plenum

versicherungen

vait - regulatorik als chance begreifen!

wie aus regulatorischen anforderungen echter mehrwert generiert werden kann

vait - regulatorik als chance begreifen

Seit Verabschiedung der VAIT im Juli 2018 sind einige Versicherungsunternehmen bereits umfangreich durch die BaFin geprüft worden. Die ersten vorliegenden Ergebnisse zeigen, dass es auch in der Versicherungswirtschaft deutlichen Nachholbedarf gibt. Laut BaFinJournal vom 15.10.2020 "IT der Versicherer im Fokus" sind 16 Erst- und Rückversicherungen sowie Pensionskassen geprüft worden. Kein Unternehmen hat die VAIT erfüllt. Schwerwiegende Feststellungen gab es insbesondere in den Bereichen Informationssicherheits- und Informationsrisikomanagement. Dieses deckt sich auch mit den Erfahrungen, die wir mit unseren Kunden gesammelt haben (siehe Abbildung 1).

prüfungsschwerpunkte und korrekturaufwand

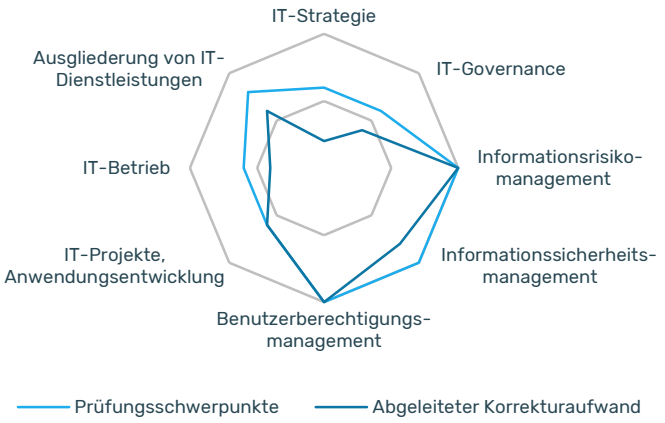


Abbildung 1: Prüfungsschwerpunkte und Korrekturaufwand VAIT

Prüfungsgebiete mit kritischen Schwachstellen:

- Informationssicherheitsmanagement
- Informationsrisikomanagement
- Benutzerberechtigungsmanagement und
- Ausgliederung von IT-Dienstleistungen

Dabei trifft es die einzelnen Disziplinen nicht singulär, sondern auch in ihrem wirksamen Zusammenspiel. Die VAIT bezieht sich nicht nur auf die IT, sondern ist ein übergreifendes Thema, in dem die Fachbereiche genauso betroffen sind. Beide müssen in der Umsetzung der VAIT gemeinsam handeln.

von der regulatorischen anforderung zur operativen chance

Viele Versicherungsunternehmen sehen in der VAIT weiterhin „nur“ eine regulatorische Anforderung, ihre IT risikooptimiert auszurichten. Diese Umsetzung wird häufig als Pflicht empfunden, bei der die Chancen-Seite häufig nicht betrachtet wird.

Zielführender ist der Ansatz, die Disziplinen der VAIT an den strategischen Zielen zu orientieren, deren Mehrwert für das Unternehmen zu analysieren, um dadurch in der Umsetzung zusätzliche Geschäfts- und Optimierungspotenziale zu heben.

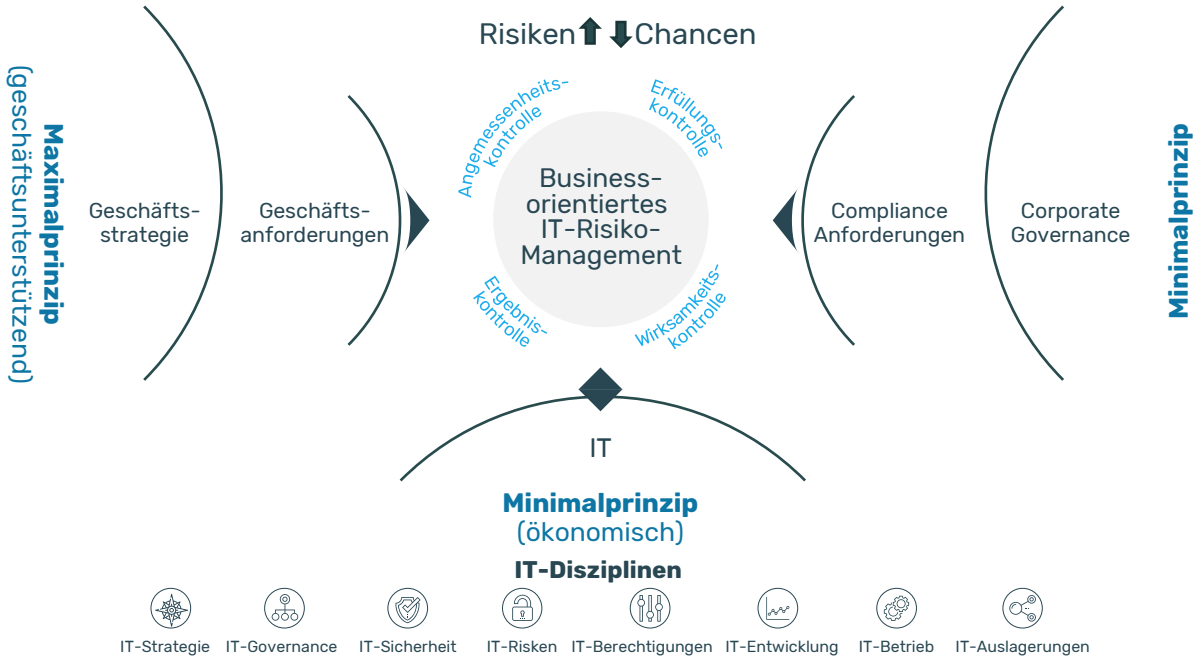


Abbildung 2: Chancen-Risiko bei der Umsetzung der VAIT

strategischer rahmen für die umsetzung der vait

Jede Maßnahme, die aus der VAIT resultiert, sollte zusätzlich auf die strategischen Ziele des Unternehmens gespiegelt werden. Somit werden zwei essenzielle Blickwinkel erreicht – eine Risikominimierung und eine Nutzenbetrachtung jeder einzelnen Maßnahme. Konkret bedeutet dies, dass ausgehend von der Geschäftsstrategie die wesentlichen Zielsetzungen eines Unternehmens (z.B. Steuerungsfähigkeit, Wachstum, Kosten, Qualität und Risiken) abgeleitet werden.

Parallel dazu werden die Lücken aus der Prüfung der VAIT als notwendige Ausprägung bewertet und in einem Maßnahmenkatalog verdichtet. Jede Maßnahme sollte eine klare Unterstützung zu einem dieser Ziele herstellen können. In diesem Fall ist eine zielgerichtete, effiziente und effektive Umsetzung der VAIT für Ihr Unternehmen möglich.

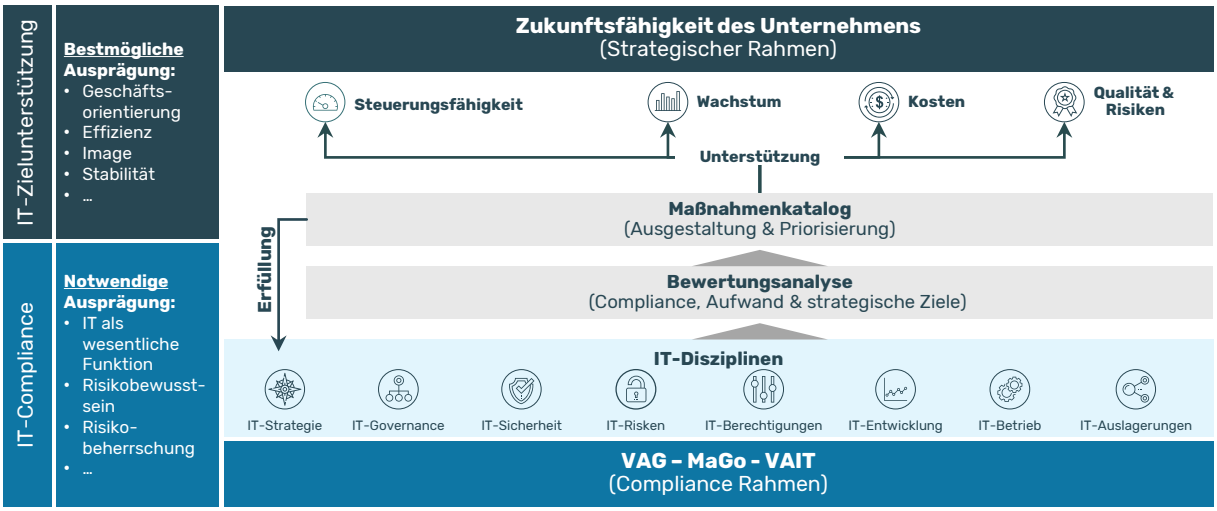
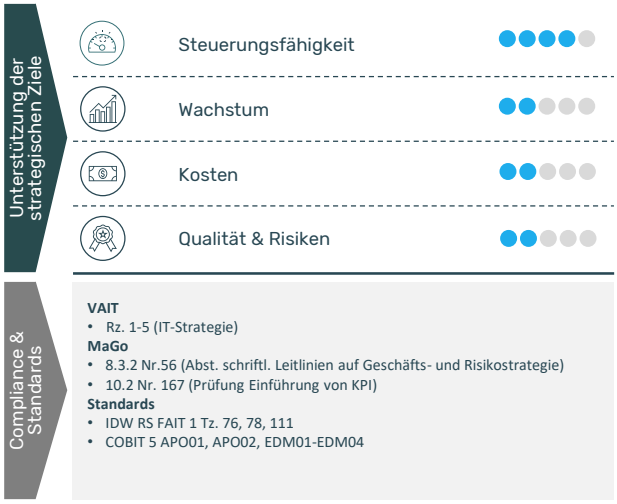


Abbildung 3: Strategischer Rahmen zur Umsetzung und Erfüllung der VAIT

sieben beispiele für die chancenorientierte umsetzung

transparenz herstellen
it-strategie

In Prüfungen wird die fehlende oder unzureichende IT-Strategie beanstandet. In vielen Versicherungen wird die IT noch als Kostenfaktor gesehen. Mangelnde Transparenz über die Leistungen und Kosten der IT tun ihr Übriges. Die Chance ergreifen und eine an der Geschäftsstrategie ausgerichteten IT-Strategie ermöglicht es, den Wertbeitrag der IT deutlich zu machen. In der Ausgestaltung sind die wesentlichen Elemente IT-Organisation, IT-Prozesse, Technik, Architektur, Sourcing, Kosten und Risiken in der Reflexion zur Geschäftsstrategie zu beschreiben. Ein klarer Auftrag für die Digitalisierung wird gesetzt und es entsteht ein klares und kommunizierbares IT-Zielbild.



steuerung etablieren
it-governance

Die IT-Governance bildet einen regulatorischen Rahmen, der die IT mit der Unternehmensstrategie verzahnt. Es wird sichergestellt, dass die IT strategisch und planvoll eingesetzt wird und so die Unternehmensziele optimal und nachhaltig unterstützt. Das wesentliche Ziel der IT-Governance ist es, ganz im Sinne der VAIT, IT-Risiken zu minimieren und dazu beizutragen, den Unternehmenswert zu steigern. Sie bietet die Chance für eine organisatorisch und prozessual professionell aufgestellte IT und unterstütz das unternehmensweite IKS.

Unterstützung der strategischen Ziele

Steuerungsfähigkeit	●●●●●
Wachstum	●●●○○
Kosten	●●●○○
Qualität & Risiken	●●●●○

Compliance & Standards

VAIT:
- Rz. 6-16 (IT-Governance)

MaGo:
- 8.1 Nr. 26-38 (Aufbau- und Ablauforganisation)
- 8.2 Nr. 43-46 (Interner Überprüfung des Governance Systems)
- 8.3 Nr. 47-74 (Schriftliche Leitlinien)

Standards:
- IDW RS FAIT 78-79
- COBIT 5 APO01

vertrauen gewährleisten
informationssicherheits- & informationsrisikomanagement

In einer digitalen Gesellschaft ist das Bedürfnis nach Vertrauen des Kunden in die Services, Produkte und Leistungen des Unternehmens vorausgesetzt. Elementarer Baustein ist hier die Informationssicherheit, um sich mit den Risiken der Digitalisierung wie z.B. den Cyber- oder den Datenschutzrisiken intensiv auseinanderzusetzen. Der Kunde vertraut der Versicherung einen Großteil seiner sensibelsten Daten an. Ein etabliertes und wirksames ISMS stellt sicher, dass diese Informationen vertraulich bleiben. Hierbei wird auf existierende Standards und Normen beispielsweise die ISO 9001, zurückgegriffen.

Unterstützung der strategischen Ziele

Steuerungsfähigkeit	●●●●●
Wachstum	●○○○○
Kosten	●○○○○
Qualität & Risiken	●●●●●

Compliance & Standards

VAIT:
- Rz. 17-24 & Rz. 25-32 (Informationsrisiko- und Informationssicherheits-management)

MaGo:
- 5. Nr. 17-20 (Wesentliche Risiken)
- 10.1 Nr. 155-156 (GL im Risikomanagementsystem)
- 10.2 Nr.157-168 (Risikomanagementleitlinien)

Standards:
- IDW RS FAIT 1 Tz. 76, 77; IDW RS FAIT Tz. 21
- COBIT 5 APO12; COBIT 5 APO13
- ISO 27001

effizienzen heben
berechtigungsmanagement

Das Berechtigungsmanagement führt bei den Prüfungen immer wieder zu Beanstandungen. Ursache hierfür ist, dass dieser Bereich häufig parallel zur Anwendungsentwicklung historisch gewachsen ist und mit Einzug modernerer Technologien nicht angepasst wurde. Der Aufwand, das Berechtigungsmanagement von seiner Struktur her richtig und zukunftsfähig aufzustellen, ist erheblich, wirkt aber sehr stark auf Qualitäts- und Risikoziele. Das reibungslose und korrekte Zuordnen von Rollen und Rechten schützt das Unternehmen zusätzlich vor Angriffen von innen. Es können wesentliche prozessuale und organisatorische Effizienzen gehoben werden, wie z. B. das reibungslose On- und Off-Boarding von Mitarbeitenden und die Zusammenarbeit in verteilten (remote) Arbeitsumgebungen.

Unterstützung der strategischen Ziele

Steuerungsfähigkeit	●●●○○
Wachstum	●○○○○
Kosten	●●●○○
Qualität & Risiken	●●●●●

Compliance & Standards

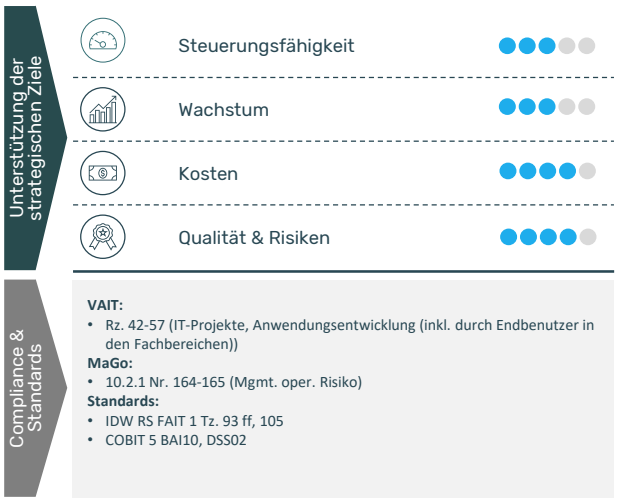
VAIT:
- Rz. 33-41 (Benutzerberechtigungsmanagement)

MaGo:
- 8.1.3 Nr. 29-30 (Trennung Zuständigkeiten)
- 9.3.3 Nr. 102 (Koord. der Berechnung vers.-math. Funktionen - Funktionstrennung)

Standards:
- IDW RS FAIT 1 Tz. 81, 82, 84, 106, 109
- COBIT 5 DSS01, DSS05
- ISO 27001 A.9

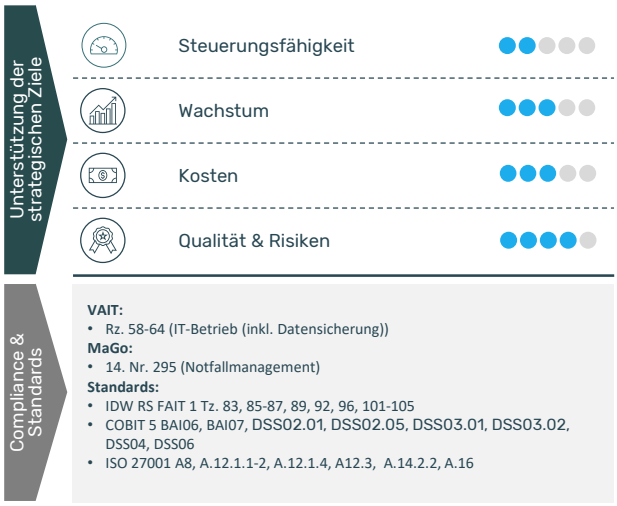
professionalisierung erreichen
it-projekte und anwendungsentwicklung

Der Druck auf die Systemlandschaft der meisten Versicherungen ist enorm. Ein Großteil der Versicherer steht vor grundlegenden Veränderungen ihrer Systemlandschaft und damit vor großen Herausforderungen. Diesen Herausforderungen kann nur durch professionelles Projekt- und Portfoliomanagement begegnet werden, denn die Risiken eines Scheiterns sind finanziell, operativ wie strategisch enorm. Ebenso wichtig ist es, Anwendungen und Systeme schnell, kostengünstig und mit hoher Qualität bereitzustellen. Die Prozesse der Anwendungsentwicklung müssen daher auch im Hinblick auf neue Methoden weiterentwickelt werden.



stabilität garantieren
it-betrieb

Ein reibungsloser, störungsfreier IT-Betrieb ist eine entscheidende Voraussetzung für die Geschäftsabwicklung und somit die operative Stabilität einer Versicherung. Eine Störung im IT-Betrieb hat erhebliche Auswirkungen auf Kunden, Partner und die gesamte Organisation. Eine komplexe Herausforderung, um dies zu gewährleisten, muss der IT-Betrieb entsprechend organisiert sein. Dies wird mit standardisierten Prozessen bzw. Prozessmodellen erreicht sowie klaren Zuordnungen von Kompetenzen und Verantwortlichkeiten. Mit Einführung von modernen Betriebsmodellen wie z.B. DevOps wird die Möglichkeit geschaffen, Innovationen schneller umzusetzen. Eine klare Kostendegression ist ein zusätzlicher Nutzeneffekt.



skalierbarkeit sicherstellen
ausgliederung von it-dienstleistungen

Die Konzentration auf das Kerngeschäft in Verbindung mit einer steigenden Flexibilität in den Produkten und Dienstleistungen stabilisieren das Geschäftsmodell jeder Versicherung und stellen die Anschlussfähigkeit für die Zukunft sicher. Das effiziente Steuern der Dienstleister steht hierbei im Mittelpunkt, um Kostenexplosionen, mangelnde Transparenz und schlechte Qualität zu vermeiden. Um dies zu gewährleisten, bedarf es eines effizienten und regulatorisch konformen Steuerungsprozesses von Dienstleistern und Partnern.

ausblick: was kommt als nächstes in der vait

Nachdem die BaFin die VAIT bereits um das KRITIS-Modul ergänzt hat, werden sicherlich auch in der Zukunft die in der BAIT formulierten Auflagen in die VAIT übernommen werden. Auch hier wird es wieder einen wesentlichen Anpassungsbedarf für die Versicherungsunternehmen geben. Als Ausblick könnten hier die bereits anvisierten Themen „Operative Informationssicherheit“ und „IT-Notfallmanagement“ in die VAIT überführt werden.

cyberabwehr stärken
operative informationssicherheit

Die operative Informationssicherheit setzt die Anforderungen des Informationssicherheitsmanagements in der IT um.

Hier kommt es zu einer Konkretisierung des ISM, der Anforderungen auf der Technologieebene. Dies umfasst neben klassischen Themen wie Schwachstellenmanagement, Netzwerksegmentierung, Systemhärtung, Verschlüsselung und Perimeterschutz einen proaktiven Überwachungsmechanismus mit den dazugehörigen Prozessen, um frühzeitig Gefährdungen zu erkennen und zeitnah (idealerweise direkt) reagieren zu können (bspw. durch ein SOC – Security Operation Center). Durch diese Vorgaben soll die Robustheit der Versicherungsunternehmen gegenüber Cyber-Risiken gesteigert werden.

krisen managen
it-notfallmanagement

Versicherungsunternehmen haben Ziele zum Notfallmanagement zu definieren und hieraus abgeleitet einen Notfallmanagementprozess festzulegen. Für Notfälle in zeitkritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept).

Auch hier erfolgt eine weitere Konkretisierung der Anforderungen für die Technologien und Prozesse in der IT. Maßnahmen zur IT-Notfallplanung werden nicht nur seit der aktuellen Pandemie zunehmend wichtiger und unterstützen die Aufrechterhaltung des Geschäftsbetriebes in Folge einer Krise. Eine angemessene Vorbereitung und regelmäßige Übungen zu möglichen (IT-)Notfallszenarien ist essenzieller Bestandteil eines wirksamen Business Continuity Managements und senkt somit Risiken.

plenum - profitieren sie von unseren erfahrungen

Unser Anspruch ist es, nachhaltige und wirksame Lösungen für Sie zu schaffen

- Wir verfügen über mehr als 30 Jahre Erfahrung in der Versicherungswirtschaft und verstehen uns als Partner unserer Kunden
- Wir kennen die Anforderungen der BaFin und wissen welche Maßnahmen notwendig sind – wir kennen aber auch die Gestaltungsspielräume
- Wir bieten exzellente Berater, die in allen Prüfungsfeldern der VAIT die regulatorische und praktische Umsetzungserfahrung bereitstellen
- Wir schaffen gemeinsam mit unseren Kunden, die Risiken zu steuern bei gleichzeitiger Hebung der Geschäftschancen

unsere themen

informationssicherheit
Wir etablieren und optimieren Ihr ISMS und orientieren uns dabei an ISO 27001 und dem IT-Grundschutz.

digital governance
Für Ihre Digitalstrategie erarbeiten wir mit Ihnen Entscheidungsstrukturen, die alle Stakeholder zusammenführen.

datenschutz
Mit einem wirksamen Datenschutzmanagement unterstützen wir Sie, die Anforderungen der DSGVO effizient umzusetzen.

compliance management
Wir unterstützen Sie in der Erfüllung der Vorgaben zu IT-Risiken und berücksichtigen dabei auch die strategischen Ziele.

berechtigugs-management (IAM)
Durch ein IAM stellen wir mit Ihnen sicher, dass nur Berechtigte mit Daten und Systemen interagieren.

integrierte managementsysteme
Wir verzahnen Ihre Managementsysteme des ISMS, des DSM, der Auslagerungen und der BCM zu einem effizienten Ganzen.

business continuity management
Wir stellen mit Ihnen sicher, dass ein wirksames BCM auf Basis ISO 22301 etabliert ist.

auslagerungs compliance
Wir stellen mit Ihnen ein Auslagerungsmanagement sicher, dass die Vorgaben einhält und Ihre Risiken minimiert.

plenum AG
Management Consulting
THE SQUAIRE WEST 15 | Am Flughafen | D-60549 Frankfurt am Main
Telefon: +49 69 6435524-0 | Fax: +49 69 6435524-60 | Internet: www.plenum.de