Während einzelne Anforderungen bereits heute zum gängigen Standard in der Versicherungswirtschaft zählen, sind andere Anforderungen zum heutigen Zeitpunkt in den wenigsten Häusern zu finden. Im Rahmen der Umsetzung sollte demnach jedes Unternehmen sorgfältig prüfen, inwieweit bereits Konformität zu den einzelnen VAIT-Anforderungen besteht. Die wesentlichen Inhalte der VAIT finden sich nachfolgend skizziert.

Abbildung 1

1) IT-Strategie

Das Themenfeld IT-Strategie verlangt von den Unternehmen im Wesentlichen das Vorhandensein einer zur Geschäftsstrategie konsistenten und nachhaltigen IT-Strategie, die klare Ziele sowie Maßnahmen zur Erreichung dieser Ziele enthalten sollte. Zur Wahrung der Aktualität ist durch die Geschäftsleitung eine regelmäßige Überprüfung samt erforderlichen Anpassungen anzuordnen. Für die Umsetzung der IT-Strategie hat ebenfalls die Geschäftsleitung die Verantwortung zu tragen. Da bereits heute das Gros der Versicherer über eine angemessene IT-Strategie verfügt, sind in diesem Themenfeld keine wesentlichen Anpassungsaufwände zu erwarten. Lediglich vor dem Hintergrund der eingeforderten Aktualität der Strategie werden sich einzelne Häuser kritisch hinterfragen müssen.

2) IT-Governance

Unter dem Aspekt der IT-Governance verstehen die VAIT die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme mit den dazugehörigen IT-Prozessen. Die Ausgestaltung der IT-Governance soll dabei auf Basis der IT-Strategie erfolgen und zu angemessenen Vorgaben bzgl. IT-Organisation und Personalausstattung sowie Informationsrisiko- und Informationssicherheitsmanagement führen. Die Ausstattung des IT-Ressorts muss dabei die Erreichung der in der IT-Strategie definierten Ziele ermöglichen. Analog zur IT-Strategie nimmt die BAIT die Geschäftsleitung für die angemessene Ausgestaltung der IT-Governance in die Pflicht. Insbesondere vor dem Hintergrund der demografischen Herausforderungen in den IT-Bereichen muss die Geschäftsleitung sicherstellen, dass es durch das Ausscheiden von Mitarbeitern zu keiner Einschränkung des Betriebs kommt.

3) Informationsrisikomanagement

Im Kontext des Informationsrisikomanagements haben die Unternehmen Informationsrisiken in der Organisation systematisch zu identifizieren. Für die Risiken sind anschließend risikoreduzierende Maßnahmen zu definieren. Für die Ausübung des Risikomanagements sind angemessene Überwachungs- und Steuerungsprozesse einzurichten und regelmäßig durchzuführen. Über die Ergebnisse des Informationsrisikomanagements ist die Geschäftsleitung zu informieren. Ist die Versicherungswirtschaft insbesondere durch Solvency II schon zu einem umfassenden Risikomanagement angehalten, gilt es dieses nun auch explizit auf die IT auszuweiten. Einige Unternehmen betreiben dies bereits heute vorbildlich, es gibt jedoch auch Häuser, welche sich mit entsprechenden Anpassungsbedarfen auseinandersetzen werden müssen.

4) Informationssicherheitsmanagement

Beim Informationssicherheitsmanage-

Dr. Jan Hendrik Sohl
Als verantwortlicher Partner bei zeb befasst sich Dr. Jan Hendrik Sohl mit IT-Strategien und IT-Transformationen im Versicherungssektor.
Michael Kötting
Senior Consultant bei zeb
Im Rahmen seiner Tätigkeit beschäftigt er sich u. a. mit IT-Transformationen und IT-Compliance in Versicherungsunternehmen.

ment greift die BaFin auf Anforderungen etablierter Standards zurück. Haben insbesondere Versicherer mit ISO/IEC-2700X-Zertifizierung schon grundlegende Maßnahmen, wie einen kontinuierlichen Verbesserungskreislauf, umgesetzt, müssen nach den VAIT nun sämtliche Versicherer einen solchen Regelkreislauf im Unternehmen etablieren. Ziel ist es, die Informationssicherheit auf dieser Basis iterativ zu verbessern und stets dem aktuellen Stand der Technik anzupassen. Die Steuerung dieses Prozesses hat ein zu benennender Informationssicherheitsbeauftragter zu übernehmen, der seine Ergebnisse regelmäßig an die Geschäftsleitung zu kommunizieren hat.

5) Benutzerberechtigungsmanagement

Unternehmen haben über ein angemessenes Benutzerberechtigungsmanagement sicherzustellen, dass Mitarbeiter nur mit Berechtigungen ausgestattet werden, welche sie für die Durchführung ihrer vorgesehenen Tätigkeit benötigen. Berechtigungen müssen somit im Rahmen eines geregelten Prozesses möglichst restriktiv vergeben und bei Nichtgebrauch wieder entzogen werden. Die Vorgaben zur Berechtigungsvergabe müssen in einem Berechtigungskonzept dokumentiert sein. Da das Berechtigungsmanagement im Rahmen von IT-Prüfungen regelmäßig zu Feststellungen führt, gilt es ein besonderes Augenmerk auf dieses Themenfeld zu legen.

Die Herausforderung bei der Etablierung eines angemessenen Berechtigungsmanagements lässt sich unter anderem mit der hohen Komplexität begründen, welche durch eine Vielzahl dezentraler Berechtigungsinhaber entsteht. Es werden sich daher nur wenige Häuser finden lassen, welche bereits heute den VAIT-Anforderungen in Bezug auf das Benutzerberechtigungsmanagement entsprechen.

6) IT-Projekte und Anwendungsentwicklung

Das Themenfeld IT-Projekte und Anwendungsentwicklung verlangt von Versicherern im Vorfeld von IT-Projekten deren Auswirkungen auf die IT-Aufbau- und IT-Ablauforganisation sowie die dazugehörigen IT-Prozesse im Rahmen einer Auswirkungsanalyse zu bestimmen. Die Gesamtheit der IT-Projekte ist dabei durch ein angemessenes Portfoliomanagement zu steuern. Neben der projekthaften Umsetzung sind nach den VAIT auch entsprechende Prozesse für das Anforderungsmanagement samt Umsetzung zu definieren.

Alle Themenfelder der VAIT legen einen hohen Wert auf eine transparente und nachvollziehbare Dokumentation

Während die Unternehmen im Rahmen der zentralen Anwendungsentwicklung wohl nur mit kleineren Anpassungen rechnen müssen, sehen die VAIT auch umfassende Anforderungen an die Entwicklung und den Betrieb von individueller Datenverarbeitung (IDV) vor. Auf diese Anforderungen dürften die wenigsten Häuser vorbereitet sein. Wie aufwendig allein die Aufstellung und Pflege eines auf wenige Teilbereiche beschränkten IDV-Inventars sein kann, sollten viele Unternehmen bereits im Rahmen von Solvency II in ihren Aktuariaten zu spüren bekommen haben. Die Erfüllung der VAIT-Anforderungen wird diesen Aufwand noch einmal deutlich übersteigen.

7) IT-Betrieb

Der IT-Betrieb hat die Anforderungen, welche sich aus der Umsetzung der IT-Strategie und IT-unterstützenden Geschäftsprozessen ergeben, umzusetzen. Neben dem reibungslosen Betrieb umfasst diese Themenstellung insbesondere auch das Portfoliomanagement der IT-Systeme unter Berücksichtigung der Risiken veralteter IT-Anwendungen. Damit dies gelingen kann, erfordern die VAIT aktuelle Dokumentationen über die Komponenten der einzelnen IT-Systeme sowie deren Beziehung untereinander. Ist eine Systemübersicht auch in vielen Häusern bereits vorhanden, muss sichergestellt werden, dass diese stets aktuell gehalten wird.

Die größere Herausforderung wird in diesem Zusammenhang jedoch die Herstellung der Transparenz über Datenflüsse zwischen einzelnen Systemen sein. Über eine vollständige und aktuelle Aufstellung verfügen aus der Erfahrung heraus die wenigsten Unternehmen.

8) Auslagerungen und sonstiger IT-Fremdbezug

Auch IT-Dienstleistungen gilt es zukünftig im Rahmen des Informationsrisikomanagements zu betrachten und in die Gesamtrisikobewertung des Unternehmens miteinzubeziehen. Weiterhin sind die aus den Risiken abgeleiteten Maßnahmen in der Vertragsgestaltung mit dem Dienstleister zu berücksichtigen. Zur Erfüllung der Anforderungen verlangen die VAIT dazu eine vollständige und strukturierte Vertragsübersicht. Auf Basis dieser Übersicht hat die Steuerung der Dienstleister zu erfolgen. Dass einzelne Dienstleistungsverträge zur Sicherstellung der VAIT-Konformität gänzlich neu abzuschließen sind, kann nicht ausgeschlossen werden.

als Zitat

Alle Themenfelder der VAIT legen einen hohen Wert auf eine transparente und nachvollziehbare Dokumentation. Die Unternehmen müssen daher sicherstellen, dass sie getroffene Abwägungen und Umsetzungsentscheidungen im Rahmen von Prüfungen unverzüglich vorlegen können. Die VAIT machen deutlich, dass die Geschäftsleitung für die Umsetzung der Regulierung in die Pflicht genommen wird. So obliegt die Verantwortung für eine ordnungsgemäße Geschäftsorganisation nach den VAIT explizit der obersten Führungsebene des Versicherungsunternehmens. Die VAIT beziehen sich dabei auf die gesamte Geschäftsleitung eines Unternehmens, sodass die Verantwortung nicht an den entsprechenden Geschäftsführer der IT abgetreten werden kann.

Abbildung 2

Nach Skizzierung der einzelnen Themenfelder soll eine grobe Einordnung hinsichtlich des entsprechenden Umsetzungsaufwands gegeben werden (siehe Abbildung 2). Während bereits erläutert wurde, dass die Anforderungen der VAIT bzgl. IT-Strategie und IT-Governance schon heute weitestgehend zum Marktstandard in der Versicherungswirtschaft gehören, finden sich in den weiteren Themenstellungen einzelne

Aspekte, die bisher überwiegend unbeachtet blieben. Ist das in Abbildung 2 dargestellte Profil zwar ohne Frage sehr individuell und von Haus zu Haus unterschiedlich ausgeprägt, gibt es erfahrungsgemäß dennoch einen guten Querschnitt der Versicherungswirtschaft wieder.

Praktische Umsetzung unter Berücksichtigung des Proportionalitätsprinzip

Bei der Umsetzung der VAIT-Anforderungen dürfen die Unternehmen nach dem Proportionalitätsprinzip agieren. Konkret bedeutet dies: eine der Komplexität des Unternehmens und der IT angemessene Ausgestaltung und Umsetzung der Anforderungen. Unter Berücksichtigung des individuellen Risikoprofils kann die geringe Größe eines Versicherers ein Hinweis dafür sein, dass die Konformität zu den Anforderungen der VAIT mit einfacheren Strukturen und Prozessen erreicht werden kann. Umgekehrt sind von Unternehmen mit hohem Risikoprofil aufwendigere Strukturen und Prozesse erforderlich.

Konkrete Angaben zum Risikoprofil und den einem Profil entsprechenden Strukturen und Prozessen finden sich in den VAIT jedoch nicht. Versicherer müssen daher im Kontext ihrer Organisation entscheiden, welche Umsetzungsmaßnahmen sie für die Erfüllung der VAIT-Anforderungen als angemessen erachten. Zu Zwecken der Transparenz sollten die entsprechenden Entscheidungen begründet und dokumentiert werden.

Da das Risikoprofil eines Unternehmens nicht statisch ist, sind Versicherer dazu angehalten, die Angemessenheit der umgesetzten Strukturen und Prozesse regelmäßig einer Überprüfung zu unterziehen. Dies kann im Rahmen des Informationsrisikomanagements erfolgen. Sollte sich das Risikoprofil eines Unternehmens verändert haben, sind die Strukturen und Prozesse in der IT entsprechend anzugleichen, sodass die angemessene Erfüllung der VAIT-Anforderungen wiederhergestellt ist. Zur Nachvollziehbarkeit der Einhaltung dieses Regelkreislaufs sollte eine transparente und stets aktuell gehaltene Dokumentation vorliegen.

Zeitnahe Umsetzung der VAIT gefordert

Nachdem der erste Entwurf der VAIT im November 2017 veröffentlicht wurde, hat die BaFin im Januar 2018 eine überarbeitete Version vorgelegt, um darauf aufbauend Mitte 2018 die Endfassung der VAIT zu verabschieden. In seinen Anmerkungen zur ersten Entwurfsfassung hat der GDV insbesondere für eine Minimierung der Dokumentationsaufwände und eine Umsetzung mit Augenmaß plädiert, um die Aufwände für kleine und mittlere Versicherungsunternehmen handhabbar zu halten.

Insbesondere vor dem Hintergrund der bereits final verabschiedeten bankaufsichtlichen Anforderungen an die IT (BAIT) wird es der BaFin jedoch ein Anliegen sein, mit der finalen Fassung der VAIT ein möglichst ähnliches Anforderungsniveau für Versicherer und Banken herzustellen und Versicherern gegenüber Banken keine allzu großen Erleichterungen und Privilegien einzuräumen. Wesentliche Erleichterungen im Rahmen weiterer Überarbeitungen sind daher nicht zu erwarten.

Versicherer sollten sich also zeitnah mit der vorliegenden Fassung der VAIT auseinandersetzen, um die Auswirkungen auf ihre Organisation abschätzen und analysieren zu können. Nur durch frühzeitige Vorbereitung werden die Unternehmen sicherstellen können, dass sie nach der Veröffentlichung der finalen Version den Anforderungen genügen. Identifizierte Lücken sollten daher unter Berücksichtigung des Proportionalitätsprinzips und entlang etablierter Standards schnellstmöglich geschlossen werden.

Fazit

Mit der Veröffentlichung des Entwurfs der VAIT unterstreicht die BaFin den hohen Stellenwert der Versicherungs-IT. So räumt die BaFin mit den VAIT ein, dass bereits einzelne IT-Risiken umfassende Auswirkungen auf die Geschäftstätigkeit von Versicherungsunternehmen haben können. Durch die Umsetzung entsprechender Strukturen und Prozesse gilt es, dem Eintreten solcher Risiken vorzubeugen. Neben der thematischen Vielfalt der VAIT sollte auch die Tiefe der Anforderungen an einzelne Prozesse anerkannt werden.

Exemplarisch wird im Rahmen des Informationssicherheitsmanagements gefordert, dass dieses nicht nur die Stufen Planung, Umsetzung und Erfolgskontrolle umfassen sollte, sondern auch die Optimierung und Verbesserung der Informationssicherheit im Rahmen eines Regelkreislaufs mit in die Betrachtung aufzunehmen sind. An diesem Beispiel wird deutlich, dass durch die VAIT ein höchstmöglicher Reifegrad eines Prozesses – nach dem Referenzmodell CMMI – zur Minimalanforderung für alle Versicherer wird.

Abbildung 1: Themenfelder der VAIT

Abbildung 2: Umsetzungsaufwand der VAIT