VAIT-Assessment: von der gesetzlichen Pflicht zum Wettbewerbsvorteil

The world is how we shape it

sopra steria

VAIT: Chancen für einen stabilen IT-Betrieb

Nahezu alle Geschäftsprozesse von Versicherern laufen IT-basiert ab. Das bedeutet: Bei einem Ausfall oder einer Störung der IT wäre der Versicherungsbetrieb praktisch lahmgelegt. Manuelle Verfahren sind längst keine Alternative mehr. Beeinträchtigungen der IT wirken sich daher absolut geschäftskritisch für einen Versicherer aus, im schlimmsten Fall ist die Existenz bedroht.

Als Beeinträchtigung der IT gelten nicht nur ein meist schnell bemerkter Serverausfall, sondern auch das oft gar nicht oder sehr spät entdeckte Ausspähen von Daten sowie die fahrlässige oder kriminell motivierte Sabotage der IT-Infrastruktur. Weil Versicherer durch die Digitalisierung der Prozesse aber mehr Systeme einsetzen und die IT-Landschaft komplexer wird, wächst die Wahrscheinlichkeit, dass es zu Störungen und Ausfällen kommt.

Mit den Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) rückt die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) daher den kontrollierten und sicheren Einsatz von IT in den Fokus. Die VAIT regeln die Ausgestaltung der IT-Systeme sowie die dazugehörigen Prozesse.

Die Umsetzung von Regularien wird von vielen Versicherern a priori als leidige Pflicht gesehen – das ist auch bei den VAIT oft so. Klug umgesetzt, bieten die VAIT aber auch Chancen: Mit den VAIT gibt die BaFin den Versicherern nämlich ein Regelwerk mit zu erfüllenden Anforderungen an die Hand. Die VAIT regeln dabei auch, wie Versicherer beispielsweise mit den IT-Dienstleistungen von Drittanbietern umgehen, die viele Versicherungsunternehmen zunehmend in Anspruch nehmen. Diese Entwicklung erfordert zwingend eine Risikoanalyse.

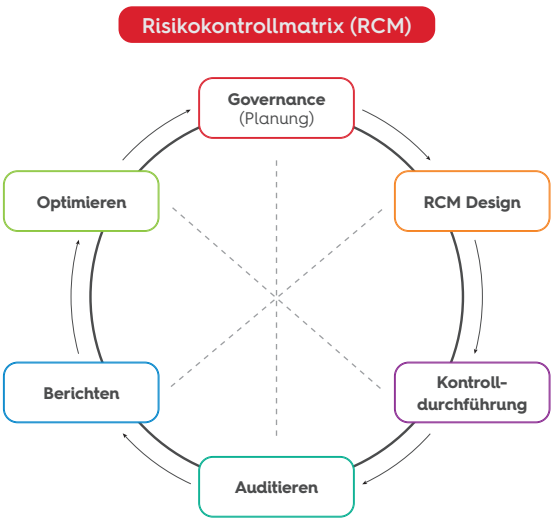
Die Versicherer können diese Vorgaben für sich nutzen, indem sie die VAIT als Grundlage und als Leitplanken für die Gestaltung ihrer IT nutzen. Auf diese Weise können sie Effizienz und Sicherheit signifikant verbessern. Geschickt umgesetzt, haben Versicherer hier eine Chance ein eine kontrollierte Softwareentwicklung, einen stabilen IT-Betrieb und ein effektives Informationssicherheitsmanagement aufzubauen und sich damit Wettbewerbsvorteile verschaffen.

Jetzt mit der Umsetzung starten!

Die VAIT fordert von den Versicherern ein generelles Nachbessern bei den eigenen Strukturen und der Sicherheit. Es geht dabei vor allem um eine Präzisierung und Konkretisierung bestehender Anforderungen an die Geschäftsorganisation, wie sie beispielsweise die Paragrafen 23 bis 34 des Versicherungsaufsichtsgesetzes (VAG) definieren. Die Berücksichtigung dieser gesetzlichen Anforderungen zur IT-Compliance ist obligatorisch.

Die Chance für Versicherer besteht darin, diese Pflicht für Schaffung einer erhöhten Transparenz durch ein umfassenderes VAIT Assessment zu nutzen. Es empfiehlt sich eine vollständige Analyse und Bewertung des Status quo, um Defizite und Risiken in der IT aufzudecken, die über das geforderte Maß hinausgehen. Versicherer können so Handlungsfelder risikoorientiert priorisieren und daraus einen spezifischen Maßnahmenplan ableiten. Wichtig ist, weitere aktuelle regulatorische Vorgaben im Blick zu behalten, so lassen sich Synergien nutzen und Mehrfacharbeiten vermeiden.

Module und Ziele der VAIT auf einen Blick



Was ist eine RCM?

- Menge organisatorischer Maßnahmen und Kontrollen
- Ziel ist die Steuerung der Einhaltung von Compliance-Anforderungen

Welche Informationen beinhaltet eine Risikokontrollmatrix typischerweise? Sie beschreibt:

- Welche Risiken es gibt
- Welche Ziele erreicht werden sollen
- Was und wie kontrolliert werden soll
- Wer und wie oft kontrollieren soll
- Wie man die Kontrollen nachweist

Ergebnisse/Resultate

- Erhöhte Transparenz der Risiken
- Technische und organisatorische Maßnahmen, um Risiken zu behandeln und dadurch compliant zu sein
- Geeignete Nachweise für das Bestehen eines Audits
- Ergebnisse von Prüfungen (Auditberichte)
- Risikobeurteilung bei Abweichungen
- Nachweis kontinuierlicher Kontrollen durch Audits
- Ursachenanalyse und Empfehlungen bei Kontrollschwächen

Unser Vorgehen: laufende, aktive Steuerung regulatorischer Vorschriften

1	2	3	4	5
Sammlung	**Konsolidierung**	**GAP-Analyse**	**Arbeitspakete**	**Umsetzung**
Sammlung von Anforderungen und Zerlegung in Einzelanforderungen	Identifikation der Überdeckungen und Synergien	Aufdeckung von Lücken zwischen Soll und Ist	Ableitung konkreter Maßnahmen, um identifizierte Lücken zu schließen	Umsetzung der abgeleiteten Arbeitspakete

Durch den Einsatz einer Risikokontrollmatrix und ihre Einbindung in das interne Kontrollsystem, können auch regulatorische Anforderungen über die VAIT hinaus gesteuert werden.

Unser Ansatz: Ganzheitliche IT Compliance orientiert sich an der Sichtweise eines IT-Prüfers

Um für eine ganzheitliche IT Compliance zu sorgen, nutzen wir eine sogenannte Risikokontrollmatrix. Sie lässt sich speziell auf die VAIT-Anforderungen zuschneiden. Besser ist, sie gleich für die Steuerung sämtlicher regulatorischer Anforderungen an die IT einzusetzen.

Im ersten Schritt werden dafür alle Regularien gesammelt, anschließend Synergien und Überschneidungen aufgezeigt. So halten Versicherer den Aufwand für die Erstellung von Nachweisen möglichst gering. Mithilfe einer Reifegradanalyse lässt sich der Umsetzungsstand dokumentieren. Anschließend bewerten wir mit Ihnen festgestellte Lücken und legen passende Maßnahmen für deren Behebung fest.

Über das Projekt hinaus empfiehlt sich, ein aktives Management durch ein übergeordnetes Steuerungssystem einzuführen. So sorgen Sie auch für eine kontinuierliche IT Compliance und beginnen ständig wieder bei bei null.

Unsere Leistungen – Ihr Nutzen

Versicherer profitieren von unserem Mix aus Prozess-Know-how sowie technologischer und fachlicher Kompetenz.

- Sopra Steria zeigt Ihnen, welche Chancen sich in jedem VAIT-Themenumfeld ergeben
- Mit unseren eigens für die VAIT entwickelten Methoden erfassen wir die Ist-Lage
- Wir identifizieren mögliche Schwächen bei der Umsetzung anderer Regularien mit Bezug auf die VAIT
- Wir bestimmen gemeinsam den Handlungsbedarf für die Umsetzung der VAIT und identifizieren Potenziale für Prozessverbesserung und Automatisierung
- Wir erarbeiten mit Ihnen eine Roadmap und priorisieren die Maßnahmen nach Risikolage
- Unsere Vorgehensweise orientiert sich an der Sichtweise eines IT-Prüfers
- Wir begleiten Sie nach Bedarf bei der Vorbereitung auf eine mögliche BaFin-Prüfung und bei der Prüfung selbst
- Auf Wunsch unterstützen wir Sie bei der Umsetzung der Maßnahmen und geben Ihnen Hinweise, wie Sie Ihre Compliance langfristig erhalten

Über Sopra Steria

Als ein führender europäischer Management- und Technologieberater unterstützt Sopra Steria mit 46.000 Mitarbeiterinnen und Mitarbeitern in 25 Ländern seine Kunden dabei, die digitale Transformation voranzutreiben und konkrete und nachhaltige Ergebnisse zu erzielen. Sopra Steria bietet mit Beratung, Digitalisierung und Softwareentwicklung umfassende End-to-End-Lösungen, die große Unternehmen und Behörden wettbewerbs- und leistungsfähiger machen – und zwar auf Grundlage tiefgehender Branchenexpertise, innovativer Technologien und eines kollaborativen Ansatzes. Das Unternehmen stellt die Menschen in den Mittelpunkt seines Handelns mit dem Ziel, digitale Technologien optimal zu nutzen und eine positive Zukunft für seine Kunden zu gestalten.

The world is how we shape it

10135

Sopra Steria SE
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
insurance.de@soprasteria.com
www.soprasteria.de

sopra steria