Entwurf eines IDW Prüfungsstandards: Prüfung der Einhaltung der nach den „Versicherungsaufsichtlichen Anforderungen an die IT“ (VAIT) eingerichteten technisch-organisatorischen Vorkehrungen (VAIT-Prüfung) (IDW EPS 590 (07.2023))

Stand: 16.06.2023[1]

Der Versicherungsfachausschuss (VFA) des IDW hat den nachfolgenden Entwurf eines IDW Prüfungsstandards: Prüfung der Einhaltung der nach den „Versicherungsaufsichtlichen Anforderungen an die IT“ (VAIT) eingerichteten technisch-organisatorischen Vorkehrungen (IDW EPS 590 (07.2023)) verabschiedet. Mit dem Prüfungsstandard trägt das IDW der zunehmenden Bedeutung der IT von Versicherungen Rechnung und verdeutlicht, wie Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit eine Prüfung der Einhaltung der nach den VAIT eingerichteten technisch-organisatorischen Vorkehrungen durchführen und über diese berichten.

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat mit dem Rundschreiben 10/2018 VA “Versicherungsaufsichtliche Anforderungen an die IT” (VAIT) veröffentlicht. Das Rundschreiben legt die Vorschriften über die Geschäftsorganisation im Versicherungsaufsichtsgesetz (VAG), soweit sie sich auf die technisch-organisatorische Ausstattung der Unternehmen beziehen, für die BaFin verbindlich aus und dient hierdurch einer konsistenten Anwendung gegenüber allen Unternehmen und Gruppen.

Bei Versicherungsunternehmen gehört eine Prüfung von IT-Systemen als Teil des Risikomanagements und Ordnungsmäßigkeit der Geschäftsorganisation nicht zu den besonderen aufsichtlichen Pflichten des Prüfers im Rahmen der Jahresabschlussprüfung nach § 35 VAG.

Eine freiwillige Prüfung der Einhaltung der nach den VAIT eingerichteten technisch-organisatorischen Vorkehrungen durch einen unabhängigen Wirtschaftsprüfer kann dem objektivierten Nachweis der ermessensfehlerfreien Ausübung der Organisations- und Sorgfaltspflichten der gesetzlichen Vertreter und eines ggf. einzurichtenden Aufsichtsorgans dienen.

Änderungs- oder Ergänzungsvorschläge zu dem Entwurf werden schriftlich an die Geschäftsstelle des IDW (Postfach 32 05 80, 40420 Düsseldorf oder stellungnahmen@idw.de) bis zum 31.12.2023 erbeten. Die Änderungs- oder Ergänzungsvorschläge werden im Internet auf der IDW Website veröffentlicht, wenn dies nicht ausdrücklich vom Verfasser abgelehnt wird.

Der Entwurf steht bis zu seiner endgültigen Verabschiedung als IDW Prüfungsstandard im Internet (www.idw.de) unter der Rubrik Verlautbarungen als Download-Angebot zur Verfügung.

[1] Verabschiedet vom Versicherungsfachausschuss (VFA) am 16.06.2023. Billigende Kenntnisnahme des Hauptfachausschuss (HFA) am 03.07.2023.

1. Vorbemerkung....2
2. Definitionen....4
3. Gegenstand und Ziel der Prüfung....5
4. Anforderungen....6
4.1. Berufspflichten....6
4.2. Auftragsannahme....6
4.3. Aufbau, Planung und Durchführung der VAIT-Prüfung....7
4.3.1. Aufbau und Planung der VAIT-Prüfung....7
4.3.2. Durchführung....8
4.3.2.1. Würdigung des Soll-Objekts....8
4.3.2.2. Angemessenheitsprüfung....9
4.3.2.3. Wirksamkeitsprüfung....9
4.3.3. Prüfungsnachweise....9
4.3.4. Ereignisse nach dem Ende des zu prüfenden Zeitraums....11
4.3.5. Schriftliche Erklärungen....11
4.4. Dokumentation....12
4.5. Berichterstattung....13
5. Anwendungshinweise und Erläuterungen....15
5.1. Vorbemerkung [Tz. 1 ff.]....15
5.2. Gegenstand und Ziel der Prüfung [Tz. 9 ff.]....15
5.3. Auftragsannahme [Tz. 15 ff.]....17
5.4. Planung, Aufbau und Durchführung der VAIT-Prüfung....18
5.4.1. Aufbau und Planung der VAIT-Prüfung [Tz. 20 ff.]....18
5.4.2. Würdigung des „Soll-Objekts“ [Tz. 29 ff]....18
5.4.3. Angemessenheits- und Wirksamkeitsprüfung [Tz. 32 ff.]....19
5.4.4. Ereignisse nach dem Ende des zu prüfenden Zeitraums [Tz. 45 ff.]....20
5.4.5. Berichterstattung [Tz. 58 ff.]....20
Anlagen....21
Anlage 1 – Indikatorenkatalog....21
Anlage 2 – Musterberichterstattung....23

1. Vorbemerkung

1 Der Einsatz von Informationstechnologie (IT), auch unter Einbeziehung von IT-Services, die durch IT-Dienstleister bereitgestellt werden, hat eine zentrale Bedeutung für Versicherungsunternehmen. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat mit dem Rundschreiben 10/2018 VA “Versicherungsaufsichtliche Anforderungen an die IT” (im Folgenden “VAIT”) veröffentlicht. Die BaFin legt mit dem Rundschreiben die Vorschriften über die Geschäftsorganisation im Versicherungsaufsichtsgesetz (VAG), soweit sie sich auf die technisch-organisatorische Ausstattung der Unternehmen beziehen, verbindlich aus. Die VAIT dient hierdurch einer konsistenten Anwendung gegenüber allen adressierten Unternehmen und Gruppen.

2 Im Rahmen der Jahresabschlussprüfung ist der Abschlussprüfer entsprechend den Anforderungen des ISA [DE] 315[2] verpflichtet, Prüfungshandlungen zur Risikobeurteilung im Zusammenhang mit der Aufstellung des Abschlusses durchzuführen, um insoweit

a. ein Verständnis von der für das Informationssystem und die Kommunikation des Unternehmens relevanten IT-Umgebung zu erlangen,

b. auf Grundlage der identifizierten Kontrollen, die IT-Anwendungen und anderen Aspekten der IT-Umgebung zu identifizieren, die Risiken aus dem IT-Einsatz unterliegen,

c. für solche identifizierten IT-Anwendungen und identifizierten anderen Aspekten der IT-Umgebung, die damit verbundenen sich aus dem IT-Einsatz ergebenden Risiken sowie die generellen IT-Kontrollen, die solche Risiken behandeln, zu identifizieren und

d. für jede identifizierte generelle IT-Kontrolle

   i. zu beurteilen, ob die Kontrolle wirksam ausgestaltet ist, um Risiken wesentlicher falschen Darstellungen auf Aussageebene zu behandeln, oder wirksam ausgestaltet ist, die Funktion anderer Kontrollen zu unterstützen und

   ii. festzustellen, ob die Kontrolle implementiert wurde, in dem zusätzlich zur Befragung des Personals der Einheit Prüfungshandlungen durchgeführt werden.

Sofern der Abschlussprüfer im Rahmen der Prüfung des Abschlusses bei der Festlegung von Art, zeitlicher Einteilung und Umfang der aussagebezogenen Prüfungshandlungen plant, die wirksame Funktion einer generellen IT-Kontrolle zu prüfen oder aussagebezogene Prüfungshandlungen alleine nicht ausreichende geeignete Prüfungsnachweise erlangen können, ist der Abschlussprüfer verpflichtet, entsprechend den Anforderungen des ISA [DE] 330[3] die wirksame Funktion dieser Kontrollen zu prüfen.

3 Die Jahresabschlussprüfung ist jedoch nicht darauf ausgerichtet, Prüfungsfeststellungen zur Einhaltung der nach Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) eingerichteten technisch-organisatorischen Vorkehrungen zu treffen. Das Prüfungsurteil im Bestätigungsvermerk bezieht sich ausschließlich auf den Abschluss und den Lagebericht und umfasst keine Aussage zur Einhaltung der VAIT. Eine nach diesem *IDW Prüfungsstandard* durchgeführte Prüfung der Einhaltung der nach den VAIT eingerichteten technisch-organisatorischen Vorkehrungen (im Folgenden: „VAIT-Prüfung“) ist hingegen darauf ausgerichtet, Feststellungen zur Angemessenheit und zur Wirksamkeit der Einhaltung der nach den VAIT eingerichteten technisch-organisatorischen Vorkehrungen zu treffen (vgl. Tz. 11). Bei einer VAIT-Prüfung werden Prüfungsfeststellungen unabhängig davon getroffen, ob sich eine Beanstandung tatsächlich bereits für den zu prüfenden Zeitraum ausgewirkt hat oder sich ggf. potenziell erst in Zukunft auswirkt.

4 Bei der von einem Wirtschaftsprüfer durchgeführten Prüfung der Einhaltung der nach den VAIT eingerichteten technisch-organisatorischen Vorkehrungen handelt es sich um eine Prüfung zur Einhaltung aufsichtlicher Anforderungen. Bei Versicherungsunternehmen gehört eine Prüfung von IT-Systemen als Teil des Risikomanagements und Ordnungsmäßigkeit der Geschäftsorganisation nicht zu den besonderen aufsichtlichen Pflichten des Abschlussprüfers im Rahmen der Jahresabschlussprüfung nach § 35 VAG.

---

[2] ISA [DE] 315 (Revised 2019) „Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen“.

[3] ISA [DE] 330 „Reaktion des Abschlussprüfers auf beurteilte Risiken“.

5 Die gesetzlichen Vertreter sind für die Einhaltung der an das beaufsichtigte Versicherungsunternehmen gerichteten aufsichtlichen Anforderungen einschließlich der VAIT verantwortlich. Demzufolge sind die gesetzlichen Vertreter auch für die Ableitung und Einrichtung der zur Einhaltung der VAIT notwendigen angemessenen und wirksamen technisch-organisatorischen Vorkehrungen verantwortlich. Die Mitglieder des Aufsichtsorgans sind für die Wahrnehmung ihrer Überwachungsfunktion verantwortlich, einschließlich der Überwachung der gesetzlichen Vertreter bei der Erfüllung der an das beaufsichtigte Versicherungsunternehmen gerichteten aufsichtlichen Anforderungen.

6 Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) legt in diesem *IDW Prüfungsstandard* die Berufsauffassung dar, nach welchen Grundsätzen Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit eine Prüfung der Einhaltung der nach den VAIT eingerichteten technisch-organisatorischen Vorkehrungen durchführen und über diese berichten (vgl. Tz. A1). Neben Definitionen (Abschn. 2.) und Gegenstand und Ziel der Prüfung (Abschn. 3) enthält dieser *IDW Prüfungsstandard* in dem Abschn. 4. zu beachtende Prüfungsanforderungen sowie Anwendungshinweise und Erläuterungen (Abschn. 5.).[4]

7 Dieser *IDW Prüfungsstandard* ist erstmals anzuwenden für VAIT-Prüfungen, mit denen nach dem 31.12.2023 begonnen wird. Eine vorzeitige Anwendung ist zulässig.

2. Definitionen

8 Die folgenden Begriffe haben für Zwecke dieses *IDW Prüfungsstandards* die nachstehende Bedeutung:

a. Aufsichtliche Anforderung: Eine durch Gesetz, Verordnung, Richtlinie, eine anderweitige Rechtsnorm oder durch eine Verlautbarung einer nationalen oder europäischen Aufsichtsbehörde konkretisierte Verpflichtung eines beaufsichtigten Versicherungsunternehmens, eine dort bezeichnete aufsichtliche Regelung einzuhalten. Darunter sind jeweils die für den zu prüfenden Zeitraum gültigen, veröffentlichten aufsichtlichen Anforderungen an die beaufsichtigten Versicherungsunternehmen zu verstehen. Im Entwurfs- bzw. Konsultationsstadium befindliche aufsichtliche Verlautbarungen stellen keine (aufsichtlichen) Anforderungen dar. Entsprechendes gilt für Verlautbarungen, die von nicht direkt für die Versicherungsaufsicht zuständigen Organisationen herausgegeben werden.

b. Aufsichtliche Angemessenheitsprüfung (nachfolgend: „Angemessenheitsprüfung“): Beurteilung, ob das Versicherungsunternehmen die aus den VAIT abgeleiteten erforderlichen technisch-organisatorischen Vorgaben angemessen in Prozesse, Regelungen und Verfahren umgesetzt hat, um die aufsichtlichen Anforderungen zu erfüllen.

c. Aufsichtliche Wirksamkeitsprüfung (nachfolgend: „Wirksamkeitsprüfung“): Beurteilung, ob die durch das Versicherungsunternehmen vorgegebenen Prozesse, Regelungen

[4] Die Anwendungshinweise und sonstigen Erläuterungen (einschließlich der Anlagen) enthalten weiterführende Hinweise zu den Anforderungen dieses *IDW Prüfungsstandards* sowie zu deren Umsetzung. Insbesondere können sie a) genauer erläutern, was eine Anforderung bedeuten oder abdecken soll; b) Beispiele für Prüfungshandlungen enthalten, die unter den gegebenen Umständen geeignet sein können. Obwohl solche erläuternden Hinweise keine Anforderungen darstellen, sind sie für die richtige Anwendung der Anforderungen dieses *IDW Prüfungsstandards* relevant.

und Verfahren innerhalb des zu prüfenden Zeitraums wie vorgesehen eingehalten wurden.

d. Beanstandungen: Negative Prüfungsfeststellungen des VAIT-Prüfers.

e. Proportionalität: Ein auf der Verhältnismäßigkeit beruhender aufsichtlicher Grundsatz, der sich auf Ebene des einzelnen Versicherungsunternehmens auf die Angemessenheit der technisch-organisatorischen Vorkehrungen bezieht.

f. Indikatoren: Aus dem Grundsatz der Proportionalität abgeleitete Maßstäbe zur Würdigung des „Soll-Objekts".

g. Mangel: Abweichung (des Versicherungsunternehmens) von den aufsichtlichen Anforderungen oder organisatorischen Vorgaben.

h. Organisatorische Vorgaben („Soll-Objekt"): Vom Versicherungsunternehmen konkretisierte Ausgestaltung der aufsichtlichen Anforderungen in der Aufbau- und Ablauforganisation.

i. Prüfungsfeststellungen: Auf Basis einer Würdigung der erlangten Prüfungsnachweise begründete Schlussfolgerungen über die im Rahmen der durchgeführten Prüfungshandlungen geprüften aufsichtlichen Sachverhalte. Prüfungsfeststellungen umfassen sowohl positive als auch negative Schlussfolgerungen.

j. Prüfungsnachweise: Informationen, die der VAIT-Prüfer nutzt, um begründete Schlussfolgerungen (Prüfungsfeststellungen) zu ziehen.

k. VAIT-Prüfer: Wirtschaftsprüfer, der mit einer VAIT-Prüfung beauftragt wird.

l. VAIT-Prüfung: Eine freiwillig beauftragte Prüfung, um Feststellungen zur Angemessenheit und Wirksamkeit der vom Versicherungsunternehmen zur Einhaltung der VAIT eingerichteten technisch-organisatorischen Vorkehrungen zu treffen.

3. Gegenstand und Ziel der Prüfung

9 Gegenstand der VAIT-Prüfung sind die vom Versicherungsunternehmen zur Einhaltung der nach den VAIT eingerichteten technisch-organisatorischen Vorkehrungen (vgl. Tz. A2).

10 Mit dem Auftraggeber kann auch vereinbart werden, dass über den aktuellen Stand der VAIT hinaus ergänzend auch weitere Anforderungen an die IT (z.B. sich im Konsultationsprozess befindliche zu erwartende Änderungen – soweit sie nicht im Widerspruch zu bestehenden Anforderungen stehen – bzw. Ergänzungen der VAIT) als aufsichtliche Anforderungen der Prüfung zugrunde zu legen sind.

11 Zielsetzung der Prüfung nach diesem *IDW Prüfungsstandard* ist es, Feststellungen zur Angemessenheit und zur Wirksamkeit der vom Versicherungsunternehmen zur Einhaltung der nach den VAIT eingerichteten technisch-organisatorischen Vorkehrungen zu treffen (Organisationsprüfung: VAIT-Prüfung).

Nach einer VAIT-Prüfung gemäß dieses *IDW Prüfungsstandards* nimmt der VAIT-Prüfer Würdigungen sowie Prüfungshandlungen unter Ausübung seines pflichtgemäßen Ermessens vor (vgl. Abschn. 4.3) und berichtet über durchgeführte Prüfungshandlungen und deren Ergebnisse (Prüfungsfeststellungen) (vgl. Abschn. 4.5).

12 Aufgrund der teilweise überschneidenden Anforderungen in den einzelnen Kapiteln der VAIT kann eine VAIT-Prüfung nach diesem *IDW Prüfungsstandard* nur für die Umsetzung der Anforderungen der VAIT als Ganzes erfolgen (vgl. Tz. A3). Hiervon ausgenommen sind die Anforderungen an kritische Infrastrukturen gemäß § 8a Abs. 1 BSIG. Gemäß § 8a Abs. 3 BSIG „kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen" eine Nachweiserbringung bzgl. der Einhaltung der Anforderungen gemäß § 8a Abs. 1 BSIG erfolgen. Für diese Prüfung außerhalb der Jahresabschlussprüfung vergleiche *IDW PH 9.860.2*[5].

13 Das Ergebnis der VAIT-Prüfung besteht in einer Berichterstattung über die durchgeführten Prüfungshandlungen, die Prüfungsfeststellungen sowie in einer Würdigung des VAIT-Prüfers zu den einzelnen negativen Prüfungsfeststellungen im Hinblick auf deren Schweregrad (Klassifizierung) (vgl. Tz. 67).

4. Anforderungen

4.1. Berufspflichten

14 Der VAIT-Prüfer hat neben den allgemeinen Berufspflichten der Unabhängigkeit, Verschwiegenheit, Eigenverantwortlichkeit und Gewissenhaftigkeit (§§ 43 Abs. 1 Satz 1, 44, 49 und 50 WPO, §§ 1 – 12 BS WP/vBP) auch die besonderen Berufspflichten nach §§ 28 – 44 BS WP/vBP zu beachten.

4.2. Auftragsannahme

15 Vor der Auftragsannahme hat sich der VAIT-Prüfer zu vergewissern, dass die Regelungen des Qualitätssicherungssystems der WP-Praxis zur Auftragsannahme und Auftragsfortführung eingehalten werden.[6] Ein Auftrag zur Durchführung einer VAIT-Prüfung darf nur angenommen werden, wenn davon auszugehen ist, dass die Berufspflichten einschließlich des Unabhängigkeitsgrundsatzes eingehalten werden können. Hierzu hat der VAIT-Prüfer sich auch zu vergewissern, dass ausreichende Erfahrung und Kompetenz sowie personelle und zeitliche Ressourcen in der WP-Praxis vorhanden sind oder erlangt werden können, um den Auftrag ordnungsgemäß durchführen zu können (§4 Abs. 2 BS WP/vBP).

16 Bei der notwendigen Beurteilung der Auftragsrisiken vor Auftragsannahme hat der VAIT-Prüfer festzustellen, ob das vorgesehene Prüfungsteam insgesamt über die für die Durchführung des Auftrags notwendigen Fach- und Branchenkenntnisse verfügt, Erfahrungen mit den einschlägigen rechtlichen Anforderungen vorliegen oder erlangt werden können und erforderlichenfalls Sachverständige des VAIT-Prüfers (vgl. Tz. A6) zur Verfügung stehen.[7] Zudem hat der VAIT-

---

5 *IDW Prüfungshinweis: Die Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen (IDW PH 9.860.2)* (Stand: 21.06.2019).

6 Vgl. *IDW Qualitätsmanagementstandard: Anforderungen an das Qualitätsmanagement in der Wirtschaftsprüferpraxis (IDW QMS 1 (09.2022))* (Stand: 28.09.2022), Tz. 28 sowie 49. WP-Praxen haben gemäß *IDW QMS 1 (09.2022)*, Tz. 6 ihre Qualitätsmanagementsysteme bis zum 15. Dezember 2023 entsprechend den Anforderungen des *IDW QMS 1 (09.2022)* auszugestalten und einzurichten. Bei einer freiwilligen vorzeitigen Anwendung des *IDW EPS 590 (07.2023)* sind bis zum 15. Dezember 2023 die einschlägigen Anforderungen des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* (Stand: 09.06.2017) anzuwenden, sofern nicht eine freiwillige frühere Anwendung des *IDW QMS 1 (09.2022)* erfolgt.

7 Vgl. *IDW QMS 1 (09.2022)* (Stand: 28.09.2022), Tz. 49 und 51.

Prüfer festzustellen, ob er davon ausgehen kann, dass die erforderlichen Prüfungsnachweise erlangt werden.

17 Der Jahresabschlussprüfer des Versicherungsunternehmens darf als VAIT-Prüfer beauftragt werden.

18 Der VAIT-Prüfer hat mit dem Auftraggeber die Auftragsbedingungen – insb. die Verantwortlichkeiten der gesetzlichen Vertreter und des VAIT-Prüfers – schriftlich zu vereinbaren (vgl. Tz. A4).

19 Werden dem VAIT-Prüfer nach Auftragsannahme Informationen bekannt, die – wenn sie ihm vorher bekannt geworden wären – zur Ablehnung des Auftrags geführt hätten, hat er über die erforderlichen Schritte zu entscheiden (vgl. Tz. A7).[8]

4.3. Aufbau, Planung und Durchführung der VAIT-Prüfung

4.3.1. Aufbau und Planung der VAIT-Prüfung

20 Bei der VAIT-Prüfung hat der Prüfer die folgenden Schritte durchzuführen (vgl. Tz. A8):

a. Würdigung des „Soll-Objekts“: Erfassung und Würdigung der Eignung (als Maßstab der Beurteilung in b.) der aus den VAIT durch das Versicherungsunternehmens als erforderlich abgeleiteten technisch-organisatorischen Vorgaben (d.h. vom Versicherungsunternehmen konkretisierte Ausgestaltung der VAIT in der Aufbau- und Ablauforganisation) (vgl. Abschn. 4.3.2.1),

b. Angemessenheitsprüfung: Beurteilung der angemessenen Umsetzung dieser technisch-organisatorischen Vorgaben in Prozesse, Regelungen und Verfahren (vgl. Abschn. 4.3.2.2),

c. Wirksamkeitsprüfung: Beurteilung der Einhaltung von vorgegebenen Prozessen, Regelungen und Verfahren in dem zu prüfenden Zeitraum (vgl. Abschn. 4.3.2.3).

21 Der VAIT-Prüfer hat die VAIT-Prüfung in sachlicher, personeller und zeitlicher Hinsicht so zu planen, dass sie in sachgerechter Weise durchgeführt werden kann. Dabei hat er die Art, die zeitliche Einteilung und den Umfang der geplanten Prüfungshandlungen festzulegen, die erforderlich sind, um die Zielsetzung der VAIT-Prüfung (vgl. Tz. 11) zu erreichen. Der VAIT-Prüfer hat die Planung so auszugestalten, dass alle Kapitel (mit Ausnahme des KRITIS-Kapitels, vgl. Tz. 12) der VAIT in die Prüfung einbezogen werden.

22 Ist eine Änderung der VAIT bzw. der technisch-organisatorischen Vorkehrungen im Berichtszeitraum erfolgt, so hat der VAIT-Prüfer dies in Abhängigkeit von den jeweiligen Umständen bei der Planung der VAIT-Prüfung zu berücksichtigen. Sofern mit dem Auftraggeber vereinbart wurde, dass über den aktuellen Stand der VAIT hinaus ergänzend auch weitere aufsichtliche Anforderungen an die IT (vgl. Tz. 10) zu beachten sind, hat der VAIT-Prüfer dies bei der Planung zu berücksichtigen.

23 Bei der Planung und Durchführung der VAIT-Prüfung hat der VAIT-Prüfer den Grundsatz der Proportionalität zu beachten (vgl. Tz. A9). Dabei hat der Prüfer im Rahmen der VAIT-Prüfung zu berücksichtigen, ob die Umsetzung der VAIT durch das Versicherungsunternehmen auf

[8] Vgl. *IDW QMS 1 (09.2022)* (Stand: 28.09.2022), Tz. 53 und A101.

eine Weise erfüllt wird, die der Wesensart, dem Umfang und der Komplexität der mit der Tätigkeit des Unternehmens einhergehenden Risiken (im Weiteren „Risikoprofil“) gerecht wird (§ 296 Abs. 1 VAG). Daher hat der VAIT-Prüfer bei der Planung seiner Tätigkeiten neben der technisch-organisatorischen Ausgestaltung der IT sowie der zu betrachtenden IT-Systeme und Infrastrukturen auch insb. die Größe und Komplexität des Versicherungsunternehmens sowie Art und Umfang des betriebenen Geschäfts zu berücksichtigen.

24 Entsprechend den Grundsätzen der risikoorientierten Prüfung und der Wesentlichkeit bei aufsichtlichen Prüfungen nach *IDW EPS 526 (03.2023)* hat der VAIT-Prüfer für das Versicherungsunternehmen und in Bezug auf die Kapitel der VAIT anhand geeigneter Indikatoren (vgl. Tz. A10) Risiko- und Wesentlichkeitseinschätzungen vorzunehmen, welche als Basis für die VAIT-Prüfung dienen.

25 Wurde für den zu prüfenden Zeitraum eine Prüfung gemäß § 294 Abs. 1 bis 5 und Abs. 8, § 306 Abs. 1 Satz 1 Nr. 1 VAG hinsichtlich der Einhaltung der VAIT durch die BaFin durchgeführt, hat der VAIT-Prüfer die Ergebnisse dieser Prüfung bei der Prüfung der aufsichtlichen Anforderungen der VAIT eigenverantwortlich zu nutzen. Der VAIT-Prüfer hat anhand des Prüfungsberichts ein Verständnis von den Tätigkeiten der BaFin zu gewinnen und die Eignung der Tätigkeit der BaFin als Prüfungsnachweis für die VAIT-Prüfung zu würdigen. Für den Fall, dass Beanstandungen getroffen wurden, ist zu prüfen, ob die Mängel fortbestehen oder abgestellt wurden.

26 Bei der Auswahl der Mitglieder des Prüfungsteams hat der VAIT-Prüfer festzustellen, dass diese insgesamt über ausreichende praktische Erfahrungen mit IT-Prüfungen, einschlägigen gängigen Standards sowie die notwendigen Branchen- und, sofern einschlägig, Rechtskenntnisse verfügen, um den Auftrag ordnungsgemäß durchführen zu können. Das Prüfungsteam hat über ausreichende Kenntnisse der VAIT zu verfügen, auf deren Einhaltung die technisch-organisatorischen Vorkehrungen abzielen.

27 Der VAIT-Prüfer hat sich zu vergewissern, dass das Prüfungsteam bei der Hinzuziehung von Sachverständigen, die nicht Mitglied des Prüfungsteams sind, sowie von anderen Prüfern im erforderlichen Umfang in die Tätigkeit des Sachverständigen bzw. des anderen Prüfers eingebunden werden kann, um die Verantwortung für seine Prüfungsfeststellungen übernehmen zu können (vgl. Tz. 41).

28 Auf der Grundlage der durchgeführten Tätigkeiten und der erlangten Informationen hat der VAIT-Prüfer vor Beendigung der VAIT-Prüfung zu würdigen, ob die der Planung zugrunde gelegten Annahmen unverändert zutreffen.

4.3.2. Durchführung

4.3.2.1. Würdigung des Soll-Objekts

29 Der VAIT-Prüfer hat zu würdigen, ob das Versicherungsunternehmen aus den für sein Geschäftsmodell einschlägigen VAIT erforderliche technisch-organisatorische Vorgaben abgeleitet hat (vgl. Tz. A13 f.).

30 Der VAIT-Prüfer hat sich als Grundlage für seine Würdigung des Soll-Objekts ein umfassendes Bild von den Prozessen, Regelungen und Verfahren des Versicherungsunternehmen zu machen, welche der Umsetzung der VAIT dienen (vgl. Tz. A15 f.).

31 Die Würdigung des Soll-Objekts hat auf Basis geeigneter Maßstäbe zu erfolgen (vgl. Tz. A18).

4.3.2.2. Angemessenheitsprüfung

32 Die Angemessenheitsprüfung dient der Beurteilung, ob das Versicherungsunternehmen die aus den VAIT abgeleiteten erforderlichen technisch-organisatorischen Vorgaben angemessen in Prozesse, Regelungen und Verfahren umgesetzt hat, um die aufsichtlichen Anforderungen zu erfüllen (vgl. Tz. A8).

33 Zur Gewinnung von Prüfungsnachweisen im Rahmen der Angemessenheitsprüfung hat der VAIT-Prüfer geeignete Prüfungshandlungen durchzuführen (vgl. Tz. A19).

4.3.2.3. Wirksamkeitsprüfung

34 Der VAIT-Prüfer hat die Wirksamkeit der Prozesse, Regelungen und Verfahren im zu prüfenden Zeitraum zu beurteilen.

35 Im Rahmen von Wirksamkeitsprüfungen hat der VAIT-Prüfer geeignete Prüfungshandlungen durchzuführen, um Prüfungsnachweise zur Wirksamkeit der Prozesse, Regelungen und Verfahren zu gewinnen. Art und Umfang (u.a. eine nachvollziehbare Auswahl von Elementen) der Prüfungshandlungen liegen im Ermessen des VAIT-Prüfers (vgl. Tz. A20).

36 Bei der Beurteilung der Kontinuität der Funktion der umgesetzten Prozesse, Regelungen und Verfahren hat der VAIT-Prüfer zu beachten, dass die Wirksamkeitsprüfung einen angemessenen Zeitraum abdeckt, i.d.R. ein Jahr bzw. mindestens ein halbes Geschäftsjahr.

37 Führt die Angemessenheitsprüfung zu dem Ergebnis, dass Prozesse, Regelungen und Verfahren die Anforderungen der VAIT nicht erfüllen, ist insoweit keine Wirksamkeitsprüfung durchzuführen (zu den Folgen für die Berichterstattung vgl. Tz. 64).

4.3.3. Prüfungsnachweise

38 Bei der Planung und Durchführung von Prüfungshandlungen hat der VAIT-Prüfer die Relevanz und Verlässlichkeit der als Prüfungsnachweise zu nutzenden Informationen – einschließlich der aus externen Informationsquellen erlangten Informationen – zu würdigen. Falls

a. aus einer Quelle erlangte Nachweise nicht mit aus einer anderen Quelle erlangten Nachweisen in Einklang stehen oder

b. der VAIT-Prüfer Zweifel an der Verlässlichkeit der als Nachweise zu nutzenden Informationen hat,

hat der VAIT-Prüfer festzustellen, welche Anpassungen oder Ergänzungen der Prüfungshandlungen notwendig sind, um den Sachverhalt zu klären, und die etwaigen Auswirkungen des Sachverhalts auf andere Aspekte der Prüfung abzuwägen.

39 Bei als Prüfungsnachweise zu nutzenden Informationen, die durch das Versicherungsunternehmen erstellt wurden, hat der VAIT-Prüfer zu beurteilen, ob die Informationen für die Zielsetzung des VAIT-Prüfers ausreichend verlässlich sind. Je nach den Umständen schließt dies erforderlichenfalls ein

a. die Erlangung von Prüfungsnachweisen über die Genauigkeit und Vollständigkeit der Informationen und

b. die Beurteilung, ob die Informationen für die Zielsetzung des VAIT-Prüfers ausreichend genau und detailliert sind.

40 Falls als Prüfungsnachweise zu nutzende Informationen unter Verwendung der Tätigkeiten eines Sachverständigen der gesetzlichen Vertreter erstellt wurden, hat der VAIT-Prüfer, soweit notwendig, unter Berücksichtigung der Bedeutung der Tätigkeit dieses Sachverständigen für die Zwecke des VAIT-Prüfers

a. die Kompetenz, Fähigkeiten und Objektivität dieses Sachverständigen zu beurteilen,

b. ein Verständnis von den Tätigkeiten dieses Sachverständigen zu erlangen, und

c. die Angemessenheit der Tätigkeiten dieses Sachverständigen als Prüfungsnachweis zu beurteilen.

41 Wenn die Tätigkeiten eines Sachverständigen des VAIT-Prüfers als Prüfungsnachweise zu nutzen sind, hat der VAIT-Prüfer auch

a. zu beurteilen, ob dieser Sachverständige über die für Zwecke des VAIT-Prüfers notwendige Kompetenz, Fähigkeiten und Objektivität verfügt. Im Falle eines externen Sachverständigen des VAIT-Prüfers hat die Beurteilung der Objektivität eine Befragung zu den Interessen und den Beziehungen einzuschließen, die eine Gefährdung der Objektivität dieses Sachverständigen hervorrufen können,

b. ein ausreichendes Verständnis von dem Fachgebiet des Sachverständigen zu erlangen,

c. mit dem Sachverständigen Art, Umfang und Ziele der Tätigkeiten zu vereinbaren, und

d. die Angemessenheit der Tätigkeiten des Sachverständigen für die Zwecke des VAIT-Prüfers zu beurteilen.

42 Wenn die Tätigkeiten eines anderen Prüfers zu nutzen sind oder im Hinblick auf ausgelagerte Dienstleistungen bei Dienstleistungsunternehmen genutzt werden sollen, hat der VAIT-Prüfer zu beurteilen, ob diese Tätigkeiten für die Zwecke des VAIT-Prüfers angemessen sind.

43 Im Falle von Beanstandungen eines anderen Prüfers oder Sachverständigen, sind diese daraufhin zu würdigen, welche Auswirkungen diese auf die VAIT-Prüfung haben und ob und inwieweit sich die Notwendigkeit ergänzender Prüfungshandlungen ergibt.

44 Soweit der VAIT-Prüfer plant, Tätigkeiten der Internen Revision im Rahmen der VAIT-Prüfung zu nutzen, hat der VAIT-Prüfer zu beurteilen,

a. inwieweit die Stellung der Internen Revision innerhalb des Versicherungsunternehmens sowie relevante Regelungen und Maßnahmen die Objektivität der Innenrevisoren fördern,

b. wie kompetent die Interne Revision ist,

c. ob die Interne Revision einer systematischen und geregelten Vorgehensweise, einschließlich Qualitätssicherung, folgt und

d. ob die Tätigkeiten der Internen Revision für die Zwecke der VAIT-Prüfung angemessen sind.

4.3.4. Ereignisse nach dem Ende des zu prüfenden Zeitraums

45 Der VAIT-Prüfer hat die Auswirkungen von Ereignissen nach dem Ende des zu prüfenden Zeitraums auf die zur Einhaltung der nach den VAIT eingerichteten technisch-organisatorischen Vorkehrungen und seinen Prüfungsfeststellungen bis zum Datum des Prüfungsberichts zu würdigen (vgl. Tz. A22).

46 Der VAIT-Prüfer ist nicht verpflichtet, nach dem Datum des Prüfungsberichts Prüfungshandlungen durchzuführen.

47 Falls dem VAIT-Prüfer nach dem Datum der Herausgabe des Prüfungsberichts Sachverhalte bekannt werden, die dazu führen, dass die Prüfungsfeststellungen in der getroffenen Form nicht hätten abgegeben werden dürfen, hat er angemessene Maßnahmen zu ergreifen, damit die vorgesehenen Nutzer hiervon Kenntnis erlangen.

4.3.5. Schriftliche Erklärungen

48 Der VAIT-Prüfer hat von den gesetzlichen Vertretern des Versicherungsunternehmens eine Vollständigkeitserklärung einzuholen, in der von diesen erklärt wird, dass dem VAIT-Prüfer alle relevanten Aufklärungen und Informationen bzw. Nachweise gegeben wurden. Zu den relevanten Informationen gehört auch die Mitteilung aller geplanten bedeutsamen Änderungen der vom Versicherungsunternehmen zur Einhaltung der VAIT eingerichteten technisch-organisatorischen Vorkehrungen. Die Einholung der Vollständigkeitserklärung ist kein Ersatz für andere nach den Anforderungen dieses *IDW Prüfungsstandards* durchzuführende Prüfungshandlungen.

49 Wenn der VAIT-Prüfer feststellt, dass es notwendig ist, über die im Rahmen der Vollständigkeitserklärung angeforderten Erklärungen hinaus weitere schriftliche Erklärungen zu erlangen, um andere für die VAIT-Prüfung relevante Prüfungsnachweise zu stützen, hat er diese weiteren schriftlichen Erklärungen einzuholen.

50 Sofern sich einzelne Aspekte der Vollständigkeitserklärung oder ggf. weitere schriftliche Erklärungen auf Sachverhalte beziehen, die bedeutsam für die VAIT-Prüfung sind, hat der VAIT-Prüfer

a. die Vertretbarkeit dieser Erklärung(en) und deren Konsistenz zu anderen erlangten Nachweisen, einschließlich anderer mündlicher oder schriftlicher Erklärungen der gesetzlichen Vertreter, zu beurteilen,
b. abzuwägen, ob zu erwarten ist, dass die Personen, welche die schriftlichen Erklärungen abgeben, in Bezug auf die betreffenden Sachverhalte ausreichend informiert sind.

51 Die Vollständigkeitserklärung ist zeitnah zum Datum des Prüfungsberichts zu datieren, aber darf nicht nach diesem datiert werden.

52 Werden eine oder mehrere angeforderte schriftliche Erklärungen nicht abgegeben, oder zieht der VAIT-Prüfer den Schluss, dass es begründete Zweifel an der Kompetenz, der Integrität, den berufsethischen Wertvorstellungen oder die Sorgfalt der Personen, welche die Vollständigkeitserklärung abgeben, oder dass die erteilten Erklärungen anderweitig nicht verlässlich sind, hat der VAIT-Prüfer

a. den Sachverhalt mit den gesetzlichen Vertretern zu erörtern,

b. die Integrität derer, von denen die Erklärungen angefordert oder erhalten wurden, erneut zu beurteilen und zu würdigen, welche Auswirkungen dies auf die Verlässlichkeit von (mündlichen oder schriftlichen) Erklärungen und Nachweisen haben kann, und

c. angemessene Maßnahmen zu ergreifen, einschließlich der Feststellung der möglichen Auswirkungen auf die Prüfungsfeststellungen.

4.4. Dokumentation

53 Der VAIT-Prüfer hat zeitgerecht eine Auftragsdokumentation zu erstellen. Die in der Auftragsdokumentation enthaltenen Aufzeichnungen dienen als Grundlage für die vom VAIT-Prüfer getroffenen Aussagen. Die Auftragsdokumentation muss ausreichend und geeignet sein, einen erfahrenen, zuvor nicht mit dem Auftrag befassten Wirtschaftsprüfer in die Lage zu versetzen, Folgendes nachvollziehen zu können:

a. Die für das jeweilige Prüffeld prägenden Merkmale, ggf. unter Verweis auf die Merkmale, die für das Versicherungsunternehmen als Ganzes oder für die Mehrzahl der Prüffelder prägend sind (vgl. Tz. 62, Anlage 1)

b. Art, zeitliche Einteilung und Umfang der Prüfungshandlungen, die durchgeführt wurden, um diesen *IDW Prüfungsstandard* einzuhalten

c. die Ergebnisse der durchgeführten Prüfungshandlungen und die erlangten Nachweise sowie

d. die den bedeutsamen Feststellungen zugrundeliegenden Sachverhalte, Schlussfolgerungen und Beurteilungen nach pflichtgemäßem Ermessen.

54 Wenn der VAIT-Prüfer während der Prüfungsdurchführung Informationen erlangt, die im Widerspruch zu den bisher erlangten Informationen für eine Feststellung stehen, hat er zu dokumentieren, wie er diese widersprüchlichen Informationen bei der abschließenden Beurteilung der Feststellung berücksichtigt hat.

55 Der VAIT-Prüfer hat die Auftragsdokumentation in einer Auftragsakte zusammenzustellen. Der Abschluss des redaktionellen Prozesses der Dokumentation der VAIT-Prüfung hat spätestens mit dem Datum des Prüfungsberichts abzuschließen.

56 Nachdem der VAIT-Prüfer die Zusammenstellung der endgültigen Auftragsakte abgeschlossen hat, darf er jegliche Art von Auftragsdokumentation nicht vor dem Ende des jeweiligen Aufbewahrungszeitraums löschen oder entfernen.

57 Wenn es der VAIT-Prüfer als notwendig erachtet, nach Abschluss der Zusammenstellung der endgültigen Auftragsakte die bestehende Auftragsdokumentation anzupassen oder eine neue Auftragsdokumentation hinzuzufügen, hat er unabhängig von der Art der Anpassungen oder Ergänzungen Folgendes zu dokumentieren:

a. Die genauen Gründe für die Anpassungen oder Ergänzungen sowie

b. wann und von wem diese vorgenommen und durchgesehen wurden.

4.5. Berichterstattung

58 Der VAIT-Prüfer hat einen schriftlichen Prüfungsbericht zu verfassen. Der Prüfungsbericht muss folgende Bestandteile enthalten:

a. Überschrift: Angabe, dass es sich um den Bericht eines unabhängigen VAIT-Prüfers handelt

b. beabsichtigte Nutzer des Prüfungsberichts

c. Prüfungsauftrag einschließlich der Angabe des Prüfungszeitraums

d. Gegenstand, Art und Umfang der Prüfung einschließlich einer zusammenfassenden Beschreibung der durchgeführten Prüfungshandlungen (Würdigung des „Soll-Objekts“, Angemessenheitsprüfung, und Wirksamkeitsprüfung sowie der zusätzlichen Prüfungshandlungen) (vgl. Tz. 62 f.)

e. Beschreibung der Verantwortlichkeiten der gesetzlichen Vertreter und des VAIT-Prüfers (vgl. Tz. 59)

f. Aussage, dass die Prüfung in Übereinstimmung mit diesem *IDW Prüfungsstandard* durchgeführt wurde; der VAIT-Prüfer darf nicht die Einhaltung dieses *IDW Prüfungsstandard*s erklären, wenn er nicht sämtliche einschlägigen Anforderungen beachtet hat

g. Aussage, dass bei der Prüfung die Berufspflichten der WPO und der Berufssatzung WP/vBP, einschließlich der Anforderungen an die Unabhängigkeit, eingehalten werden und dass die WP-Praxis die Anforderungen an die Qualitätssicherung anwendet

h. ggf. Benennung spezifischer Prüfungshandlungen oder von Besonderheiten bei Beurteilungskriterien, soweit diese nicht durch die allgemeinen Erläuterungen abgedeckt sind bzw. für das Verständnis von Prüfungsfeststellungen als zweckdienlich angesehen werden

i. Angabe der Prüfungsfeststellungen sowie Beanstandungen; dabei müssen wesentliche Beanstandungen als solche erkennbar sein (vgl. Tz. 67 ff.)

j. falls relevant: Aussage, dass der Auftrag für einen bestimmten Zweck bzw. Adressatenkreis durchgeführt wurde und deshalb die Verwendung der Ergebnisse für andere Zwecke ausgeschlossen ist

k. zusammenfassende Schlussbemerkung

l. eine Aussage über die inhärenten Grenzen der geprüften zur Einhaltung der VAIT eingerichteten technisch-organisatorischen Vorkehrungen und zum Risiko, die Feststellungen zu den geprüften technisch-organisatorischen Vorkehrungen auf die Zukunft zu übertragen; zudem ein Hinweis, dass die Einschätzung der BaFin zu Prüfungsfeststellungen und deren Schweregrad von der Einschätzung des VAIT-Prüfers abweichen kann

m. Datum des Prüfungsberichts: Das Datum darf nicht vor dem Datum liegen, an dem der VAIT-Prüfer ausreichende und angemessene Nachweise als Grundlage für die Prüfungsfeststellungen zur Einhaltung der VAIT erlangt hat.

n. Name und Ort des VAIT-Prüfers

o. Unterschrift des VAIT-Prüfers.

59 In die Beschreibung der Verantwortlichkeiten der gesetzlichen Vertreter und des VAIT-Prüfers (vgl. Tz. 58e) hat der VAIT-Prüfer aufzunehmen, dass die gesetzlichen Vertreter des Versicherungsunternehmens für die Einhaltung der an das beaufsichtigte Versicherungsunternehmen gerichteten aufsichtlichen Anforderungen einschließlich der VAIT und demzufolge auch für die Ableitung und Einrichtung der zur Einhaltung der VAIT notwendigen angemessenen und wirksamen technisch-organisatorischen Vorkehrungen verantwortlich sind. Zudem hat der VAIT-Prüfer aufzunehmen, dass die Mitglieder des Aufsichtsorgans für die Wahrnehmung ihrer Überwachungsfunktion verantwortlich sind, einschließlich der Überwachung der gesetzlichen Vertreter bei der Erfüllung der an das beaufsichtigte Versicherungsunternehmen gerichteten aufsichtlichen Anforderungen. Schließlich hat der VAIT-Prüfer auch aufzunehmen, dass die gesetzlichen Vertreter die Verantwortung für die Richtigkeit und Vollständigkeit der dem VAIT-Prüfer erteilten Auskünfte und Erläuterungen sowie zur Verfügung gestellten Unterlagen tragen.

60 Der VAIT-Prüfer hat bei der Darstellung seiner Verantwortung (vgl. Tz. 11 f.) zudem auch aufzunehmen, dass er die Aufgabe hat, die erteilten Auskünfte und Erläuterungen sowie die zur Verfügung gestellten Unterlagen im Rahmen seiner Tätigkeiten zu berücksichtigen und zu würdigen.

61 Im Rahmen der Berichterstattung hat der VAIT-Prüfer anzugeben, ob die gesetzlichen Vertreter die verlangten Aufklärungen und Informationen bzw. Nachweise erbracht haben, welche der VAIT-Prüfer nach seinem pflichtgemäßen Ermessen zur ordnungsgemäßen Durchführung der VAIT-Prüfung benötigt. Kommen die gesetzlichen Vertreter diesen Pflichten nach, hat der VAIT-Prüfer zumindest die Feststellung aufzunehmen, dass alle verlangten Aufklärungen und Informationen bzw. Nachweise erbracht wurden. Auf eine eingeholte Vollständigkeitserklärung hat der VAIT-Prüfer zu verweisen. Hat der VAIT-Prüfer nicht die zur Durchführung seines Auftrags erforderlichen Aufklärungen, Informationen bzw. Nachweise von den gesetzlichen Vertretern des Versicherungsunternehmens erhalten bzw. wurden aufgetretene Zweifel nicht ausgeräumt, so hat er unbeschadet der Auswirkungen auf einzelne Feststellungen oder Darstellungen in der Berichterstattung darauf hinzuweisen.

62 Der VAIT-Prüfer hat zur Erläuterung von Art und Umfang der VAIT-Prüfung (vgl. Tz. 58d) die Grundsätze zu nennen, nach denen diese durchgeführt wurden (vgl. Tz. A23).

Der VAIT-Prüfer hat i.S. einer allgemeinen Erläuterung auch auf Merkmale des Versicherungsunternehmens (vgl. Anlage 1) einzugehen, die für die VAIT prägend sind.

63 Sofern einschlägig hat der VAIT-Prüfer bei der Beschreibung der Prüfungshandlungen (vgl. Tz. 58d) auch spezifische Prüfungshandlungen oder Besonderheiten bei der Beurteilung zu benennen, soweit diese nicht durch die allgemeinen Erläuterungen abgedeckt sind bzw. für das Verständnis von Prüfungsfeststellungen als zweckdienlich angesehen werden.

64 Für den Fall, dass die Angemessenheitsprüfung zu dem Ergebnis führt, dass Prozesse, Regelungen und Verfahren die Anforderungen der VAIT nicht erfüllen und als Folge davon insoweit keine Wirksamkeitsprüfung durchgeführt wurde (vgl. Tz. 37), hat der VAIT-Prüfer darauf in seiner Berichterstattung hinzuweisen.

65 Eine Darstellung der Prozesse, Regelungen und Verfahren des Versicherungsunternehmens zur Einhaltung der VAIT ist nur notwendig, soweit diese zum Verständnis der aus der Tätigkeit

des VAIT-Prüfers getroffenen Prüfungsfeststellungen, insb. bei Beanstandungen von Mängeln, erforderlich ist.

66 Sofern in Bezug auf die Umsetzung bestimmter Anforderungen keine bzw. nur unzureichende Aufzeichnungen durch das Versicherungsunternehmen erfolgen, liegt eine zu berichtende Beanstandung vor.

67 Der VAIT-Prüfer hat bei Beanstandungen eine Klassifizierung der Beanstandungen je Abschnitt der VAIT vorzunehmen (vgl. Tz. A24). Hierbei hat er die folgende Beschreibung des Klassifizierungsschemas der Feststellungen (F1 bis F4) anzuwenden:

- F1 geringfügig – bezieht sich auf einen Normenverstoß mit geringfügigen Auswirkungen
- F2 mittelschwer – bezieht sich auf einen Normenverstoß mit mittelschweren Auswirkungen
- F3 gewichtig – bezieht sich auf einen Normenverstoß mit gewichtigen Auswirkungen
- F4 schwerwiegend – bezieht sich auf einen Normenverstoß mit schwerwiegenden Auswirkungen

Die Klassifizierung der Feststellung ist zusammenfassend je Kapitel der VAIT vorzunehmen und nicht für die einzelnen Beanstandungen in den jeweiligen Kapiteln.

68 Bei der Berichterstattung ist in einer zusammenfassenden Schlussbemerkung zu allen wichtigen Fragen Stellung zu nehmen (vgl. Tz. A25). Dabei hat sich der VAIT-Prüfer auf bedeutsame Feststellungen (positiv wie negativ) zu beschränken. In diesem Rahmen hat der VAIT-Prüfer über aus seiner Sicht für die Berichtsadressaten wesentliche Beanstandungen (wesentliche negative Feststellungen als Teilmenge der bedeutsamen negativen Feststellungen) zu berichten. Wesentliche Beanstandungen i.S. des Prüfungsstandards sind zumindest mit F4 (schwerwiegende) oder F3 (gewichtige) klassifizierte Beanstandungen.

5. Anwendungshinweise und Erläuterungen

5.1. Vorbemerkung [Tz. 1 ff.]

A1 Dieser *IDW Prüfungsstandard* berücksichtigt die in *IDW EPS 526 (03.2023)*[9] dargestellten einschlägigen Anforderungen für die Durchführung aufsichtlicher Prüfungen im Rahmen der Abschlussprüfung von Instituten nach § 29 KWG.

5.2. Gegenstand und Ziel der Prüfung [Tz. 9 ff.]

A2 Im ersten Kapitel der VAIT (IT-Strategie) werden Anforderungen hinsichtlich der strategischen Ausrichtung des Unternehmens im Hinblick auf die Versicherungsaufsichtlichen Anforderungen an die IT beschrieben, deren Umsetzung in den folgenden Kapiteln der VAIT konkretisiert wird. In Teilen erstrecken sich die Anforderungen der VAIT bis in die operativen Bereiche eines Unternehmens hinein, sodass ein kompletter Querschnitt durch ein Unternehmen, von der

[9] *Entwurf eines IDW Prüfungsstandards: Pflichten des Abschlussprüfers nach § 29 KWG (IDW EPS 526) (03.2023)* (Stand: 29.03.2023).

Strategie bis zur operativen Umsetzung, gezogen wird. Folgende Aspekte werden in den VAIT entsprechend der Reihenfolge der Kapitel konkretisiert:

1. **IT-Strategie:** Anforderungen hinsichtlich der Inhalte und der Kommunikation der IT-Strategie, sowie der Erreichung der festgelegten Ziele
2. **IT-Governance:** Anforderungen hinsichtlich der Struktur zur Steuerung und Überwachung der IT auf Basis der IT-Strategie, sowie Vorgaben zur Ressourcenausstattung
3. **Informationsrisikomanagement:** Anforderungen hinsichtlich der angemessenen Ausgestaltung eines Informationsrisikomanagements inkl. der Festlegung eines Informationsverbundes
4. **Informationssicherheitsmanagement:** Anforderungen, um die Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität) angemessen zu adressieren und das Thema Informationssicherheit innerhalb des Unternehmens zu steuern
5. **Operative Informationssicherheit:** Anforderungen zur Umsetzung der Anforderungen des Informationssicherheitsmanagements, damit die IT-Systeme, die zugehörigen IT-Prozesse und sonstige Bestandteile des Informationsverbundes die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten ermöglichen
6. **Identitäts- und Rechtemanagement:** Anforderungen hinsichtlich der angemessenen Ausgestaltung von Zugriffs-, Zugangs- und Zutrittsrechten für die Bestandteile des Informationsverbunds
7. **IT-Projekte und Anwendungsentwicklung:** Diverse Anforderungen hinsichtlich des Managements von Projekten, der Entwicklung und des Testens von Anwendungen sowie des Umgangs mit Individueller Datenverarbeitung (IDV)
8. **IT-Betrieb:** Anforderungen hinsichtlich des operativen Betriebs von IT-Systemen; Diese umfassen u.a. die Themen Inventarisierung von IT-Systemen, Change- und Incident Management sowie Datensicherung
9. **Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen:** Anforderungen hinsichtlich der Ausgliederung von IT-Dienstleistungen bzw. der vorab durchzuführenden Risikoanalyse; Erkenntnisse aus der Risikoanalyse müssen gemäß VAIT angemessen in der Vertragsgestaltung berücksichtigt werden.
10. **IT-Notfallmanagement:** Anforderungen hinsichtlich der Widerstandsfähigkeit von Bereichen und Prozessen im Unternehmen, um in möglichen Notfallsituationen die Fortführung der Geschäftstätigkeit durch im Vorfeld definierte Verfahren zu ermöglichen
11. **Kritische Infrastrukturen:** Spezifische Anforderungen gelten für Versicherungen, die gemäß der KRITIS-Verordnung eine kritische Infrastruktur darstellen, wodurch die BaFin die Wichtigkeit der Umsetzung des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz – BSIG) im Rahmen der KRITIS-Verordnung zusätzlich unterstreicht. (Die Anforderungen an kritische Infrastrukturen sind nicht Gegenstand der Prüfung, vgl. Tz. 12).

A3 Eine VAIT-Prüfung nach diesem *IDW Prüfungsstandard* ist auf die Umsetzung der Anforderungen der VAIT als Ganzes ausgerichtet (vgl. Tz. 12). Dies schließt jedoch nicht aus, dass Wirtschaftsprüfer auch eine Prüfung einzelner Kapitel der VAIT vornehmen und hierbei auf die Anforderungen dieses *IDW Prüfungsstandards* zurückgreifen; insb. wenn über die Einhaltung

der Vorgaben der VAIT aus anderen Kapiteln der VAIT Kenntnisse vorliegen (z.B. aus vorherigen VAIT-Prüfungen) bzw. hierzu Annahmen getroffen werden können oder konkrete Vorgaben zu den durchzuführenden Beurteilungen (z.B. bei von der BaFin in Auftrag gegebene Sonderprüfungen) vereinbart wurden.

5.3. Auftragsannahme [Tz. 15 ff.]

A4 Folgende Aspekte werden im Allgemeinen mit dem Auftraggeber schriftlich vereinbart (vgl. Tz. 17):

- Ziel und Gegenstand der VAIT-Prüfung
- die Verantwortung der gesetzlichen Vertreter für die Einhaltung der VAIT
- Art und Umfang der VAIT-Prüfung und der Berichterstattung einschließlich einer Bezugnahme auf diesen *IDW Prüfungsstandard*
- die Tatsache, dass keine Vollprüfung, sondern eine Prüfung in einer Auswahl vorgenommen wird und deshalb ein unvermeidbares Risiko besteht, dass selbst wesentliche Verstöße gegen die VAIT unentdeckt bleiben
- Hinweise auf die Nutzung von Arbeiten der Internen Revision, anderer Prüfer sowie von Sachverständigen des VAIT-Prüfers
- das Erfordernis eines unbeschränkten Zugangs des VAIT-Prüfers zu den für die Prüfung erforderlichen Informationen und der Bereitschaft der gesetzlichen Vertreter, Auskünfte in dem erforderlichen Umfang vollständig und richtig zu erteilen
- die Grundlagen der Honorarabrechnung und für den Auslagenersatz
- Haftungsbeschränkungen
- die Verpflichtung der gesetzlichen Vertreter, eine Vollständigkeitserklärung abzugeben
- ggf. Verwendungsvorbehalt des VAIT-Prüfungsberichts sowie
- ggf. Hinweis auf Berichtspflichten gegenüber dem Aufsichtsorgan.

A5 Wenn der VAIT-Prüfer auch mit anderen Dienstleistungen (z.B. der Jahresabschlussprüfung des Versicherungsunternehmens) beauftragt war und er in deren Rahmen für die VAIT-Prüfung evtl. relevante Informationen erlangt hat, kann es sinnvoll sein zu vereinbaren, dass er das Ergebnis dieser Tätigkeiten bei der VAIT-Prüfung berücksichtigt.

A6 Bei den Sachverständigen des VAIT-Prüfers (vgl. Tz. 16) kann es sich z.B. um IT-Spezialisten bei der Beurteilung der Sicherheit von IT-gestützten Prozessen im Rahmen der VAIT-Prüfung handeln.

A7 Zu den erforderlichen Schritten bei nach Auftragsannahme bekannt gewordenen Informationen (vgl. Tz. 19), kann z.B. bei Unabhängigkeitsgefährdungen die Ergreifung von Schutzmaßnahmen i.S. von § 30 BS WP/vBP oder ggf. die Niederlegung des Mandats gehören.

5.4. Planung, Aufbau und Durchführung der VAIT-Prüfung

5.4.1. Aufbau und Planung der VAIT-Prüfung [Tz. 20 ff.]

A8 Die Würdigung des „Soll-Objekts“ (vgl. Abschn. 4.3.2.1) und die Angemessenheitsprüfung (vgl. Abschn. 4.3.2.2) werden häufig innerhalb eines Arbeitsschritts im Rahmen der VAIT-Prüfung erfolgen.

A9 Die Beachtung der Proportionalität (vgl. Tz. 23) ermöglicht es dem VAIT-Prüfer, bei der Planung die Prüfaktivitäten und Prüfungsschwerpunkte risikoorientiert für das jeweilige Versicherungsunternehmen festzulegen.

A10 Für die Risiko- und Wesentlichkeitseinschätzungen anhand geeigneter Indikatoren (vgl. Tz. 24) kann beispielhaft die Anlage 1 herangezogen werden.

A11 Für die Aufsichtliche Prüfung relevante Informationen können sich auch aus Medienberichten oder anderen externen Quellen ergeben.

A12 Entsprechende Möglichkeiten zur Nutzung von Erkenntnissen aus anderen Prüfungen können sich bspw. auch aus Controls Reports nach *IDW PS 951 n.F.*[10], ISAE 3402[11] oder SOC I&II[12] ergeben.

5.4.2. Würdigung des „Soll-Objekts“ [Tz. 29 ff]

A13 Die erforderlichen technisch-organisatorischen Vorgaben schlagen sich in einer durch Prozesse, Regelungen und Verfahren vom Versicherungsunternehmen konkretisierten Ausgestaltung der aufsichtlichen Anforderungen in der Aufbau- und Ablauforganisation nieder.

A14 Die Verantwortung für die Angemessenheit des Soll-Objekts liegt bei den gesetzlichen Vertretern des Versicherungsunternehmens.

A15 Zur Gewinnung eines umfassenden Bilds (vgl. Tz. 30) stützt sich der VAIT-Prüfer bspw. auf Beschlüsse, Leitlinien, Richtlinien, Handbücher, Anweisungen oder Anwendungsdokumentationen.

A16 Das abgeleitete Soll-Objekt (vgl. Tz. 30) dient dem VAIT-Prüfer als Beurteilungsmaßstab für die Beurteilung der angemessenen Umsetzung der Anforderungen aus den VAIT unter Berücksichtigung der Proportionalität.

A17 Bei der Würdigung, ob das Versicherungsunternehmen aus den für sein Geschäftsmodell einschlägigen VAIT erforderliche technisch-organisatorische Vorgaben abgeleitet hat, kann es sich anbieten, die erforderlichen technisch-organisatorischen Vorgaben des Versicherungsunternehmens je Kapitel der VAIT zu identifizieren.

---

[10] *IDW Prüfungsstandard: Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen IDW PS 951 n.F. (03.2021)* (Stand: 26.03.2021).

[11] International Standard on Assurance Engagements (ISAE) 3402 „Assurance Reports on Controls at a Service Organization“, IFAC, Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements, New York 2012, Part II, S. 117 ff.

[12] AICPA System and Organization Controls (SOC) Suite of Services: https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome (letzter Abruf: 06.07.2023).

A18 Für die Würdigung des Soll-Objekts auf Basis geeigneter Maßstäbe (vgl. Tz. 31) ist in der Anlage 1 beispielhaft ein Indikatorenkatalog beigefügt.

5.4.3. Angemessenheits- und Wirksamkeitsprüfung [Tz. 32 ff.]

A19 Zur Gewinnung von Prüfungsnachweisen im Rahmen der Angemessenheitsprüfung (vgl. Tz. 33) können folgende Prüfungshandlungen in Betracht kommen:

- Befragungen von Mitgliedern der Leitungsebene und sonstigen Mitarbeitern auf unterschiedlichen organisatorischen Ebenen
- Einsichtnahme in Unterlagen, z.B. Beschlüsse, Leitlinien, Richtlinien, Handbücher, Anweisungen, Anwendungsdokumentationen, Protokolle, Prozessbeschreibungen und Stellenbeschreibungen, sowie von Unterlagen, die im Rahmen der Umsetzung von Prozessen, Regelungen und Verfahren generiert werden
- Beobachtung bzw. Nachvollzug von Aktivitäten und Arbeitsabläufen im Versicherungsunternehmen (einschließlich IT-gestützter Verfahren) sowie ggf. von vorgesehenen Qualitätssicherungsmaßnahmen und definierter Kontrollverfahren.

A20 Gegenstand der Wirksamkeitsprüfungen können Kontrollen oder andere Maßnahmen zur wirksamen Durchführung von Prozessen und Verfahren bzw. zur Einhaltung von Regelungen sein. Bei Wirksamkeitsprüfungen insb. (vgl. Tz. 35) können folgende Prüfungshandlungen in Betracht kommen:

- Befragungen von Mitgliedern der Leitungsebene und Mitarbeitern auf den relevanten organisatorischen Ebenen
- Durchsicht von Unterlagen, die die Durchführung von Prozessen, Regelungen und Verfahren dokumentieren (z.B. Durchsicht von IT-Protokollierungen, systemseitige Parametereinstellungen, Dokumentationen über konkrete Erstellungs- und Kontrollaktivitäten)
- Beobachtungen von Tätigkeiten und Arbeitsabläufen unter Berücksichtigung von Prozessen, Regelungen und Verfahren
- Nachvollzug von Tätigkeiten.

A21 Es kann Fälle geben, in denen Prüfungshandlungen zur Beurteilung der Angemessenheit der Prozesse, Regelungen und Verfahren gleichzeitig sachgerechte Prüfungsnachweise zur Beurteilung von deren Wirksamkeit darstellen. Dies kann dann der Fall sein, wenn

- nur ein Element von dem Prozess / der Regelung / dem Verfahren betroffen ist oder
- es sich um automatisierte Prozesse / Kontrollen handelt,

und dieses / diese Gegenstand der Angemessenheitsprüfung waren („test of one“).

Im Regelfall wird es zur Prüfung der Wirksamkeit jedoch notwendig sein, eine Auswahl von Elementen zu treffen. Art (z.B. bewusste bzw. zufallsbasierte Auswahl) und Umfang der Auswahl von Elementen können von einer Reihe von Faktoren abhängen. Anhaltspunkte für die Bestimmung des Umfangs können sich nach prüferischem Ermessen aus einzelnen in Anlage 1 aufgeführten Indikatoren ergeben.

5.4.4. Ereignisse nach dem Ende des zu prüfenden Zeitraums [Tz. 45 ff.]

A22 Als Prüfungshandlungen zur Feststellung von Ereignissen nach Ende des prüfpflichtigen Zeitraums (vgl. Tz. 45) kommen z.B. in Betracht:

- Lesen von Protokollen über in diesem Zeitraum stattgefundene Sitzungen der Verwaltungsorgane des zu prüfenden Unternehmens
- Lesen von unternehmensinternen Berichten, wie z.B. Berichte der Internen Revision, sowie
- Befragungen von für die Einhaltung der VAIT operativ verantwortlichen Personen und erforderlichenfalls der gesetzlichen Vertreter und der Mitglieder des Aufsichtsorgans.

5.4.5. Berichterstattung [Tz. 58 ff.]

A23 Die Erläuterungen dienen (vgl. Tz. 62) dient dazu, den Adressaten in die Lage zu versetzen, Konsequenzen für die eigene Überwachungsaufgabe zu ziehen.

A24 Bei der Klassifizierung von Beanstandungen (Tz. 67) können Feststellungen, die über mehrere Jahre nicht behoben wurden, oder eine Kumulierung von Feststellungen in einer niedrigen Klassifizierungsstufe zu einer Einstufung in eine höhere Klassifizierung führen.

A25 Im Rahmen der Zusammenfassenden Schlussbemerkung (vgl. Tz. 68) können die Ausführungen zu vergleichbaren aufsichtlichen Sachverhalten in geeigneter Form zusammengefasst werden. In der Anlage 2 zu diesem *IDW Prüfungsstandard* ist ein Formulierungsbeispiel für eine zusammenfassende Schlussbemerkung enthalten.

A26 Da die freiwillige Prüfung der Einhaltung der VAIT keine Vorbehaltsaufgabe i.S. des § 48 Abs. 1 Satz 1 WPO ist, besteht keine Pflicht zur Führung des Siegels.

Anlagen

Anlage 1 – Indikatorenkatalog

Bei der Umsetzung der Anforderungen an die Geschäftsorganisation und somit auch der Ausgestaltung der Strukturen, IT-Systeme oder Prozesse spielt das Proportionalitätsprinzip eine erhebliche Rolle. Die Anforderungen sind auf eine Weise zu erfüllen, die der Wesensart, dem Umfang und der Komplexität der mit der Tätigkeit des Unternehmens einhergehenden Risiken (im Weiteren „Risikoprofil“) gerecht wird (§ 296 Abs. 1 VAG). Das Proportionalitätsprinzip knüpft also an das individuelle Risikoprofil eines jeden Unternehmens an.

Ausgehend vom Grundsatz der Proportionalität, wurde beispielhaft nachfolgender Indikatorenkatalog erarbeitet. Hierbei werden mögliche Indikatoren in den Bereichen betriebenes Geschäft, Organisation des Versicherungsgeschäfts, Komplexität der Infrastruktur sowie weitere bedeutsame Eigenschaften) zur Einschätzung der Proportionalität aufgeführt.

	Proportionalität: Angemessenheit der Umsetzung der organisatorischen Vorkehrungen auf Ebene des Versicherungsunternehmens
Betriebenes Geschäft	● Betriebene Sparten (Sach, Leben und Kranken) sowie Anteil der einzelnen Sparten am Gesamtgeschäft des Versicherungsunternehmens ● passive/aktive Rückversicherung ● Anzahl Versicherungszweige/Produkte sowie Anteil am Gesamtgeschäftsvolumen ● Kundengruppen (Privat, Gewerbe, Industrie, institutionelles Geschäft B2B) ● Art und Umfang der Anlageklassen ● monetäres Volumen wesentlicher KPI’s, z.B. Beiträge, Schäden/Leistungen, Schadenrückstellung, Deckungsrückstellung, Alterungsrückstellung, Kapitalanlagen ● Anzahl Verträge/Schäden/Leistungsfälle je Sparte/Zweige/Produkte
Organisation des Versicherungsunternehmens	● Komplexität der Geschäftsorganisation (Anzahl Gesellschaften, Shared Servicecenter, lokale oder globale Organisation ● Grad der Ausgliederung/Fremdbezug (konzerninterne Servicegesellschaft, externe Services wie IBM, DXC, sowie Nutzung von Cloud Services) ● Organisation der IT (Verortung in der Gesamtorganisation, aufbauorganisatorische Gliederung, Aufhängung des CISO) ● Ablauforganisation (z.B. agile Organisation, DevOps etc.)
Komplexität der Infrastruktur	● Anzahl/Art der Technologien (Hardware, Betriebssysteme, Datenbanken, Programmiersprachen) ● Komplexität der Anwendungslandschaft (redundante Systeme, Anteil Host-basierter Systeme, Eigenentwicklungen vs. Standardsoftware) ● Projektlandschaft (Änderungshäufigkeit, Decommissioning-Programme) ● Alter der Systeme/Infrastruktur (Wartung vorhanden) ● Die IT-Systeme werden zentral oder dezentral betrieben

	Proportionalität: Angemessenheit der Umsetzung der organisatorischen Vorkehrungen auf Ebene des Versicherungsunternehmens
Weitere bedeutsame Eigenschaften	● Mitarbeiterstruktur in der IT (Alter, Know How) und Anzahl sowie Anteil an der Gesamtbelegschaft ● Fluktuation auf Führungspositionen in der IT ● Anzahl abgebrochene Projekte im Verhältnis zu allen Projekten (nach Größenclustern) ● Auffälligkeiten hinsichtlich Systemausfälle, Incidents, Data breaches, Cyberangriffe etc. ● Hinweise auf Verstöße aus internen und externen Prüfungen

Anlage 2 – Musterberichterstattung

Zusammenfassende Schlussbemerkung

Um Feststellungen zur Angemessenheit und Wirksamkeit der vom Versicherungsunternehmen zur Einhaltung der nach den VAIT eingerichteten technisch-organisatorischen Vorkehrungen zu treffen, haben wir die dargestellten Prüfungshandlungen durchgeführt. Hierzu haben wir die aus den VAIT durch das Versicherungsunternehmen als erforderlich abgeleiteten technisch-organisatorischen Vorgaben erfasst und deren Eignung basierend auf den im Abschn. […] dargestellten Indikatoren gewürdigt (Würdigung des Soll-Objekts).

Auf der Grundlage der dargestellten und durchgeführten Prüfungshandlungen vorgenommenen Beurteilung [mit Ausnahme der nachfolgend dargestellten Feststellungen] wurde keine unangemessene Umsetzung der aus den VAIT durch das Versicherungsunternehmen als erforderlich abgeleiteten technisch-organisatorischen Vorgaben in den Prozessen, Regelungen und Verfahren festgestellt.

Nach unserer auf der Grundlage der dargestellten durchgeführten Prüfungshandlungen vorgenommenen Beurteilung haben wir [mit Ausnahme der nachfolgend dargestellten Ausnahmen] keine mangelnde Einhaltung der Prozesse, Regelungen und Verfahren der durch das Versicherungsunternehmen vorgegebenen Prozesse, Regelungen und Verfahren im Zeitraum vom [*Datum*] bis [*Datum*] festgestellt.

Die von uns getroffenen Feststellungen sind hiernach im Einzelnen ausgeführt:

[…]

Wir weisen darauf hin, dass unsere Feststellungen in keiner Weise die Auffassung der Aufsichtsbehörden, insb. der BaFin, vorwegnimmt. Die aufsichtliche Prüfung der Einhaltung der VAIT basiert auf den VAIT mit Stand [*Datum*] sowie ergänzenden Veröffentlichungen und Auslegungen der BaFin bis zum [*Datum*]. Künftige Entwicklungen der VAIT oder ihrer Interpretationen können daher die Einschätzung in einer derzeit nicht vorhersehbaren Weise ändern.