VAIT – Aktualisierung 2022

Hoher Wiederverwendungsanteil aus BAIT und ZAIT

Dr. Waldemar Grudzien
Nadine Hofmann

April 2022
Blogpost

Key Facts

- Der Anteil neuer Inhalte ist in Textziffer-Zählweise im Vergleich zu BAIT und ZAIT kleiner 8%, weitere 16% der Textziffern wurden leicht ergänzt
- Bei Ausgliederungen folgt die VAIT nicht der ZAIT, sondern bleibt weitgehend dem schlanken Ansatz der BAIT für Auslagerungen treu
- IT-Notfallkonzept muss anlassbezogen und regelmäßig, aber nicht jährlich wie bei BAIT und ZAIT aktualisiert werden
- Versicherungsunternehmen dürfen die IT-Strategie ausdrücklich als Teil der Geschäfts- oder Risikostrategie verfassen; ein gesondertes Dokument ist nicht notwendig
- Vereinigung von BAIT, VAIT und ZAIT zu einem sektoriellen IT-Anforderungskatalog mit branchenspezifischen Ergänzungen angesichts der Gleichanteile für Bündelung der personellen und organisatorischen Ressourcen von BaFin und Bundesbank geboten

Einleitung

Anfang März 2022 hat die BaFin das Rundschreiben 10/2018 in der Fassung vom 03.03.2022 „Versicherungsaufsichtliche Anforderungen an die IT (VAIT)“ veröffentlicht und die VAIT in der Fassung vom 20.03.2019 abgelöst. Nach den Rundschreiben 10/2017 (BAIT) und 11/2021 (ZAIT) vom 16.08.2021 wurde der Dreiklang der aufsichtlichen Anforderungen an die IT der drei Gruppen von Finanzmarktakteuren - Versicherungsunternehmen, Banken sowie Zahlungs- und E-Geld-Instituten - aktualisiert.

Die BaFin passt mit der neuen Version die VAIT an die im Oktober 2020 durch die EIOPA[1] veröffentlichten „Leitlinien zur Sicherheit und zum Risikomanagement der Informations- und Kommunikationstechnologie (IKT)“ an.

In unseren nachfolgenden Ausführungen folgt die Analyse der VAIT, auch im Kontext der BAIT und ZAIT.

Technische Analyse

Die aktualisierte VAIT besteht aus den zwei Teilen „I. Vorbemerkung“ und „II. Anforderungen“, mit 11 Kapiteln im zweiten Teil und insgesamt 104 Textziffern.

Abschnitt I „Vorbemerkung“ besteht aus 12 Textziffern und damit im Vergleich zu BAIT (4) und ZAIT (6) aus deutlich mehr Inhalt, der zudem über fünf neue Textziffern verfügt. Sieben Textziffern wurden aus BAIT und ZAIT übernommen. Die neuen fünf Textziffern weisen neben versicherungsspezifischen Inhalten (Textziffern 3 und 5) Selbstverständlichkeiten (Textziffern 10 bis 12) auf:

- Tz. 3: Rundschreiben gilt auch für Gruppen von Erst- und Rückversicherungsunternehmen mit Sitz im Inland

[1] European Insurance and Occupational Pensions Authority

- Tz. 5: Sicherstellung der Einhaltung der Anforderungen in Ausgliederungsvereinbarungen mit IT-Dienstleistern
- Tz. 10: Feststellung, dass Risikoprofil abhängig von Strukturen, IT-Systemen oder Prozessen ist
- Tz. 11: Feststellung, dass ein Risikoprofil fortwirkt, sofern sich keine Veränderungen ergeben
- Tz. 12: Zuweisung der Gesamtverantwortung aus dem Rundschreiben auf alle Mitglieder der Geschäftsleitung, diese kann nicht delegiert werden und untereinander von sich gewiesen werden

Textziffer 5 markiert die Wichtigkeit von Kapitel 9 (mit Fokus auf Ausgliederungen). Textziffern 10 und 11 führen das in den Textziffern 7 bis 9 beschriebene Proportionalitätsprinzip weiter aus.

Der **zweite Abschnitt** wurde im Vergleich zur Vorversion der VAIT um die zwei Kapitel „Kapitel 5: Operative Informationssicherheit“ und „Kapitel 10: IT-Notfallmanagement“ erweitert. **Error! Reference source not found.** verdeutlicht die inhaltlich gleichen Anteile und Unterschiede zwischen den drei Anforderungskatalogen der VAIT, BAIT und ZAIT. Die drei Anforderungskataloge wurden unter mehreren Blickwinkeln verglichen: Inhaltgleichheit, Gleichheit nach Auslegung sowie Gleichheit nach Wirkung der umgesetzten Anforderung.

In der x-Achse sind die Kapitel der beiden Abschnitte zu sehen, die wiederum in die einzelnen Textziffern unterteilt sind. Zum besseren Verständnis der Abbildung 1 folgen zwei Lesebeispiele:

- Feld „II 2.X/10“: VAIT Textziffer 2.10 ist eine ergänzte inhaltliche Übernahme der Textziffer 3.1 im Abschnitt II Kapitel 3 und aus der Textziffer 3 im Abschnitt I der BAIT
- Feld „II 7.X/16“: VAIT Textziffer 7.16 ist eine inhaltliche Übernahme der Textziffer 7.14 im Abschnitt II Kapitel 7 aus BAIT und Textziffer 7.15 im Abschnitt II Kapitel 7 aus ZAIT

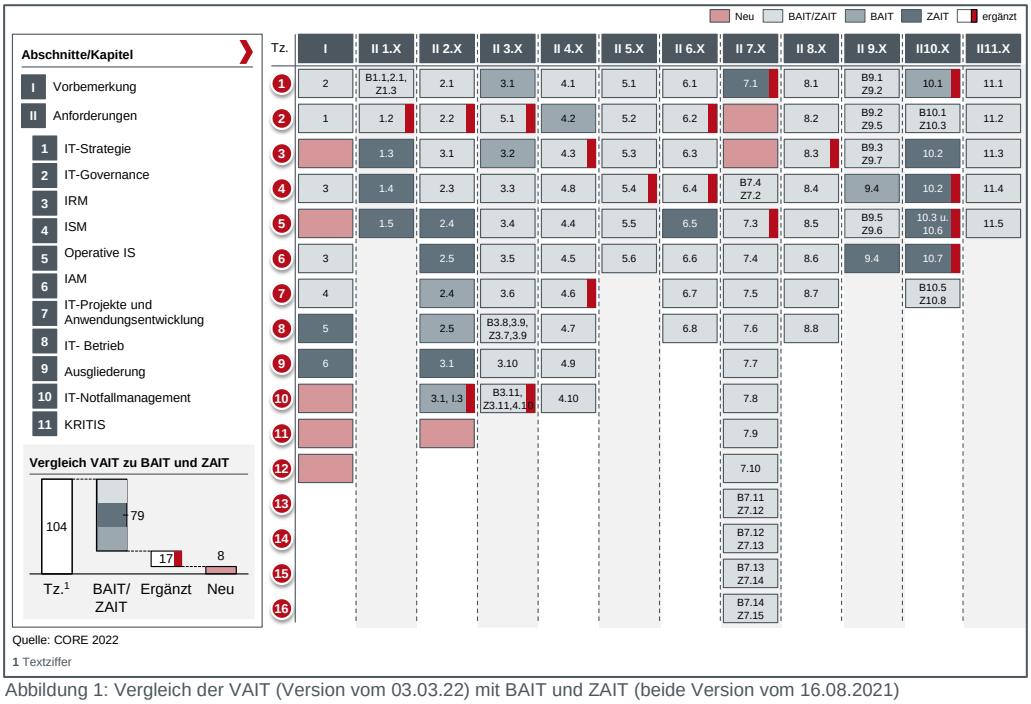

Abbildung 1: Vergleich der VAIT (Version vom 03.03.22) mit BAIT und ZAIT (beide Version vom 16.08.2021)

Sofort ins Auge springen die Gleichanteile (alle drei Abstufungen von grau), denn die VAIT besteht zum größten Teil aus Inhalten von BAIT und ZAIT: Von 104 Textziffern der VAIT wurden 8 Textziffern neu formuliert, 96 Textziffern sind entweder unverändert (79) oder - zumeist leicht - ergänzt (17). In Prozenten besteht die VAIT zu 76% aus gleichen Inhalten von BAIT und ZAIT, zu 16,3% aus ergänzten Textziffern und zu 7,7% aus neuen Inhalten im Vergleich zu BAIT und ZAIT. BAIT und ZAIT wurden im August letzten Jahres aktualisiert und waren mit den zwei Kapiteln „Kapitel 5: Operative Informationssicherheit“ und „Kapitel 10: IT-Notfallmanagement“ der VAIT voraus. Dies hat die BaFin mit der neuen VAIT korrigiert. Allerdings wurden nicht alle neuen Inhalte der ZAIT (vergleiche CORE-Blogpost „ZAIT – Vergleich zur BAIT“) in die VAIT übernommen, was bei den Ausgliederungen (Kapitel 9: „Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen“) verwundert.

Zu Kapitel 1 „**IT-Strategie**“:

Der Satz „Die Geschäftsleitung muss für die Umsetzung der IT-Strategie Sorge tragen.“ in Tz. 1.1 ist ein Gemeinplatz und wurde der ebenfalls am 16.08.2021 veröffentlichten MaRisk entnommen.

Ergänzung der Tz. 2.1: In den Erläuterungen (rechte Spalte) gesteht die VAIT den Versicherungsunternehmen ausdrücklich die Freiheit zu, die IT-Strategie als Teilkapitel in der Geschäfts- oder Risikostrategie zu verfassen. Gemeinhin wird die IT-Strategie als gesondertes Dokument erstellt. In BAIT und ZAIT gibt es hierzu keine Aussagen.

Den Strategieprozess haben die Verfasser der VAIT aus der ZAIT übernommen (die BAIT beschreibt keinen IT-Strategieprozess, jedoch ist dieser in der MaRisk beschrieben, welche die BAIT als Mindestanforderung vorschreibt).

Zu Kapitel 2 „**IT-Governance**“:

Kapitel 2.2 wurde um den folgenden Satz ergänzt: „Diese Leitlinien [zur IT-Aufbau- und IT-Ablauforganisation] sind im Unternehmen entsprechend dem Risikoprofil zu treffen.“

Kapitel 2.10 wurde um den Prozess der Rechtevergabe mit Nennung eines möglichen Rollenmodells ergänzt. Des Weiteren wird die 1LoD[2]-Pflicht zur Prüfung der Geeignetheit der IT-Systeme und IT-Prozesse zur Erreichung der Schutzziele benannt. Der Teil zur Rechtevergabe sollte zu Kapitel 6 verschoben werden.

Das neue Kapitel 2.11 stellt die Forderung nach Arbeitsablaufbeschreibungen (auch Organisationsrichtlinien oder Arbeitsanweisungen genannt) auf. Diese Anforderung entspricht der weitgehend gelebten Praxis und kodifiziert somit ein notwendiges Best Practice.

[2] 1st Line of Defense

Zu Kapitel 3 „**Informationsrisikomanagement**“:

Die Erklärung in Tz. 3.2 ist neu und beschreibt Anforderungen an die Festlegung von Risikokriterien und die sie bestimmenden Faktoren.

Kapitel 3.10 wurde mit dem letzten Satz um Berichtsfrequenzen eines Statusberichts ergänzt. Der Statusbericht „enthält beispielsweise die Bewertung der Risikosituation“ und unterscheidet sich vom im gleichen Kapitel genannten „schriftlichen Bericht mit Ergebnissen der Risikoanalyse“ um einen einschätzenden, den deskriptiven Teil des schriftlichen Berichts ergänzenden Teil.

Zu Kapitel 4 „**Informationssicherheitsmanagement**“:

Dieses Kapitel verzeichnet lediglich zwei Ergänzungen: In Kapitel 4.3 wurde im Erklärungsteil der letzte Satz hinzugefügt: „Zu den Ergebnissen des Informationsrisikomanagements zählen u. a die definierten Sollmaßnahmen (vgl. 3.7).“ Die BaFin unterstreicht hier nochmal die Wichtigkeit, Risiken mit Maßnahmen zu ihrer Behandlung zu unterlegen.

Kapitel 4.7 legt im Erklärungsteil die Anforderungen bei Ausgliederung der Rolle des Informationssicherheitsbeauftragten selbst als auch seiner Funktionstrennung im Falle der Ausgliederung IT-bezogener Geschäftsaktivitäten dar.

Zu Kapitel 5 „**Operative Informationssicherheit**“:

Auch Kapitel 5 erfuhr nur wenige Änderungen im Vergleich zu BAIT und ZAIT. So weist Kapitel 5.4 im Erklärungsteil den neuen Satz auf: „Die Regeln müssen dazu geeignet sein, anomale Aktivitäten und Bedrohungen zu erkennen.“ Ein Hinweis auf die Selbstverständlichkeit zum Beispiel ein SIEM mit einem sinnvollen Set an Regeln und Alarmen zu betreiben. In Kapitel 5.5 gibt es dann eine Überraschung, und zwar nicht durch eine Ergänzung, sondern durch Weglassen: Es fehlt der Hinweis auf ein SOC (Security Operations Center). Während an gleicher Stelle sowohl die BAIT als auch die ZAIT diesen Satz enthalten – „Die zeitnahe Analyse und Reaktion können eine ständig besetzte zentrale Stelle, z. B. in Form eines Security Operation Centers (SOC), erfordern.“ – wurde dieser in die VAIT nicht übernommen. Ein SOC wird bei BAIT und ZAIT als Möglichkeitsraum beispielhaft genannt, somit nicht konkret gefordert. Vielleicht wollten die Verfasser der VAIT Unschärfen in der Auslegung vermeiden. Vielleicht wird ein SOC im zumeist nicht zeitkritischen Geschehen eines Versicherungsunternehmens nicht zur ersten Priorität von Maßnahmen gesehen.

Zu Kapitel 6 „**Identitäts- und Rechtemanagement**“:

In Kapitel 6.2 wurde im Erklärungsteil der Satz „Im Rahmen des Sparsamkeitsgrundsatzes sind auch die Zugriffsrechte jedes einzelnen technischen Benutzers auf das unbedingt erforderliche Minimum zu beschränken und nicht benötigte Benutzerkonten sind zu löschen.“ zur Unterstreichung der „Need-to-know“ und „Least Privilege“ Prinzipien im IAM ergänzt.

Eine zweite Ergänzung findet sich im Kapitel 6.4 in Form des neuen Satzes im Erklärungsteil: „Bei Einrichtung und Änderung von Berechtigungen bedarf es der vorherigen Zustimmung der fachlich verantwortlichen Stelle, bei Deaktivierung oder Löschung ist sie zeitnah zu informieren." – eigentlich sind das Selbstverständlichkeiten, die jedoch erstmals schriftlich für Versicherungen festgehalten werden.

Zu Kapitel 7 „**IT-Projekte und Anwendungsentwicklung**":

Kapitel 7 weist mit 7.2 und 7.3 inhaltlich Neues im Vergleich zu BAIT und ZAIT auf, zudem wurden zwei Textziffern ergänzt. Kapitel 7.1 wurde um die drei letzten Sätze ergänzt. Diese legen den Versicherungsunternehmen die Pflicht auf, bei IT-Projekten und Anwendungsentwicklungen auch die „unabhängige Risikokontrollfunktion, die Compliance-Funktion und die versicherungsmathematische Funktion zu beteiligen, sofern das Unternehmen die jeweiligen Funktionen von Gesetzes wegen einzurichten hat. Die Funktion der internen Revision kann beratend beteiligt werden." Ferner gilt Kapitel 7.1 auch beim „erstmaligen Einsatz sowie wesentliche Veränderungen von IT-Systemen".

Die neue Textziffer 7.2 thematisiert das Testen von IT-Systemen vor dem Produktivbetrieb und schreibt die Trennung der Betriebsumgebung von Entwicklung und Test vor; sodass nun faktisch die drei klassischen Software-Umgebungen Entwicklung, Test und Produktion kodifiziert sind.

Kapitel 7.3 adressiert unter Verweis auf vier andere Textziffern – 2.9 und 2.10 zu der technisch-organisatorischen Ausstattung, 3.2 zu Risikokriterien und 7.2 zum Testen und getrennte Umgebungen für Entwicklung, Test und Betrieb – das schwierige Thema IDV[3]. Hinzu kommt der Hinweis auf den Schutzbedarf der durch IDV verarbeiteten Daten zur Ableitung angemessener Maßnahmen.

Kapitel 7.5 erfuhr eine Ergänzung zur Beachtung des Change Managements: „Werden im Rahmen von IT-Projekten größere Änderungen an Prozessen mit Auswirkungen auf die Informationssicherheit erforderlich, sind entsprechende Änderungsanträge zu stellen und zu bearbeiten." Es fehlt der Hinweis auf eine vollständige Dokumentation der Änderung.

Zu Kapitel 8 „**IT-Betrieb**":

Der einzige Unterschied zu BAIT und ZAIT findet sich in Kapitel 8.3 mit zwei ergänzten Sätzen zu Hardware-Komponenten: Diese müssen entsorgt werden, wenn sie nicht mehr verwendet werden. Im Erklärungsteil werden „insbesondere Datenträger" zu Hardware-Komponenten hinzugezählt.

[3] Individuelle Datenverarbeitung

Zu Kapitel 9 „**Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen**“:

Dieses Kapitel gibt ein Rätsel auf. Es entspricht BAIT und ZAIT, geht aber die große Erweiterung der ZAIT gegenüber der BAIT im August 2021 (vergleiche CORE-Blogpost „ZAIT – Vergleich zur BAIT“) nicht mit.

Zur Erinnerung: Die ZAIT adressiert im entsprechenden Kapitel 9 Themen und Detailbeschreibungen in den folgenden Textziffern, die sich in der VAIT nicht oder nicht in der Detailtiefe wiederfinden:

- 9.3: Verbleibende Mindestkenntnisse im auslagernden Unternehmen
- 9.8: Ergebnisse von Risikoanalysen in Verträgen
- 9.9: Geschäftsfortführung nach Beendigung von Auslagerungen
- 9.10: Inhalte des Auslagerungsvertrages
- 9.11: Weiterverlagerungen im Auslagerungsvertrag
- 9.12: Zentraler Auslagerungsbeauftragter
- 9.13: Berichte zu Auslagerungen
- 9.14: Gemeinsame Notfallkonzepte von IT-Verbünden
- 9.15: Auslagerungsregister

Kapitel 9.1 ZAIT gilt spezifisch für Zahlungsdienstleister.

Zu Kapitel 10 „**IT-Notfallmanagement**“:

Kapitel 10 wurde weitestgehend von BAIT und ZAIT übernommen und in vier Textziffern ergänzt. In Textziffer 10.1 findet sich der Hinweis, bei Ausgliederungen das IT-Notfallmanagement auch bei Weiterverlagerungen zu berücksichtigen.

In Textziffer 10.2 findet sich im Vergleich zur ZAIT eine Petitesse, die aber für Versicherungsunternehmen eine enorme Aufwandsreduktion im Vergleich zu Zahlungs- und E-Geld-Instituten bedeuten kann: Während bei BAIT und ZAIT das IT-Notfallkonzept „jährlich“ oder anlassbezogen zu aktualisieren ist, muss das bei Versicherungsunternehmen nur „regelmäßig“ oder anlassbezogen erfolgen. Ein Plus für die VAIT gegenüber BAIT und ZAIT aus Sicht der Autoren da es weitaus praxisnäher für Versicherungen ist.

Textziffer 10.4 weist im deklaratorischen Teil eine Ergänzung auf, mit der die Ergebnisse von Auswirkungsanalysen und Risikoanalysen bis hin zur Bestimmung von Maßnahmen erklärt werden.

Textziffer 10.5 wird im deklaratorischen Teil um zwei Details ergänzt: Erstens sollen IT-Notfallpläne die Bedingungen zu ihrer Aktivierung enthalten, zweitens sollen alternative Optionen einbezogen werden, wenn die Herstellung des Normalbetriebs kurzfristig nicht möglich ist.

Textziffer 10.6 fordert ergänzend die schriftliche Dokumentation der Ergebnisse von Notfalltests, die Analyse von Mängeln und deren Berichterstattung an die Geschäftsleitung.

Kapitel 11 „**Kritische Infrastrukturen**“:

Entspricht der BAIT und ZAIT.

Fazit

Die Veränderungen der VAIT im Vergleich zur BAIT und ZAIT sind eher als marginal zu bezeichnen. Die VAIT übernimmt nicht die durch die ZAIT vorgelegten Anforderungen an Outsourcing-Verhältnisse in Kapitel 9 und folgt damit der „Vorgabe“ der BAIT; die Nähe von Bankenaufsicht zur Versicherungsaufsicht sowie der unterlegten Aufsichtsobjekte manifestiert sich hier. Abgesehen von denen im Text identifizierten und analysierten Ergänzungen stellt sich angesichts der Inhalte in BAIT, VAIT und ZAIT die Frage nach einer Vereinheitlichung der IT-Anforderungen zu einem gemeinsamen sektoriellen IT-Anforderungskatalog für Banken, Versicherungsunternehmen sowie Zahlungs- und E-Geld-Institute mit den dann fokussierten branchenspezifischen Ergänzungen in drei Unterkapiteln von aufsichtlichen Anforderungen an die IT, subsummiert zu XAIT. Diese Vereinheitlichung wäre der erste Schritt zu einer gebündelten IT-Aufsicht für alle Aufsichtsobjekte und damit zu einer Konzentration der Kräfte von BaFin und Bundesbank und der daraus folgenden Erhöhung der Fachexpertise und personeller Prüfungsstärke. Die Aufsichtsobjekte selbst hätten den Vorteil einer verbesserten Prüfungssituation in Dauer sowie Qualität der Prüfung. XAIT würde dem Sektor zudem eine gute technische Grundlage zum Ausbau eines nationalen Umsetzungsrundschreibens für die kommende DORA[4] bieten.

[4] Digital Operational Resilience Act

Verfasser

Waldemar Grudzien ist Expert Director bei CORE. Er wurde in Elektrotechnik promoviert und verfügt über ein Diplom in VWL. Schwerpunkte seiner Arbeit sind Informationssicherheit und Datenschutz – in Theorie und Praxis, inklusive der Tätigkeit als ISB und DSB in verschiedenen Klientenstrukturen.

Mail: waldemar.grudzien@core.se

Nadine Hofmann ist Expert Managerin bei CORE. Sie studierte Luft- und Raumfahrttechnik in Braunschweig und Dresden. Ihre Beratungskompetenz fokussiert sich auf technischen Datenschutz und Informationssicherheit (Schwerpunkte IAM, SOC/SIEM, Management von Risiken, ISO27001 und DSGVO). Sie unterstützt Klienten bei der Strukturierung und dem Aufbau von Financial Compliance Systemen. Zusätzlich fungiert sie als stellvertretende ISB.

Mail: nadine.hofmann@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se