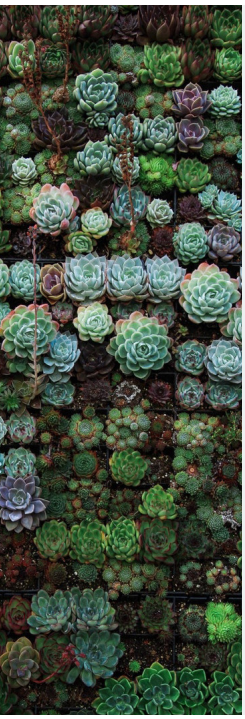
Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

BaFin fordert mehr IT-Sicherheit von Versicherungsunternehmen

Anja Zimmer
Gerhard Günther
Michaela Burger
Nadja Karlson

Übersicht der VAIT



- BaFin plant die Veröffentlichung der VAIT für Mitte 2018
- Konkretisierung der Mindestanforderungen an die Geschäftsorganisation (MaGo) im Bereich der Ressourcenausstattung
- Umfangreiche Dokumentationsvorgaben, u.a. Informationssicherheits-leitlinie, zentrales Register über alle Anwendungen (inkl. individuelle Datenverarbeitung), Datensicherungskonzept und Anwendungsentwicklung
- Einrichtung der Funktion eines Informationssicherheitsbeauftragten
- Vertragsübersicht für IT-bezogene Ausgliederungen inkl. Subdelegationen

Die BaFin hat am 13. März 2018 die öffentliche Konsultation zu den „Versicherungsaufsichtlichen Anforderungen an die IT“ (VAIT) gestartet. Unternehmen hatten Zeit, bis zum 20. April 2018 Stellung zu nehmen. Es ist beabsichtigt, die Anforderungen Mitte dieses Jahres in Kraft treten zu lassen. Eine Umsetzungsfrist ist nicht vorgesehen.

Basierend auf dem aktuellen Bedrohungsumfeld in Bezug auf Cyberrisiken schafft die BaFin mit den VAIT eine verbindliche Handlungsgrundlage für Versicherungsunternehmen für den verlässlichen Betrieb von IT-Systemen, für Kontrollprozesse sowie für die Behandlung von Notfällen und Schäden.

Ziel der VAIT ist die Förderung der Transparenz und des Bewusstseins für IT-Risiken in Unternehmen. Im Rahmen der Etablierung der VAIT werden die Vorschriften über die Geschäftsorganisation im Versicherungsaufsichtsgesetz (§ 23 VAG) sowie die Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) berücksichtigt und spezifiziert, insbesondere im Hinblick auf die personelle und technisch-organisatorische Ausstattung. Für den Bankensektor hat die BaFin bereits im November 2017 einen analogen Standard veröffentlicht, die sogenannten „Bankaufsichtliche Anforderungen an die IT“, kurz BAIT. Erwartungsgemäß finden sich viele der Anforderungen auch in der VAIT wieder.
Allerdings zeigt der uns vorliegende Entwurf, dass die BaFin die Anforderungen für Versicherungsunternehmen in einigen Bereichen noch verschärfen will. So sollen u.a. die Vorschriften für Ausgliederungen auch für den isolierten Bezug von Hard- und/oder Software gelten.

Das unter Solvency II verankerte Proportionalitätsprinzip soll auch bei der Umsetzung der VAIT Anwendung finden. Die Anforderungen sind auf eine Weise zu erfüllen, die der Wesensart, dem Umfang und der Komplexität der mit der Tätigkeit des Unternehmens einhergehenden Risiken gerecht wird (§ 296 Abs. 1 VAG).

Die VAIT gliedern sich in acht Themengebiete. Abbildung 1 gibt einen Überblick über die wesentlichen Inhalte.

IT-Strategie	Festlegung einer mit der Geschäftsstrategie konsistenten und nachhaltigen IT-Strategie	▪ Strategische Entwicklung der IT-Aufbau- und Ablauforganisation, Ausgliederungen und IT-Architektur ▪ Zuordnung gängiger IT-Standards ▪ Einbindung Informationssicherheit ▪ Notfallmanagement
IT-Governance	Etablierung einer Struktur zur Steuerung, Überwachung und Weiterentwicklung der IT auf Basis der IT-Strategie	▪ Umsetzung und Wirksamkeit verantwortet die Geschäftsleitung ▪ Angemessene Ressourcenausstattung, sowohl personell als auch technisch-organisatorisch ▪ Kriterienkatalog zur Steuerung und Überwachung
Informations-risiko-management	Implementierung eines internen Kontrollsystems für IT-Systeme und zugehöriger Prozesse	▪ Sicherstellung der Schutzziele von Daten durch Schutzbedarfsermittlung und Sollmaßnahmenkatalog ▪ Risikoanalyse anhand definierter IT-Risikokriterien sowie Restrisikoüberwachung ▪ Regelmäßige Berichtspflichten, u.a. vierteljährlicher Statusbericht
Informations-sicherheits-management	Definition, fortlaufende Überprüfung und Steuerung von Sollvorgaben und Prozessen zur IT-Sicherheit	▪ Erstellung einer Informationssicherheitsleitlinie und Definition von IT-Prozessen gemäß gängiger Standards ▪ Schaffung der Position eines unabhängigen Informationssicherheitsbeauftragten ▪ Regelungen zu Informationssicherheitsvorfällen sowie regelmäßige Berichterstattung
Benutzer-berechtigungs-management	Ausgestaltung der Berechtigungen entsprechend den organisatorischen und fachlichen Vorgaben des Unternehmens	▪ Berechtigungskonzepte unter Beachtung der Aufbau- und Ablauforganisation sowie der Funktionstrennung ▪ Genehmigungs- und Kontrollprozesse für Zugriffsrechte sowie regelmäßige Überprüfung und Aktualisierung ▪ Protokollierung und Überwachung der ordnungsgemäßen Ausübung von Berechtigungen
IT-Projekte, Anwendungs-entwicklung	Angemessene Steuerung und Überwachung der IT-Projekte und Anwendungsentwicklung	▪ Vorschriften gelten auch für eigenentwickelte Anwendungen (IDV) ▪ Implementierung eines unternehmensweiten IT-Projekt- und Anwendungsentwicklungsmanagementprozesses ▪ Führung eines zentralen Registers für alle Anwendungen ▪ Berichtspflicht für wesentliche IT-Projekte und -Risiken
IT-Betrieb	Ausgestaltung und Umsetzung der Anforderungen für IT-unterstützte Geschäftsprozesse	▪ Geeignete Verwaltung von IT-Systemkomponenten und ihrer Beziehungen sowie angemessene Steuerung des Portfolios aus IT-Systemen ▪ Ausgestaltung von Prozessen für Änderungen, Neu- oder Ersatzbeschaffungen ▪ Datensicherungskonzept und Notfallmanagement
Ausgliederungen	Ausweitung des Ausgliederungsbegriffs auf IT-Dienstleistungen basierend auf der IT-Strategie	▪ Verpflichtende revolvierende Risikoanalyse für jeglichen Fremdbezug von IT-Dienstleistungen ▪ Führung eines Vertragsregisters zur jederzeitigen Vorlage der Ausgliederungsverträge sowie der Verträge für sämtliche Subdelegationen ▪ Ausweitungen der Vorschriften auf den isolierten Bezug von Hard- und Software

Abbildung 1: Modularer Aufbau der VAIT

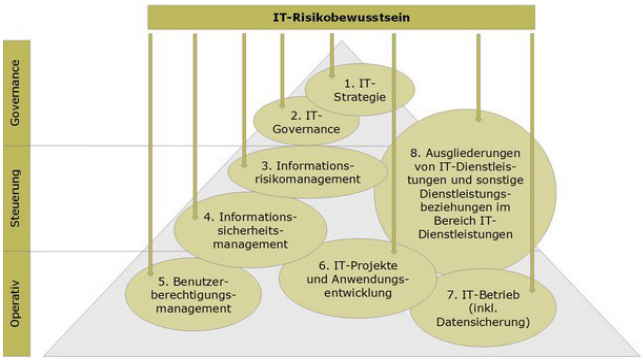
Neuerungen aus regulatorischer Sicht

Ausgliederungen

Durch den zunehmenden Drittbezug von Dienstleistungen im IT-Bereich gelten detaillierte Ausgliederungsanforderungen im Einklang mit dem strategischen IT-Leitbild. Durch die Ausweitung auf Subdelegationen beabsichtigt die BaFin ein Durchgriffsrecht entlang der gesamten Wertschöpfungskette. Die Letztverantwortung trägt die Geschäftsleitung.
Die umfangreichen Vorgaben zu Ausgliederungen – etwa die obligatorische Risikoanalyse und -bewertung (inkl. Ausfallrisiko des Dienstleisters) oder die Führung eines Vertragsregisters – gelten auch für den isolierten Bezug von Soft- und Hardware.

Dokumentationspflichten

Die VAIT weiten bereits bestehende Dokumentationspflichten aus der MaGo auf den Themenkomplex IT und Informationssicherheit aus. Im Wesentlichen fordern sie künftig eine Informationssicherheitsleitlinie, ein Datensicherungskonzept, ein Anwendungsregister sowie ein Vertragsregister für Ausgliederungen.
Versicherer haben daher mit höherem Aufwand zu rechnen. Etwa für den Aufbau eines Registers zur Identifizierung aller von den Fachbereichen genutzten Anwendungen (inklusive IDV).
In diesem Zusammenhang sind umfangreiche Anforderungen hinsichtlich der Risikoklassifizierung und Schutzbedarfseinstufung der Anwendungen sowie zu Programmierrichtlinien, zur Methodik von Testverfahren und zur Rezertifizierung der Berechtigungen umzusetzen.



Schärfung des IT-Risikobewusstseins durch die VAIT; © BaFin

IT-Strategie und -Governance

Die Sicherstellung der Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit sensibler Geschäftsdaten sind ein Hauptziel der VAIT. Hierfür sollen die Unternehmen ein holistisches und transparentes Governancesystem durch Spezifizierung der allgemeinen Regeln zur IT-Strategie, Aufbau- und Ablauforganisation, Ressourcenausstattung und Dokumentationspflichten etablieren. Dieser angestrebte einheitliche Rahmen zur Steuerung, Überwachung und Weiterentwicklung der IT-gestützten Geschäftsprozesse zieht sich durch alle Teilaspekte der prinzipienorientierten VAIT:
Vom IT-Leitbild (inkl. damit einhergehendem Outsourcing) über IT-Risiko- und Informationssicherheitsmanagement bis hin zu IT-Projekten und dem Betrieb von IT-Systemen. Solche detaillierten und aufeinander abgestimmten Risikosteuerungs- und Controllingprozesse sind essentiell, um kontinuierlich IT-Risiken adäquat zu begegnen.

Risikokultur

Ein weiteres Anliegen der BaFin ist, die Risikokultur innerhalb der Unternehmen zu fördern und zu etablieren.

Geschäftsleitung wie Mitarbeiter sollen sich bewusst mit den relevanten Risiken im täglichen Geschäft und Handeln auseinandersetzen.

Um dieses Risikobewusstsein zu schärfen, definieren die VAIT eine Reihe von Anforderungen. U.a. soll die Geschäftsleitung die Bedeutung der Informationssicherheit im Unternehmen sowie deren Einbettung in die Fachbereiche im Rahmen der IT-Strategie klar herausstellen.

Es ist darauf zu achten, dass die auf der IT-Strategie basierenden Organisationsrichtlinien sachgerecht und für die Mitarbeiter des Unternehmens nachvollziehbar sind.

Rollenmodelle sind so zu gestalten, dass Interessenkonflikte zwischen Aktivitäten, etwa der Anwendungsentwicklung und den Aufgaben des IT-Betriebs, vermieden werden.

Von den VAIT gefordert werden ferner Maßnahmen, die fortlaufend ein angemessenes Qualifikationsniveau der Mitarbeiter im Bereich der IT sicherstellen.

Handlungsbedarf und mögliche Maßnahmen

Die acht Themengebiete der VAIT sind für die meisten Unternehmen nicht neu: Viele Versicherer berücksichtigen schon heute die gängige Standards wie den IT-Grundschutzkatalog oder den internationaler Sicherheitsstandard (ISO/IEC2700X) für das Management ihrer IT-Ressourcen und die Ausgestaltung ihrer IT-Systeme sowie der dazugehörigen Prozesse.

Neu ist, dass die BaFin mithilfe der VAIT die Anforderungen an die IT aus regulatorischer Sicht präzisiert und hier in Zukunft eine adäquate Umsetzung sowie die Offenlegung im Rahmen der Berichterstattung erwartet.

Die Audit- und Beratungserfahrung der metafinanz zeigt, dass einige Themen in der IT-Praxis bisher eher unzureichend umgesetzt sind. Handlungsbedarf besteht daher zunächst in der Identifizierung noch nicht berücksichtigter Anforderungen.

Aus unserer Sicht ist u.a. zu prüfen, ob sich die IT-Strategie an der Geschäftsstrategie ausrichtet. Hat das Unternehmen Richtlinien, welche die Ziele und den Geltungsbereich von Informationssicherheit festhalten und die organisatorischen Aspekte des Informationssicherheitsmanagements beschreiben? Gibt es einen unabhängigen Informationssicherheitsbeauftragten?

Die strategische, qualitative und quantitative Ressourcenplanung für den Betrieb und die Weiterentwicklung von Dienstleistungen müssen im Einklang mit aktuellen und künftigen IT-Bedrohungsszenarien stehen.

Im Rahmen der Dokumentationspflichten liegt der Handlungsbedarf bei der Identifizierung der Dokumentationsanforderungen, die im Unternehmen noch nicht abgedeckt sind (Abweichungsanalyse).

Unternehmen sollten prüfen, inwieweit sich die Dokumentationsvorgaben (u.a. Register für eigen- und fremdentwickelte IT-Anwendungen, Vertragsregister für Ausgliederungen) in bereits bestehende Dokumentationsprozesse einbinden lassen.

Für die Dokumentation sind Verantwortliche zu definieren, die für die Erstellung, Abstimmung sowie regelmäßige Überprüfung und Aktualisierung zuständig sind. Hierfür ist ein Prozess zur Dokumentenlenkung (z.B. Versionskontrolle, Speicherung, Kommunikation) einzuführen.

Versicherer müssen außerdem Maßnahmen ergreifen, um einerseits die Geschäftsleitung über die wesentlichen IT-Risiken jederzeit in Kenntnis zu setzen und anderseits eine adäquate Steuerung und Überwachung des IT-Betriebs und der Datensicherheit zu gewährleisten.

Ein wesentliches Element zur Erhöhung des IT-bezogenen Risikobewusstseins ist das Schaffen einer angemessenen Risikokultur z.B. durch Schulungen. Als Handlungsleitfaden für ein einheitliches und erprobtes Rahmenwerk für die IT-Governance dienen internationale Best-Practice-Standards (z.B. COBIT 5). Das Kernstück ist dabei die Angleichung zwischen der Geschäfts- und der IT-Strategie und die Integration auf Prozessebene.

Prozessreferenzmodelle liefern einen wertvollen Beitrag zur Konkretisierung der Kernelemente der VAIT. Diese lassen sich unter anderem für die Steuerung des Portfolios von IT-Systemen im IT-Betrieb oder im Rahmen des Programm- und Projekt-Managements einsetzen.

Ein weiterer Bestandteil zur Umsetzung der VAIT ist der Einsatz von integrierten und auditsicheren Governance, Risk & Compliance (GRC-)Systemen. Diese unterstützen sowohl die Dokumentation als auch die Überwachung der Risiken, der Kontroll- und der Auditprozesse. Hierdurch wird die erforderliche Transparenz und Sicherheit gegenüber internen und externen Gefahren gewährleistet.

metafinanz: Adäquate Lösungen an der Schnittstelle Fachbereich und IT.

Für die wesentlichen Konkretisierungen der VAIT steht Ihnen die metafinanz jederzeit als verlässlicher Partner zur Verfügung.

Ausgehend von einer detaillierten und transparenten Analyse des Status Quo, der Prozesse und des geforderten Handlungsbedarfs, formulieren wir Empfehlungen und konkrete Maßnahmen.

Gerne unterstützen wir Sie bei der Implementierung geeigneter Lösungen.
Profitieren Sie von unserer langjährigen Erfahrung in der Implementierung und Konfiguration aufeinander abgestimmter, modularer GRC-Systeme für die wesentlichen IT-bezogenen Neuerungen, wie Richtlinien-, Risiko-, Workflow- und Vertragsmanagement.

Unsere Leistungen für Sie:

- **Transformieren gesetzlicher Anforderungen in organisatorische und technologische Lösungen**
- **Implementierung, Konfiguration und Wartung einer integrierten und zukunftssicheren GRC-Landschaft**
- **Expertise in der Identifizierung und dem Management von Cyberrisiken und Operational Risk**
- **Jahrelange Erfahrung im IT-gestützten Veränderungs-, Prozess- und Projektmanagement**
- **Umfangreiches Expertennetzwerk**

We. Ensure. Success.

Ihre Ansprechpartner

Dr. Anja Zimmer
Project Lead

+49 89 360531-5492
Anja.Zimmer@metafinanz.de

Gerhard Günther
Lead RegTech

+49 89 360531-5618
Gerhard.Guenther@metafinanz.de

Michaela Burger
Project Lead

+49 89 360531-5685
Michaela.Burger@metafinanz.de

Nadja Karlson
Project Lead

+49 89 360531-5680
Nadja.Karlson@metafinanz.de

metafinanz Informationssysteme GmbH
Leopoldstr. 146
80804 München