plenum

versicherungen

vait – novellierung 2021

nach der VAIT ist vor der konsultation
- neuigkeiten von der BaFin -

grundlagen und motivation

Am 17.08.2021 hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) das novellierte Rundschreiben „Versicherungsaufsichtliche Anforderungen an die IT“ (VAIT) zur öffentlichen Konsultation gestellt. Anlass der Novellierung sind die von der Europäischen Versicherungsaufsichtsbehörde (EIOPA) im Oktober 2020 veröffentlichten „EIOPA Leitlinien zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie“ (ICT-Guidelines). Diese definieren einheitliche Anforderungen an das Management von Informationstechnik und -sicherheit für Versicherungen. Durch die Ergänzungen und Aktualisierungen soll die VAIT den europäischen Anforderungen, insbesondere hinsichtlich aktueller Risiken der Unternehmen im Zusammenhang mit der Informationsverarbeitung, gerecht werden. Die Veröffentlichung der finalen VAIT wird im ersten Quartal 2022 erwartet. Dabei ist mit der Wirksamkeit bzw. dem Umsetzungszeitraum der Anforderungen sofort ab Veröffentlichung zu rechnen, da die inhaltliche Basis von der BaFin als bekannt vorausgesetzt wird.

die kapitel der novellierten vait

1. IT-Strategie
2. IT-Governance
3. Informationsrisiko-management
4. Informationssicherheits-management
5. Operative Informations-sicherheit NEU
6. Identitäts- und Rechte-management
7. IT-Projekte und Anwendungsentwicklung
8. IT-Betrieb
9. Ausgliederungen von IT-Dienstleist. und sonstige Dienstl.-Beziehungen
10. IT-Notfallmanagement NEU
11. Kritische Infrastrukturen

Abb. 1: Die Kapitel der novellierten VAIT

gesamtbetrachtung der kapiteländerungen

Die VAIT-Novelle umfasst die beiden zusätzlichen Kapitel „operative Informationssicherheit“ und „IT-Notfallmanagement“. Mit dem Kapitel „operative Informationssicherheit“ zielt die BaFin auf die Stärkung der operativen Widerstandsfähigkeit der IT ab. Es steht in engem Zusammenhang mit den Kapiteln „Informationsrisikomanagement“ sowie „Informationssicherheitsmanagement“ und ist als Abgrenzung der entsprechenden Aufgaben der ersten Verteidigungslinie (1st LoD) im Rahmen des Modells der drei Verteidigungslinien (3 LoD Modells) zu betrachten. Das Kapitel „IT-Notfallmanagement“ verschärft die Vorsorge sowie die Maßnahmen bei IT-Notfällen. Es beinhaltet konkrete Vorgaben zu Konzepten, Plänen sowie deren Prüfung und Übung. Damit wird im Schulterschluss mit dem fachlichen Business Continuity Management (BCM) die systematische Gewährleistung der Wiederherstellbarkeit der IT vorgeschrieben.

Acht weitere, bereits bestehende Kapitel wurden inhaltlich geändert bzw. ergänzt. Basis der Änderungen und Ergänzungen sind auch, neben den ICT-Guidelines, von der BaFin in Prüfungen ermittelte Defizite (Prüfungs-feststellungen) sowie punktuell erforderliche, explizitere bzw. detailliertere Vorgaben. Das Kapitel „kritische Infrastrukturen“ ist unverändert geblieben.

strukturelle änderungen

Die VAIT wurden auch strukturell novelliert. Da die zwei neuen Kapitel eingefügt und nicht angehängt wurden, ergibt sich eine neue Nummerierung der Gesamtabfolge. Die bisherigen, übergreifenden Randnummern wurden zugunsten eine Nummerierung innerhalb der Kapitel abgelöst, was eine klare Themenzuordnung ermöglicht. Die Überschriften der Kapitel 6, 7 und 9 wurden textuell angepasst, so dass sie deren Anforderungsinhalt bzw. -intention besser widerspiegeln.

ausmaß und wesentliche inhalte der änderungen im überblick

anpassungsbedarfe für die versicherungsunternehmen

Die VAIT-Ergänzungen bzw. Änderungen bedeuten insgesamt einen Handlungsbedarf für Versicherungsunternehmen. Der Handlungsbedarf ergibt sich in unterschiedlichem Ausmaß aus den neuen bzw. geänderten Kapiteln und ist abhängig von der individuellen „Absprunghöhe" des Unternehmens. Insbesondere für kleine und mittlere Versicherer ist die Beachtung bzw. Ausgestaltung der Proportionalität bei der Erfüllung der Anforderungen ein zentrales Thema.

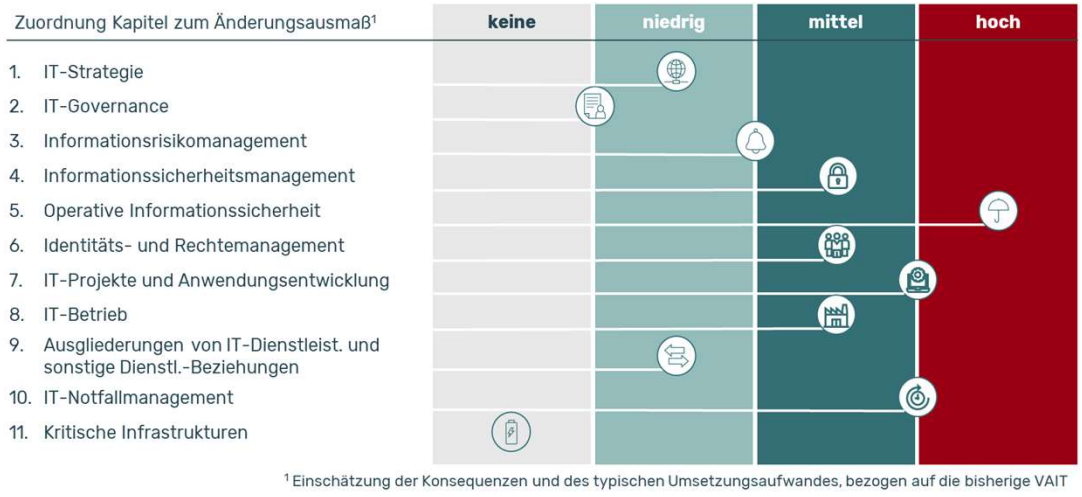

Abb. 2: Ausmaß der Änderungen im Überblick

die wichtigsten änderungen im überblick

it-strategie

Prozess zur Überwachung und Messung der Strategieziele; strategische Einordnung sonstiger, wichtiger Abhängigkeiten von Dritten; Schulungs-/Sensibilisierungsmaßnahmen zur Informationssicherheit

it-governance

Regelmäßige Überprüfung IT-Governance Vorgaben durch IT-qualifizierte Revisoren

informationsrisikomanagement

Erweiterung Informationsverbund (insb. Vernetzung mit Dritten); regelmäßige/anlassbezogene Ermittlung Schutzbedarf und Verantwortung Informationseigentümer; Überprüfung Schutzbedarfsfeststellung; Koordination/Überwachung Soll-Ist-Vergleiche; kompetenzgerechte Entscheidungen zur Risikobehandlung; Analyse Bedrohungen und Schwachstellen

informationssicherheitsmanagement

Obligatorische Inhalte Informationssicherheitsleitlinie; Richtlinien zu physischer Sicherheit und Überprüfung Informationssicherheit (Penetrationstest); Konkretisierung Aufgaben/Befugnisse ISB; Abgrenzung IS-Vorfälle, sicherheitsrelevante Ereignisse, Störungen; Festlegung/Überprüfung kontinuierliches Sensibilisierungs-/Schulungsprogramm

operative informationssicherheit

Abgrenzung operative IT-Sicherheit (1st LoD) zum ISM (2nd LoD); Informationssicherheitsmaßnahmen und -prozesse; zeitnahe, regelbasierte Identifizierung/Bewertung Bedrohungen/sicherheitsrelevante Ereignisse (SIEM) u. Analyse/Reaktion (SOC); regelm./anlassbezogene Überprüfungen Sicherheit IT-Systeme

identitäts- und rechtemanagement

Standardisierung IAM; sofortige Umsetzbarkeit Berechtigungslöschungen/-änderungen; Berücksichtigung Berechtigungen außerhalb Anwendungsebene; Protokollierung/Überwachung privilegierte Benutzer

it-projekte und anwendungsentwicklung

Umgebungstrennung Produktion/Entwicklung; organisatorische Grundlagen IT-Projekte; Change Requests, bei Auswirkungen auf Informationssicherheit mit Akzeptanz-/Testkriterien; Dokumentationstypen; Test Schutzmaßnahmen; Penetrationstest in Anwendungstests; Programmierrichtlinie IDV

it-betrieb

Neue CI-Attribute; Anforderungsstellung bei Wartungsaktivitäten; Prozess für zeitkritische Änderungen; sichere Entsorgung von Hardware; Leistungs-/Kapazitätsmanagement

ausgliederungen von it-dienstleistungen

Erhebung und Bewertung funktionale und nicht funktionale Anforderungen sonstiger Dienstleistungsbeziehungen; Berücksichtigung Vereinbarungen zum IT-Betrieb in Vertragsgestaltung für IT-Dienstleistungen

it-notfallmanagement

IT-Notfallkonzept (obligatorische Inhalte/Szenarien); Identifikation zeitkritische Aktivitäten/Prozesse via Auswirkungsanalysen (BIA); Durchführung Risikoanalysen für zeitkritische Aktivitäten/Prozesse; Maßnahmen zur Risikoreduzierung/Wiederherstellung der Prozesse; IT-Notfallpläne mit obligatorischen Inhalten; regelmäßige/anlassbezogene IT-Notfalltests; Nachweis Betriebsfähigkeit bei RZ-Ausfall (Übungen)

delta erkennen - zeit zu handeln

Auch wenn sich die novellierte VAIT noch in der Konsultation befindet, empfehlen wir eine frühzeitige Prüfung der spezifischen Auswirkungen im jeweiligen Unternehmen. Inwiefern Ihr Haus konkreten Handlungsbedarf aufweist, können Sie in einem ersten Schritt mit unserem VAIT Delta-Self Assessment ermitteln. Falls Sie eine der Fragen nicht eindeutig bejahen können, ist eine tiefergehende Analyse angebracht.

vait delta-self assessment – auszug aus dem anforderungskatalog

Ausgewählte Fragestellungen der VAIT	ja	tlw.	nein	?
1. IT-Strategie				
Ist ein Prozess zur Überwachung, Messung, Beurteilung und Anpassung der IT-Strategieziele etabliert?	☐	☐	☐	☐
Führt die IT-Strategie die sonstigen, wichtige Abhängigkeiten von Dritten mit ihrer strategischen Einordnung auf?	☐	☐	☐	☐
2. IT-Governance				
Werden die Vorgaben zur IT-Governance regelmäßig durch IT-qualifizierte Revisoren überprüft?	☐	☐	☐	☐
3. Informationsrisikomanagement				
Sind die Schutzbedarfsfeststellungen nachvollziehbar dokumentiert und werden sie durch das IRM überprüft?	☐	☐	☐	☐
Werden Risikoanalysen (Maßnahmen Soll-Ist) durchgeführt und die Ergebnisse kompetenzgerecht genehmigt?	☐	☐	☐	☐
4. Informationssicherheitsmanagement				
Existieren Richtlinien zur physischen Sicherheit und zum Testen/ Überprüfen der Maßnahmen zum Schutz der Informationssicherheit?	☐	☐	☐	☐
Ist ein kontinuierliches Sensibilisierungs- & Schulungsprogramm zur Informationssicherheit (inkl. Erfolgsüberprüfung) vorhanden?	☐	☐	☐	☐
5. Operative Informationssicherheit				
Existiert ein Verfahren zur zeitnahen regelbasierten Identifizierung und Bewertung von Bedrohungen mit zeitnaher Reaktion (SIEM/SOC)?	☐	☐	☐	☐
Sind die operative IT-Sicherheit und das ISM gemäß dem 3 LoD Modell getrennt aufgestellt und die Verantwortlichkeiten klar definiert?	☐	☐	☐	☐
Sind IS-Prozesse und -Maßnahmen etabliert und erfolgen regelmäßige/ anlaßbezogene Überprüfungen der Sicherheit der IT-Systeme?	☐	☐	☐	☐
6. Identitäts- und Rechtemanagement				
Bestehen Berechtigungskonzepte auf allen Ebenen der IT-Systeme und sind SoD auch berechtigungskonzeptübergreifend gewährleistet?	☐	☐	☐	☐
Sind Protokollierungs- & Überwachungsmaßnahmen der Berechtigungsverwendung, insbesondere für Aktivitäten mit privilegierten (besonders kritischen) Benutzer- und Zutrittsrechten, etabliert?	☐	☐	☐	☐
7. IT-Projekte und Anwendungsentwicklung				
Sind für alle Anforderungen zugehörige Akzeptanz- und Testkriterien definiert?	☐	☐	☐	☐
Werden die Maßnahmen zum Schutz der Informationen (z.B. via Penetrationstests) im Rahmen der Entwicklung systematisch getestet?	☐	☐	☐	☐
8. IT-Betrieb				
Wird der aktuelle Leistungs- & Kapazitätsbedarf der IT-Systeme erhoben, zukünftiger abgeschätzt, geplant und überwacht?	☐	☐	☐	☐
Werden für die Wartungsaktivitäten Anforderungen (im Rahmen des Change Prozesses) gestellt?	☐	☐	☐	☐
9. Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen				
Sind die Vorgaben des IT-Betriebs in den Vereinbarungen/ Verträgen zu IT-Dienstleistungen enthalten (bzw. die Notwendigkeit geprüft)?	☐	☐	☐	☐
10. IT-Notfallmanagement				
Ist ein Notfallkonzept mit den obligatorischen Szenarien vorhanden und mit BCM, IRM/ ISM hinsichtlich der Ziele und Inhalte verzahnt?	☐	☐	☐	☐
Sind die zeitkritischen Aktivitäten/ Prozesse via Auswirkungsanalysen (BIA) identifiziert und werden für diese Risikoanalysen durchgeführt?	☐	☐	☐	☐
Sind IT-Notfallpläne für alle IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, vorhanden, aktuell und werden sie regelmäßig auf Wirksamkeit überprüft (Notfalltests)?	☐	☐	☐	☐
Ist die Bedienbarkeit zeitkritischer Aktivitäten und Prozesse bei Komplettausfall des Rechenzentrums nachweislich gegeben?	☐	☐	☐	☐

Abb. 3: Ausgewählte Fragestellungen der VAIT

unser angebot - der vait delta-check

plenum führt seit vielen Jahren sehr erfolgreich regulatorische Projekte für die IT von Versicherungen, Banken und Kapitalanlagegesellschaften durch. Die hier gewonnenen Erkenntnisse über die Prüfungspraxis der BaFin kombinieren wir für Sie zu einem „VAIT Delta-Check“, der Ihnen in kurzer Zeit Ihre individuellen Handlungsbedarfe aufzeigt. Als Partner der IT betrachten wir die IT und ihre Risiken hierbei „end-to-end“ entlang der Leistungsprozesse und gehen den Risikoursachen sorgfältig auf den Grund. Denn unser Auftrag endet nicht damit, die IT durchzuprüfen, sondern beginnt damit erst. Mit einem kompakten und ressourcenschonenden Vorgehen bieten wir Ihnen eine Standortbestimmung innerhalb weniger Wochen. Neben den Schwachstellen Ihrer IT aus Sicht der novellierten Teile der VAIT zeigen wir Ihnen hierin auf, mit welchen Sofortmaßnahmen Sie Ihre Compliance kurzfristig steigern können. Der wichtigste Mehrwert in unserem Vorgehen liegt jedoch darin, dass wir auf Basis unserer mehr als 30-jährigen Erfahrung mit Ihnen zukunftsorientierte Maßnahmen erarbeiten, die für eine angemessene und nachhaltige Compliance sorgen – damit Sie sich wieder voll auf Ihr Kerngeschäft konzentrieren können.