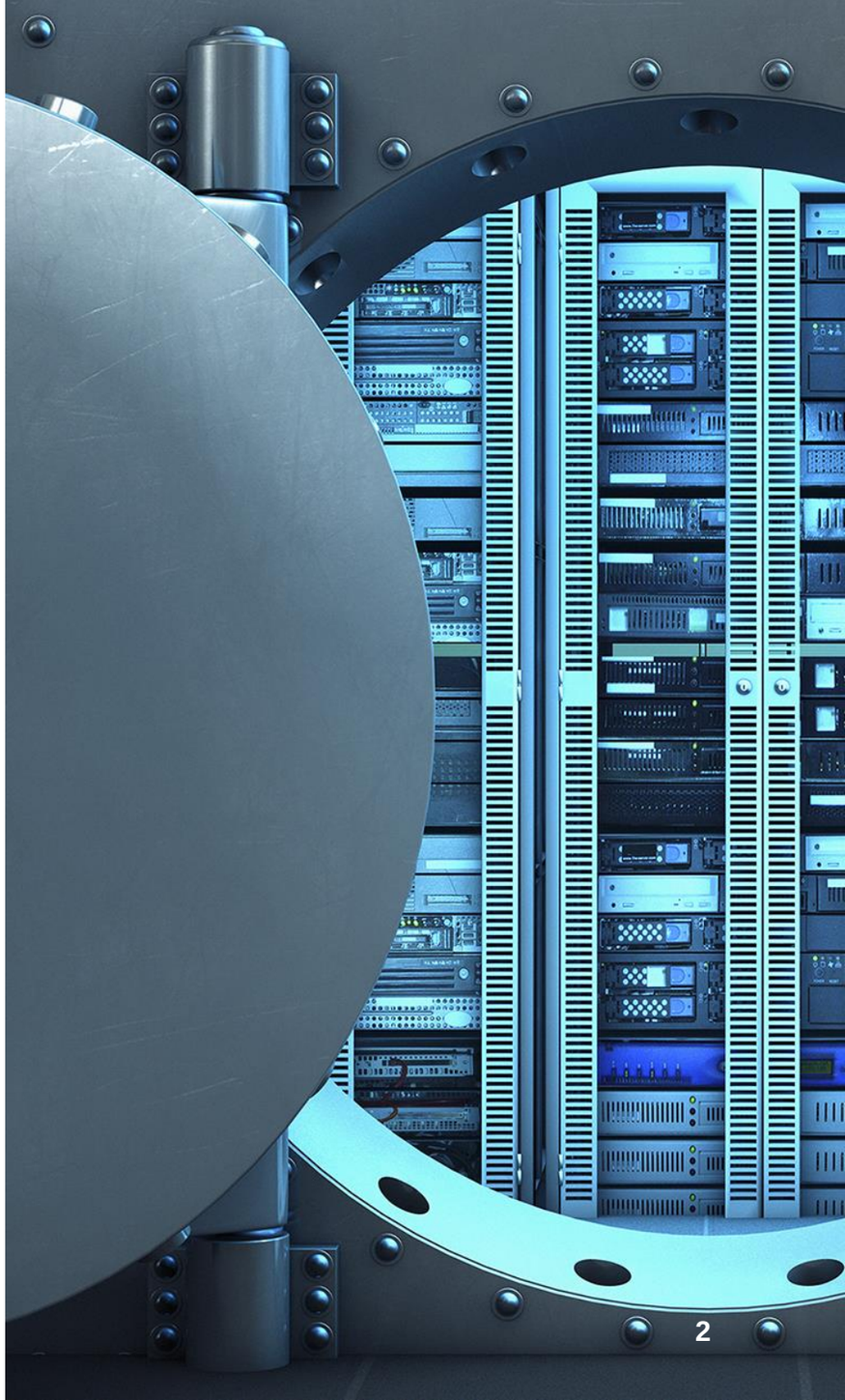
TaylorWessing

Das überarbeitete VAIT-Rundschreiben der BaFin

Taylor Wessing Insurance Day München

Ingo Vinck | 23. Juni 2022

Inhalt



1 Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

- Die **Versicherungsaufsichtlichen Anforderungen an die IT**, abgekürzt **VAIT**, sind Verwaltungsanweisungen der Bundesanstalt für Finanzdienstleitungsaufsicht (BaFin) für die sichere Ausgestaltung der IT-Systeme, der dazugehörigen Prozesse und die Anforderungen an die IT-Governance.
- Rundschreiben 10/2018 (VA) der BaFin (**Rundschreiben**) vom 2. Juli 2018 der BaFin.
- Eine Aktualisierung des Rundschreibens 10/2018 ist am 3. März 2022 in Kraft getreten.
- Anwendungsbereich: Gilt für alle Versicherungsunternehmen, die nach § 1 Abs. 1 VAG der Versicherungsaufsicht unterfallen.
- Das Rundschreiben konkretisiert die §§ 23 ff. VAG, also die versicherungsaufsichtsrechtlichen Anforderungen an die Geschäftsorganisation von Versicherungsunternehmen.

- Das Rundschreiben tritt neben das Rundschreiben 02/2017 *Aufsichtsrechtliche Mindestanforderungen an die Geschäfts-organisation von Versicherungsunternehmen* (MaGo) und konkretisiert dieses.
- Das überarbeitete Rundschreiben formuliert erstmals ganz neue Anforderungen in puncto **operative Informations-sicherheit** und **IT-Notfallmanagement**. Bestehende Anforderungen werden erweitert.
- Darüber hinaus besteht bei der Umsetzung konkreter Handlungsbedarf

Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

- **IT-Strategie:** Strategiepapier über Ziele und Maßnahmen zur Zielerreichung, strategische Entwicklung der IT
- **IT-Governance:** Steuerung und Überwachung des Betriebs und der IT-Systeme auf Basis der IT-Strategie
- **Informationsrisikomanagement:** Definition von Aufgaben, Kompetenzen, Verantwortlichkeiten und Kontrollen; Schutzbedarfsanalyse
- **Informationssicherheitsmanagement:** Geschäftsleitung formuliert Informationssicherheitsleitlinie, Informationssicherheitsbeauftragter, Sensibilisierungs- und Schulungsprogram für IT-Sicherheit
- **NEU: Operative Informationssicherheit:** Implementierung operativer IT-Sicherheitsmaßnahmen im Tagesgeschäft (u.a. Schwachstellenmanagement, Segmentierung und Kontrolle des Netzwerks, sichere Konfiguration der Endgeräte, Verschlüsselung)
- **Identitäts- und Rechtemanagement:** Zugriffs- und Zugangsrechte, jede Berechtigung muss einer handelnden oder verantwortlichen Person zugeordnet sein

- **IT-Projekte und Anwendungsentwicklung:** Analyse der Auswirkung geplanter Veränderungen
- **IT-Betrieb:** Verwaltung der IT, Aktualisierung von Software
- **Ausgliederungen von IT-Dienstleistungen** und sonstigen Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen
- **NEU: IT-Notfallmanagement:** IT-Notfallpläne für technische Ausfälle; Notfallpläne sind für alle IT-Systeme mit zeitkritischen Abläufen zu erstellen; jährliche Notfalltests, Nachweis für ausreichend langen Notbetrieb aus anderem Rechenzentrum
- **Kritische Infrastrukturen:** richtet sich an Betreiber kritischer Infrastrukturen

2 | Handlungsbedarf für Versicherungsunternehmen

TaylorWessing

Cyberrisiken im Focus der BaFin

- Die BaFin geht davon aus, dass Cyberrisiken weiter zunehmen.
- Für die BaFin ist daher von entscheidender Bedeutung, wie sich Banken, Versicherer und andere Unternehmen des Finanzmarktes vor Cyberangriffen und internen Vorfällen schützen.
- Die Prüfung der IT-Sicherheit bei Versicherern steht damit im Focus der BaFin. Die BaFin beabsichtigt gerade im Hinblick auf die IT-Sicherheit zu prüfen.
- BaFin prüft seit 2018
- Prüfung in der Regel mehrere Wochen mit mehreren IT-Prüfern. Am Ende der Prüfung Bericht/Prüfungsurteil

Wie die BaFin vorgeht

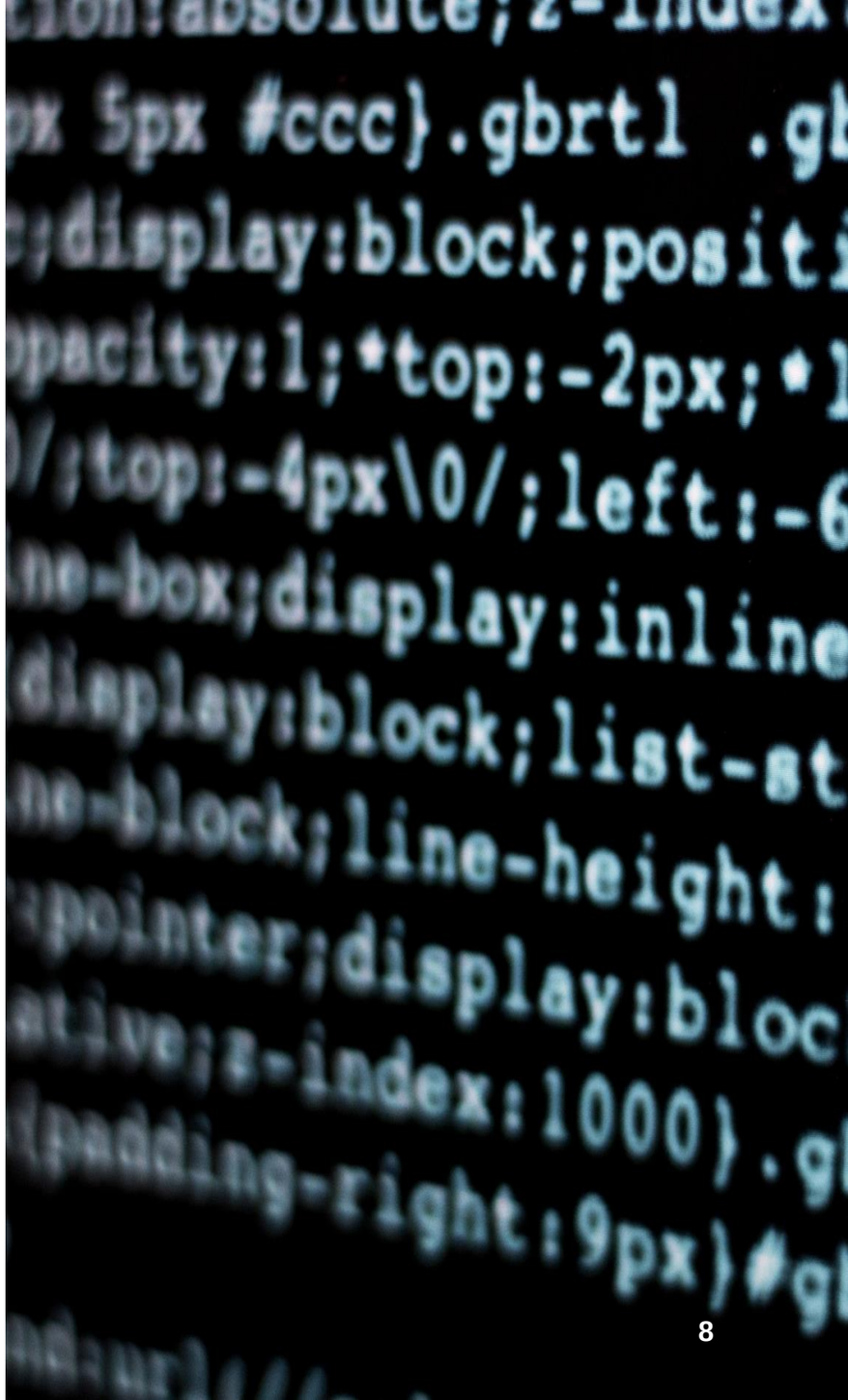
- *„Die BaFin wird sich auch im Jahr 2022 intensiv mit Cyberrisiken befassen und dazu unter anderem verstärkt dezidierte IT-Prüfungen bei den Instituten und Unternehmen vornehmen. Abhängig von den Ergebnissen wird sie weiteren Handlungsbedarf ableiten.“*
- *„Auch bei der laufenden operativen Aufsicht wird die BaFin Aspekte der IT-Sicherheit und die Einhaltung aufsichtlicher IT-Anforderungen verstärkt überprüfen. Wenn erforderlich, wird sie die Einhaltung der Standards durchsetzen.“*

(Risiken im Focus der BaFin, März 2022, Seite 17)

Handlungsbedarf für Versicherungsunternehmen

- Aus aktualisierten VAIT und Focus der BaFin auf Cyberrisiken und IT-Sicherheit folgt konkreter Handlungsbedarf für Versicherungsunternehmen.
- VAIT sind bei der Geschäftsleitung verortet: Verantwortlich ist Gesamtgeschäftsführung.
- Bestandsaufnahme und Umsetzung erfordern Zusammenarbeit von verschiedenen Funktionen (z.B. Vorstand, IT, Recht).

- **Proportionalitätsprinzip:** Umsetzung knüpft an individuelles Risikoprofil an. Beispiel: Geringe Größe des Unternehmens kann Indikator für schwächer ausgeprägtes Risikoprofil sein, d.h. einfachere IT-Systeme oder Prozesse (Rundschreiben, Vorbemerkung Ziffer 7 ff.).
- Proportionalitätsprinzip führt zu Gestaltungsspielraum und Rechts-unsicherheit.
- Typsicherweise Handlungsbedarf z.B. bei **Informationssicherheitsmanagement**, **Berechtigungsmanagement**, **Ausgliederung**, auch bei **Dokumentation** und **Ausgliederungs-verträgen.**



Handlungsbedarf für Versicherer
Beispiele

- **IT-Governance**: Fehlende Richtlinien, unübersichtliche Sharepoints
- **Informationsrisikomanagement**: Häufig ein Prüfungsschwerpunkt der BaFin
- **Informationssicherheitsmanagement**: Sicherheitsrichtlinie häufig unvollständig
- **Berechtigungsmanagement:** Aus Sicht der BaFin häufig mangelhafte oder veraltete Berechtigungskonzepte

Häufiger Handlungsbedarf beim Informationsrisikomanagement:

- Im Risikomanagement keine Berücksichtigung der gesamten risikorelevanten IT
- Keine ausreichende Berücksichtigung des ermittelten Schutzbedarfs
- Es wird auf Sicherheitsmaßnahmen verzichtet, ohne die sich auf dem Verzicht ergebenden Risiken zu analysieren

Handlungsbedarf für Versicherer **Dokumentation**

- Die VAIT betreffen nicht nur die IT, sondern auch die IT-betreffende interne Dokumentation.
- Im Verhältnis zur BaFin kommt der schriftlichen Dokumentation eine besondere Bedeutung zu, besonders im Hinblick auf die Gesamtverantwortung der Geschäftsleitung.
- Aktualisierung der IT-Dokumentationen bedeutet auch die persönlichen Haftungsrisiken des Vorstandes zu reduzieren.
- Seit Inkrafttreten des überarbeiteten VAIT-Rundschreibens am 3. März 2022 ist die bisherige Dokumentation nicht mehr aktuell.

Beispiele für Anpassungsbedarf im IT-Strategiepapier:

- **IT-Strategiepapier ü**berhaupt vorhanden?
- **IT-Strategiepapier** vom Vorstand verabschiedet?
- **IT-Strategiepapier** dem Aufsichtsrat vorgelegt?
- Mindestinhalt abgedeckt?
- Überprüfbare Ziele formuliert?
- Ausgliederung berücksichtigt?

Handlungsbedarf für Versicherer **Ausgliederung**

- Jedes Versicherungsunternehmen kann Funktionen und Versicherungstätigkeiten ausgliedern. Beim Outsourcing muss aber die Erfüllung aller aufsichtsrechtlichen Anforderungen gewährleistet bleiben. Die Letztverantwortung für die ausgegliederte Funktionen verbleibt bei dem ausgliedernden Versicherungsunternehmen und dessen Geschäftsleitung (vgl. § 32 Abs. 1 VAG)
- § 32 Abs. 2 Satz 1 VAG: Prüfungs- und Kontrollrechte der BaFin dürfen durch die Ausgliederung nicht beeinträchtigt werden. Das ausgliedernde Unternehmen hat hinsichtlich der von der Ausgliederung betroffenen Funktionen sicherzustellen, dass
  - das Unternehmen selbst, seine Abschlussprüfer und die Aufsichtsbehörde auf alle Daten zugreifen können,
  - der Dienstleister mit der Aufsichtsbehörde zusammenarbeitet und
  - die Aufsichtsbehörde Zugangsrechte zu den Räumen des Dienstleisters erhält, die sie selbst oder durch Dritte ausüben kann.
- § 32 Abs. 4 Satz 1 VAG: Das ausgliedernde Versicherungsunternehmen hat sich die erforderlichen Auskunfts- und Weisungsrechte vertraglich zu sichern
- *„Unternehmen haben auch bei Ausgliederungen an IT-Dienstleister durch angemessene Regelungen in der Ausgliederungsvereinbarung die Einhaltung der Anforderungen aus diesem Rundschreiben durch den IT-Dienstleister sicherzustellen.“* (BaFin Rundschreiben 10/2018 (VA) vom 3. März 2022, Vorbemerkung Ziffer 5)
- BaFin moniert häufig **fehlende oder mangelhafte Risikoanalyse** und, dass Versicherungsunternehmen **keinen Überblick** über Ausgliederungen haben.
- Bestehende IT-Outsourcing-Verträge sind nun anzupassen, da vertragliche IT-Dienstleistung den geänderten Anforderungen entsprechen muss (z.B. sind **operative Informationssicherheit** und **IT-Notfall-Management** einzuarbeiten).

Ihr Ansprechpartner

Ingo Vinck berät Versicherungs- und Rückversicherungsunternehmen bei M&A- und anderen Transaktionen, d.h. beim Erwerb und der Veräußerung von Geschäftsanteilen oder Versicherungsbeständen, bei der Gründung von Versicherungsunternehmen und deren (Niederlassungen) in Deutschland sowie bei der Abwicklung von Beständen und bei Outsourcings.

Darüber hinaus beurteilt er Haftungsszenarien für Führungskräfte im Zusammenhang mit der Organhaftpflichtversicherung (D&O). Herr Vinck hat besondere Expertise im Handels- und Gesellschaftsrecht, einschließlich Joint-Venture-Gesellschaften, M&A und Technologietransfer mit besonderem Fokus auf China.

Sprachen: Deutsch, Chinesisch, Spanisch und Englisch

Ingo Vinck

Senior Associate
Beijing Office

+49 211 8387137
i.vinck@taylorwessing.com

Europa > Mittlerer Osten > Asien

taylorwessing.com