plenum

versicherungen

versicherungs-rechtliche anforderungen an die it (vait)

handlungsbedarfe für die versicherungsindustrie

“jetzt den regler hochfahren!”

Nachdem das Versicherungsaufsichtsgesetz (VAG) und Solvency II ihre Konkretisierung der Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) erfahren haben, steht nun aus Sicht des BaFin-Chef Felix Hufeld (vgl. http://positionen.gdv.de/interview-mit-bafin-chef-felix-hufeld: „Jetzt den Regler hochfahren“) die IT im Mittelpunkt regulatorischer Anforderungen. Was aber genau soll nun in der VAIT (Versicherungsrechtliche Anforderungen an die IT) umgesetzt werden? In einem Rundschreiben an die Versicherungsunternehmen im Frühjahr 2018 sind hierzu erste Ansätze deutlich geworden. In acht Themenfeldern sind über sechzig Einzelanforderungen benannt worden, die es zu erfüllen gibt.

spezifische risiken in der it

Die Banken haben sie bereits hinter sich, den Versicherungen steht sie nun bevor: Die Fokussierung der Regulierung auf operationelle Risiken in der IT.

Analog zu den Banken verarbeiten Versicherungen sensible Daten ihrer Kunden und stellen in ihrer Gesamtheit eine kritische Infrastruktur dar.

besonderheiten der versicherungs-it

Im Detail stellt sich die Situation bei Versicherungen anders dar als bei Kreditinstituten. Das Krisenreaktionszentrum für Cybergefahren und die sicherheitszertifizierte Cloud TGIC sind Leuchtturm-projekte der Versicherungsindustrie.

Zudem sind die meisten Institute auf einem guten Weg, hohe Standards für Datensicherheit, Datenübermittlung und Krisenreaktionsprozesse zu definieren und umzusetzen.

Zur Wahrheit gehört aber auch, dass die Mehrzahl der Versicherungsunternehmen mittlerweile eine erhebliche Komplexität in der Architektur erreicht hat, die sie nun nicht nur störanfälliger, sondern auch angreifbarer macht.

Zusätzlich machen die erhöhten Cyberrisiken die Aufsicht sensibler. Versicherungen sind mittlerweile über das Internet mit zahlreichen Marktpartnern und Kunden vernetzt und sind damit aus verschiedenen Richtungen ständigen Bedrohungen ausgesetzt.

In Summe geht daher die Aufsicht davon aus, dass eine Konkretisierung der Anforderungen an die IT geboten ist. Diese Konkretisierung soll durch die VAIT erreicht werden.

vait noch in 2018

Ziel der VAIT ist, eine verbindliche, einheitliche und zu Kreditinstituten vergleichbare Auslegung der Anforderungen aus §21 VAG und MaGo für die IT-Organisation in Versicherungen zu erreichen.

fahrplan für die einführung der vait

Seit November 2017 befindet sich nun der erste Entwurf der VAIT in der Konsultationsphase. Mit einem überarbeiteten Entwurf wird spätestens zum Ende des ersten Quartals 2018 gerechnet.

In Kraft treten sollen die VAIT dann bereits Mitte 2018, ohne Übergangsfristen für die Versicherungen – denn aus Sicht der Aufsicht sind die Anforderungen genau genommen bereits seit 2017 zu erfüllen gewesen.

Prüfungen, die im zweiten Halbjahr 2018 und v.a. ab 2019 in Versicherungen durchgeführt werden, werden daher die VAIT vollumfänglich einbeziehen.

(fast) gleiche standards für alle

Die Bafin setzt bei der Formulierung der VAIT auf etablierte und anerkannte Standards. So werden zu verschiedenen Regelungsbereichen der IT-Sicherheit die IT-Grundschutzkataloge des BSI und die ISO 27001 herangezogen.

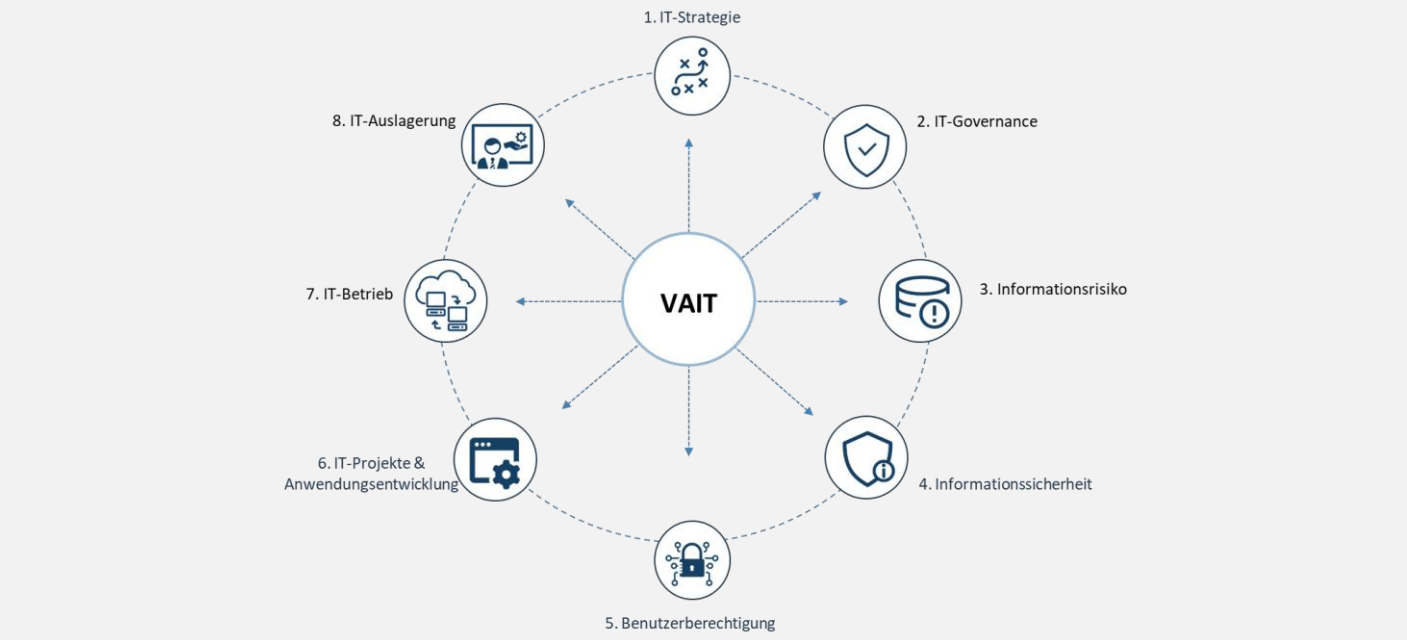
Für die Anforderungen an die Governance der IT wiederum setzen die VAIT auf den Frameworks CobIT und ITIL auf.

Die Aufsicht erwartet, dass durch Anwendung dieser Standards ein für jede Versicherung gestaltbarer Rahmen geschaffen wird, der die konkrete Umsetzung erleichtert – und gleichzeitig das Prüfungshandeln vereinheitlichen und damit vereinfachen wird.

Ob Versicherungen bei der VAIT Vereinfachungen vornehmen dürfen, wird sich v.a. an der Komplexität des Unternehmens und seiner IT orientieren.

die acht themenfelder der vait

Die VAIT bündelt die über sechzig Einzelanforderungen in acht Themenfeldern und lehnt sich in deren Strukturierung eng an die BAIT der Kreditinstitute an. Die VAIT werden jedoch gegenüber den BAIT deutlich konkretere Anforderungen an die IT stellen, da die übergeordnete Regulierung, v.a. die MaGo, im Vergleich zur MaRisk nur einen geringen Detaillierungsgrad zu IT-spezifischen Fragestellungen aufweist.



1. it-strategie

Formulierung einer detaillierten und konkreten IT-Strategie, die u.a. Organisations- und IT-Risiko-Fragestellungen adressiert.

2. it-governance

Mechanismen zur wirksamen Umsetzung der IT-Strategie durch eine Organisation, die frei von Interessenkonflikten gestaltet ist.

3. informations-risikomanagement

Nutzung von Prozessen zur Erkennung und Steuerung von Risiken für die Schutzziele der Informationssicherheit.

4. informations-sicherheitsmanagement

Etablierung eines Systems zur Herstellung und Aufrechterhaltung eines angestrebten Sicherheitsniveaus.

5. benutzerberechtigungs-management

Verfahren zur Einrichtung, Änderung und Entfernung von Berechtigungen unter Wahrung von Minimal- und Funktionstrennungsprinzip.

6. it-projekte & anwendungsentwicklung

Regelungen zur Bereitstellung von Änderungen an IT-Systemen, von der Anforderungsdefinition bis zur Produktivstellung (inkl. Individuelle Datenverarbeitung).

7. it-betrieb

Sicherstellung eines sicheren IT-Betriebs und kontrollierter Änderungen der IT-Systeme – unter Zuhilfenahme eines aktuellen Asset-Registers.

8. it-auslagerungen

Steuerung insbesondere der Risiken von IT-Auslagerungen und sonstigem Fremdbezug.

zeit zu handeln!

Mit der in wenigen Monaten anstehenden Verabschiedung der VAIT ist die verbleibende Zeit für die Versicherungen eng bemessen. Inwiefern Ihr Haus konkreten Handlungsbedarf aufweist, können Sie in einem ersten Schritt mit unseren VAIT Self Assessment ermitteln: Falls Sie eine der Fragen nicht eindeutig mit „Ja“ beantworten können, ist eine tiefergehende Analyse angeraten.

Ausgewählte Fragestellungen der VAIT	ja	tlw.	nein	?
IT Strategie				
Wird Ihre IT-Strategie fortlaufend an die Geschäftsstrategie angepasst, mit Performance Indikatoren überwacht und durch Maßnahmen umgesetzt?	☐	☐	☐	☐
Enthält Ihre IT-Strategie Aussagen u.a. zu Informationssicherheit, Auslagerungen, Notfallmanagement und individueller Datenverarbeitung?	☐	☐	☐	☐
IT Governance				
Beachtet Ihre Aufbau- und Ablauforganisation das Funktionstrennungsgebot?	☐	☐	☐	☐
Sind u.a. IT-Sicherheit, IT-Risiko, IT-Betrieb und Anwendungsentwicklung quantitativ und qualitativ ausreichend personell besetzt?	☐	☐	☐	☐
Informationsrisikomanagement				
Ist ein integriertes, die Fachbereiche umfassendes Informationsrisikomanagement etabliert, das in das Risikoreporting eingebunden ist?	☐	☐	☐	☐
Verfügen Sie über einen aktuellen und vollständigen Überblick über die Bestandteile des Informationsverbundes, dessen Abhängigkeiten und Schnittstellen?	☐	☐	☐	☐
Informationssicherheitsmanagement				
Sind die Informationssicherheitsleitlinien als konkretisierende, aktuelle Richtlinien und Prozesse definiert und wird deren Einhaltung kontrolliert?	☐	☐	☐	☐
Verfügt Ihr Institut über einen organisatorisch unabhängigen Informationssicherheitsbeauftragten, der regelmäßig direkt an die Geschäftsleitung berichtet?	☐	☐	☐	☐
Benutzerberechtigungsmanagement				
Berücksichtigt Ihr Benutzerberechtigungsmanagement das Prinzip der Funktionstrennung und den Sparsamkeitsgrundsatz?	☐	☐	☐	☐
Sind aufbauend auf diesen Prinzipien Berechtigungskonzepte für alle IT-Systeme definiert und wird Ihre Beachtung unabhängig überprüft?	☐	☐	☐	☐
IT-Projekte & Anwendungsentwicklung				
Werden die Vorgaben der Anwendungsentwicklung in Ihrem Institut an den Schutzbedarf der Anwendungen bzw. der verarbeiteten Daten angepasst?	☐	☐	☐	☐
Gilt dies auch für sog. „Individuelle Datenverarbeitung“, wie dezentral, in den Fachbereichen erstellte Anwendungen (bspw. auf Basis von Office-Produkten erstellte Anwendungen)?	☐	☐	☐	☐
IT-Betrieb				
Sind die Komponenten aller IT-Systeme sowie deren Beziehungen untereinander erfasst und werden diese Informationen aktuell gehalten?	☐	☐	☐	☐
Werden Datensicherungen gemäß der Geschäftsfortführungspläne vorgenommen und werden diese Sicherungen auf Wiederherstellbarkeit und Lesbarkeit geprüft?	☐	☐	☐	☐
Auslagerungen				
Werden Risikobewertungen für Auslagerungen und sonstigen Fremdbezug durchführt? Werden diese Risiken überwacht und gesteuert?	☐	☐	☐	☐
Integrieren Sie in dieses Verfahren auch den Fremdbezug von Cloud-Diensten, auch wenn dieser dezentral seitens der Fachbereiche erfolgt?	☐	☐	☐	☐

Abb.1: VAIT Self Assessment – Auszug aus dem Anforderungskatalog

unser angebot: der vait quick check

plenum führt seit vielen Jahren erfolgreich regulatorische Projekte für die IT in Versicherungen und Banken durch. Unser „VAIT Quick Check“ bündelt diese Erfahrung mit unseren konkreten Erkenntnissen aus der BAIT Prüfungspraxis zu einem praxisnahen Kompass zur Positionsbestimmung im ausziehenden regulatorischem Sturm in der Versicherungsindustrie.

Das Assessment zeigt Ihnen in kurzer Zeit Ihre individuellen Handlungsbedarfe in einem ganzheitlichen Rahmen (inkl. DSGVO, BSI, etc.) auf und ist damit eine gute Basis für den Aufbau einer ganzheitlichen IT Compliance. plenum bietet Ihnen einen prüfungserprobten, pragmatischen Ansatz, um die neuen regulatorischen Anforderungen der VAIT vollständig zu erkennen und in einen ganzheitlichen, für Ihr Haus angemessene Compliance-Organisation zu übersetzen.

Mit einem kompakten und ressourcenschonenden Vorgehen bieten wir Ihnen eine Standortbestimmung innerhalb von 6-8 Wochen. Neben den Prüfungsstellen Ihrer IT aus Sicht der VAIT zeigen wir Ihnen auf, mit welchen Sofortmaßnahmen Sie Ihre Compliance kurzfristig verbessern können.

Wichtigster Mehrwert unseres Vorgehens ist, auf Basis unserer mehr als 30 Jahre Erfahrung in der IT von Versicherungsunternehmen gemeinsam mit Ihnen zukunftsorientierte Maßnahmen zu erarbeiten, die für eine angemessene und nachhaltige Compliance in Ihrem Hause sorgen.