IDW Sonderdruck

IDW Verlautbarungen zur IT-Prüfung außerhalb der Abschlussprüfung

1. Auflage

IDW VERLAG GMBH

Gesamtherstellung: IDW Verlag GmbH, Düsseldorf
KN 11903/0/0

ISBN 978-3-8021-2491-0

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://www.d-nb.de abrufbar.

www.idw-verlag.de

Inhalt

IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)

(Stand: 02.03.2018)

IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)

(Stand: 02.03.2018)[1]

[1] Verabschiedet vom Fachausschuss für Informationstechnologie (FAIT) am 14.02.2018. Billigende Kenntnisnahme durch den Hauptfachausschuss (HFA) am 02.03.2018. Redaktionelle Änderungen aufgrund der Anpassung an die neuen, vom IDW festgestellten deutschen Grundsätze ordnungsmäßiger Abschlussprüfung (vgl. ISA [DE] 200, Anlage D.1) am 26.03.2021.

1. Einleitung

1.1. Vorbemerkungen

1 Unternehmen nehmen häufig Veränderungen an den von ihnen eingesetzten IT-Systemen vor. Aufgrund der stetig steigenden Anforderungen an die Einhaltung der Ordnungsmäßigkeit, Sicherheit sowie Compliance der IT-Systeme ergibt sich hieraus der Bedarf, diese Veränderungen außerhalb der Abschlussprüfung durch einen Wirtschaftsprüfer prüfen zu lassen (vgl. Tz. A1).

2 Prüfungen i.S. dieses IDW Prüfungsstandards sind betriebswirtschaftliche Prüfungen, bei denen der Wirtschaftsprüfer neben den allgemeinen Berufspflichten der Unabhängigkeit, Verschwiegenheit, Eigenverantwortlichkeit und Gewissenhaftigkeit (§§ 17 Abs. 1, 43 Abs. 1 Satz 1, 49 WPO, §§ 1–12 BS WP/vBP) auch die besonderen Berufspflichten nach §§ 28–44 BS WP/vBP zu beachten hat.

3 Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) legt in diesem *IDW Prüfungsstandard* die Berufsauffassung dar, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit die Prüfung von IT-Systemen außerhalb der Abschlussprüfung planen, durchführen sowie darüber Bericht erstatten.

4 Dieser *IDW Prüfungsstandard* ist nicht anzuwenden auf Prüfungen von Systemen, für die spezielle *IDW Prüfungsstandards* bestehen (vgl. Tz. A2).

5 Ein Prüfungsauftrag i.S. dieses *IDW Prüfungsstandards* ist insb. durch folgende Merkmale gekennzeichnet:

- Der Wirtschaftsprüfer erteilt ein Prüfungsurteil mit hinreichender Sicherheit, ob durch das Prüfungsobjekt bestimmte Kriterien erfüllt werden; Prüfungsurteile mit begrenzter Sicherheit sind nicht Gegenstand dieses *IDW Prüfungsstandards*.
- Involvierte Parteien sind neben dem Wirtschaftsprüfer und dem Unternehmen, das für das Prüfungsobjekt verantwortlich ist, weitere vorgesehene Nutzer des Prüfungsvermerks oder des Prüfungsberichts, die sich vom Adressaten (i.d.R. die beauftragende Partei) unterscheiden können.

- Das Prüfungsobjekt ist geeignet, d.h. klar bestimmbar und abgrenzbar, und richtet sich auf andere Arten von Sachverhaltsinformationen als vergangenheitsorientierte Finanzinformationen.
- Die bei der Ausgestaltung des Prüfungsobjekts durch das Unternehmen verwendeten Kriterien sind geeignet, um eine konsistente Messung bzw. Beurteilung des Prüfungsobjekts zu ermöglichen. Kriterien können allgemein anerkannt oder für die Zwecke des Prüfungsobjekts entwickelt worden sein.
- Voraussetzung für die Auftragsannahme ist, dass ausreichende geeignete Prüfungsnachweise erlangt werden können.
- Der Wirtschaftsprüfer berichtet über die Prüfung entsprechend der Informationsbedürfnisse der vorgesehenen Nutzer der Berichterstattung. Bei der Berichterstattung des Wirtschaftsprüfers kann es sich um einen Prüfungsvermerk oder um einen Prüfungsbericht handeln.

6 In diesem *IDW Prüfungsstandard* wird zwischen den folgenden Auftragsarten unterschieden:

- Prüfung einer Erklärung zum IT-System
- direkte IT-Prüfung.

7 Neben Definitionen (Abschn. 2.), Gegenstand, Ziel und Umfang der Prüfung (Abschn. 3.) sowie Anforderungen an die schriftliche Erklärung der gesetzlichen Vertreter zum IT-System (Abschn. 4.) enthält dieser *IDW Prüfungsstandard* in den Abschn. 5.–10. zu beachtende Prüfungsanforderungen sowie Anwendungshinweise und sonstige Erläuterungen (Tz. A1 ff. und Anlagen).[2]

8 Dieser *IDW Prüfungsstandard* steht im Einklang mit dem International Standard on Assurance Engagements (ISAE) 3000 (Revised) „Assurance Engagements Other than Audits or Reviews of Historical Financial Information“ (Stand Dezember 2013).[3]

9 Dieser *IDW Prüfungsstandard* ist erstmals anzuwenden bei IT-Prüfungen außerhalb der Abschlussprüfung, die nach dem 30.04.2018 beauftragt werden.[4]

1.2. Definitionen

10 Für Zwecke dieses *IDW Prüfungsstandards* gelten die folgenden Begriffsbestimmungen:

a) *Prüfung einer Erklärung zum IT-System*: Ein Prüfungsauftrag, bei dem der Wirtschaftsprüfer prüft, ob die Erklärung der gesetzlichen Vertreter zum IT-System als Prüfungsobjekt frei von wesentlichen Fehlern ist. Die gesetzlichen Vertreter beurteilen das IT-System anhand von Kriterien und stellen die daraus resultierenden Sachverhaltsinformationen in einer schriftlichen Erklärung dar.

---

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

[3] www.ifac.org, Rubrik „Publications“.

[4] Eine freiwillige frühere Anwendung dieses *IDW Prüfungsstandards* ist zulässig.

b) *Direkte IT-Prüfung*: Ein Prüfungsauftrag, bei dem der Wirtschaftsprüfer das durch die Auftragsvereinbarung abgegrenzte IT-System als Prüfungsobjekt anhand der vereinbarten Kriterien prüft und die daraus resultierenden Sachverhaltsinformationen als Teil seiner Berichterstattung darstellt.

c) *Vorgesehene Nutzer*: Die natürliche(n) Person(en) oder Organisation(en) oder (eine) Gruppe(n) dieser, von der der Wirtschaftsprüfer erwartet, dass sie seine Berichterstattung über die Prüfung verwendet bzw. verwenden. In einigen Fällen kann es weitere als die in der Berichterstattung als Empfänger genannten vorgesehenen Nutzer geben (vgl. Tz. A3).

d) *Kriterien*: Die zur Messung bzw. Beurteilung des zugrunde liegenden Sachverhalts angewandten Maßstäbe. Die „verwendeten Kriterien" sind die Kriterien, die bei einem bestimmten Auftrag zur Anwendung kommen (vgl. Tz. A4–A7).

e) *Prüfungsobjekt*: Das IT-System, das auf Grundlage der Erklärung der gesetzlichen Vertreter zum IT-System oder direkt Gegenstand der Prüfung ist.

f) *Erklärung der gesetzlichen Vertreter zum IT-System*: Aussagen der gesetzlichen Vertreter des Unternehmens zum IT-System sowie zur Angemessenheit und – sofern einschlägig – zur Wirksamkeit der zur Einhaltung der Kriterien getroffenen Grundsätze, Verfahren und Maßnahmen in Bezug auf das IT-System in schriftlicher Form.

g) *IT-System*: Ein System – Grundsätze, Verfahren und Maßnahmen –, das unter Einsatz von IT Daten verarbeitet und folgende Elemente[5] beinhaltet:

   – IT-gestützte Geschäftsprozesse
   – IT-Anwendungen
   – IT-Infrastruktur.

   Das Zusammenwirken dieser Elemente wird durch das IT-Kontrollsystem bestimmt, das von dem IT-Kontrollumfeld und der IT-Organisation abhängt.

h) *Zu prüfendes IT-System*: Diejenigen IT-Infrastrukturen, IT-Anwendungen und/oder IT-gestützten Geschäftsprozesse innerhalb des IT-Systems, die auf der Grundlage der Erklärung der gesetzlichen Vertreter zum IT-System oder direkt einer Prüfung nach diesem IDW Prüfungsstandard unterzogen werden sollen.

j) *Angemessenheit des zu prüfenden IT-Systems*: Die Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems sind geeignet, mit hinreichender Sicherheit (vgl. Tz. A8) die Kriterien einzuhalten und sie sind implementiert, d.h. wie vorgesehen eingerichtet. Dies schließt ein, dass die Grundsätze, Verfahren und Maßnahmen mit hinreichender Sicherheit geeignet sind, die wesentlichen Risiken für die Einhaltung der Kriterien rechtzeitig zu erkennen, zu bewerten, zu steuern und zu überwachen.

k) *Wirksamkeit des zu prüfenden IT-Systems*: Die Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems wurden mit hinreichender Sicherheit (vgl. Tz. A8) in dem zu prüfenden Zeitraum wie von den gesetzlichen Vertretern vorgesehen durchgeführt.

---

[5] Vgl. auch *IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)* (Stand: 24.09.2002), Tz. 7 ff.

l) *Prüfungsrisiko*: Risiko, dass der Wirtschaftsprüfer ein uneingeschränktes Prüfungsurteil abgibt, wenn die Erklärung der gesetzlichen Vertreter zum IT-System einen wesentlichen Fehler aufweist (Prüfung einer Erklärung zum IT-System) bzw. das zu prüfende IT-System einen wesentlichen Mangel enthält (direkte IT-Prüfung).

m) *Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System*: Die Erklärung ist unvollständig oder enthält falsche oder irreführende Aussagen (vgl. Tz. A9).

n) *Mangel des IT-Systems*: Beanstandung hinsichtlich der Grundsätze, Verfahren und Maßnahmen, die auf die Einhaltung der Kriterien in Bezug auf das zu prüfende IT-System gerichtet sind.

o) *Sachverständiger des Wirtschaftsprüfers*: Eine Person oder Organisation mit Fachkenntnissen auf einem anderen Gebiet als betriebswirtschaftliche Prüfungen, deren Arbeit auf diesem Gebiet verwertet wird, um den Wirtschaftsprüfer dabei zu unterstützen, ausreichende geeignete Prüfungsnachweise zu erlangen. Bei einem Sachverständigen des Wirtschaftsprüfers kann es sich entweder um einen internen Sachverständigen des Wirtschaftsprüfers handeln (d.h. einen Partner oder einen fachlichen Mitarbeiter – einschließlich eines befristeten Mitarbeiters – der Praxis des Wirtschaftsprüfers oder eines Mitglieds des Netzwerks) oder um einen externen Sachverständigen des Wirtschaftsprüfers.

11 Für Zwecke dieses *IDW Prüfungsstandards* umfasst der Begriff „Unternehmen“ nicht nur Unternehmen im rechtlichen Sinne, sondern auch andere Einheiten (vgl. Tz. A10).

1.3. Gegenstand, Ziel und Umfang der Prüfung

1.3.1. Prüfung einer Erklärung zum IT-System

12 Gegenstand der Prüfung ist die Erklärung der gesetzlichen Vertreter zum IT-System über die Einhaltung bestimmter Kriterien in Bezug auf das zu prüfende IT-System.

13 Die Verantwortung für die Erklärung der gesetzlichen Vertreter zum IT-System und deren Inhalt liegt bei den gesetzlichen Vertretern des Unternehmens. Diese Verantwortung umfasst auch die Dokumentation der angewandten Grundsätze, Verfahren und Maßnahmen, um eine konsistente Anwendung und personenunabhängige Funktion des zu prüfenden IT-Systems im Zeitablauf zu ermöglichen (vgl. Tz. A11–A12).

14 Eine Prüfung einer Erklärung zum IT-System kann in der Form einer Angemessenheitsprüfung oder einer Wirksamkeitsprüfung durchgeführt werden.

15 Ziel der Angemessenheitsprüfung ist es, dem Wirtschaftsprüfer ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob

- die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet sind,
- die Erklärung der gesetzlichen Vertreter zum IT-System in allen wesentlichen Belangen frei von wesentlichen Fehlern ist,
- die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems in allen wesentlichen Belangen mit hinreichender Sicherheit

- geeignet sind, die Kriterien einzuhalten, und
- zu dem zu prüfenden Zeitpunkt implementiert sind.

16 Ziel der Wirksamkeitsprüfung ist über die Angemessenheitsprüfung hinaus zu beurteilen, ob die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems in dem zu prüfenden Zeitraum wirksam gewesen sind.

1.3.2. Direkte IT-Prüfung

17 Gegenstand einer direkten IT-Prüfung ist das in der Auftragsvereinbarung abgegrenzte, zu prüfende IT-System hinsichtlich der Einhaltung bestimmter Kriterien.

18 Die Verantwortung für die Einrichtung des zu prüfenden IT-Systems sowie dessen Angemessenheit und Wirksamkeit in Bezug auf die Einhaltung der Kriterien liegt bei den gesetzlichen Vertretern des Unternehmens. Diese Verantwortung umfasst auch die Dokumentation der angewandten Grundsätze, Verfahren und Maßnahmen, um eine konsistente Anwendung und personenunabhängige Funktion des zu prüfenden IT-Systems im Zeitablauf zu ermöglichen (vgl. Tz. A11–A12).

19 Bei einer direkten IT-Prüfung ist eine Bestandsaufnahme des Prüfungsobjekts durch den Wirtschaftsprüfer erforderlich.

20 Eine direkte IT-Prüfung kann in der Form einer Angemessenheitsprüfung oder einer Wirksamkeitsprüfung durchgeführt werden.

21 Ziel der Angemessenheitsprüfung ist es, dem Wirtschaftsprüfer ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob

- die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet sind,
- die vom Unternehmen angewandten Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet sind, die Kriterien einzuhalten, und
  - zu dem zu prüfenden Zeitpunkt implementiert sind.

22 Ziel der Wirksamkeitsprüfung ist über die Angemessenheitsprüfung hinaus zu beurteilen, ob die vom Unternehmen angewandten Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems in dem zu prüfenden Zeitraum wirksam gewesen sind.

1.4. Erklärung der gesetzlichen Vertreter zum IT-System

23 Die Erklärung der gesetzlichen Vertreter zum IT-System enthält Aussagen der gesetzlichen Vertreter zu den von ihnen eingerichteten Grundsätzen, Verfahren und Maßnahmen des zu prüfenden IT-Systems, um die Einhaltung der verwendeten Kriterien mit hinreichender Sicherheit zu gewährleisten.

24 Die Erklärung der gesetzlichen Vertreter zum IT-System hat folgende Mindestinhalte zu umfassen:

- Darstellung der bei der Ausgestaltung des zu prüfenden IT-Systems verwendeten Kriterien (vgl. Tz. A4–A7)

- klare, verständliche, vollständige und aktuelle Darstellung der Grundsätze, Verfahren und Maßnahmen zur Steuerung und Überwachung des zu prüfenden IT-Systems zur Einhaltung der Kriterien
- Beschreibung des vom Unternehmen eingerichteten IT-Kontrollumfelds einschließlich der übergreifenden Regelungen der Unternehmensleitung, die für die Ausgestaltung, die Bereitstellung bzw. den Betrieb des zu prüfenden IT-Systems erforderlich sind
- Aussage der gesetzlichen Vertreter des Unternehmens, dass die eingerichteten Grundsätze, Verfahren und Maßnahmen zur Einhaltung der Kriterien angemessen und – soweit einschlägig – im Berichtszeitraum wirksam gewesen sind
- Veränderungen des zu prüfenden IT-Systems bezogen auf den Berichtszeitraum, sofern zutreffend.

25 Angaben, die nicht Gegenstand der Auftragsvereinbarung sind, sind zu unterlassen oder eindeutig von den prüfungsrelevanten Angaben der Erklärung der gesetzlichen Vertreter zum IT-System abzugrenzen.

26 Die Erklärung der gesetzlichen Vertreter zum IT-System hat zumindest im Entwurf zu Beginn der Prüfung vorzuliegen und ist bis zum Abschluss der Prüfung von den gesetzlichen Vertretern fertigzustellen (vgl. Tz. A21).

2. Anforderungen

2.1. Auftragsannahme

27 Vor der Auftragsannahme hat sich der Wirtschaftsprüfer zu vergewissern, dass die Regelungen des Qualitätssicherungssystems der WP-Praxis[6] zur Auftragsannahme und Auftragsfortführung beachtet werden.

28 Ein Auftrag darf nur angenommen werden, wenn der Wirtschaftsprüfer davon ausgehen kann, dass die Berufspflichten einschließlich der Pflicht zur Unabhängigkeit eingehalten werden. Auf der Grundlage der vorläufigen Kenntnisse über den Auftrag hat der Wirtschaftsprüfer insb. 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 zur Verfügung stehen,[7]
- das Verhältnis zwischen Auftraggeber, vorgesehenen Nutzern und Wirtschaftsprüfer hinreichend klar definiert und im Hinblick auf das vorgesehene Prüfungsobjekt, die Berichterstattung und die Durchführung der Prüfung angemessen ist,
- das zugrunde liegende Prüfungsobjekt hinreichend abgrenzbar und beurteilbar ist und der Wirtschaftsprüfer davon ausgehen kann, ausreichende geeignete Prüfungsnachweise als Grundlage für sein Prüfungsurteil zu erhalten,

---

6 Vgl. *IDW Qualitätssicherungsstandard: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* (Stand: 09.06.2017), Tz. 70 ff.

7 Vgl. *IDW QS 1*, Tz. 75.

- die für die Beurteilung des Prüfungsobjekts vereinbarten Kriterien für den Prüfungszweck geeignet und für die vorgesehenen Nutzer verfügbar sind (vgl. Tz. A13) und
- die Art der Berichterstattung festgelegt ist.

29 Ist der Wirtschaftsprüfer mit der Abschlussprüfung für das Unternehmen beauftragt, steht dies einer Beauftragung des Wirtschaftsprüfers nach diesem *IDW Prüfungsstandard* grundsätzlich nicht entgegen.

30 Die Feststellung, ob die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Kriterien (Prüfung einer Erklärung zum IT-System) bzw. die zur Ausgestaltung des zu prüfenden IT-Systems verwendeten Kriterien (direkte IT-Prüfung) als Beurteilungsmaßstab für die Prüfung geeignet sind, hat auch die Feststellung zu umfassen, ob gesetzliche und sonstige regulatorische Anforderungen – soweit einschlägig – angewendet wurden oder Standards und Rahmenwerke, die einen allgemein anerkannten, definierten Formulierungs-, Abstimmungs- und Veröffentlichungsprozess durchlaufen haben. Ist dies der Fall, muss der Wirtschaftsprüfer beurteilen, ob diese Kriterien in Bezug auf den Prüfungszweck vollständig angewandt wurden (vgl. Tz. A14).

31 Andere Standards und Rahmenwerke oder vom Unternehmen selbst entwickelte Kriterien sind stets vom Wirtschaftsprüfer auf ihre Eignung zu beurteilen.

32 Geeignete Kriterien müssen sämtliche folgende Anforderungen erfüllen (vgl. Tz. A15–A17):

- Relevanz
- Vollständigkeit
- Verlässlichkeit
- Neutralität und
- Verständlichkeit.

33 Der Wirtschaftsprüfer hat festzustellen, ob durch die verwendeten Kriterien die Einhaltung der anzuwendenden regulatorischen, aufsichtsrechtlichen und aufgabenbezogenen Anforderungen an die Ausgestaltung von IT-Systemen ermöglicht wird (vgl. Tz. A18).

34 Bei IT-Prüfungen von rechnungslegungsrelevanten Verfahren und Prozessen hat der Wirtschaftsprüfer darüber hinaus festzustellen, ob durch die verwendeten Kriterien die Einhaltung der Grundsätze ordnungsmäßiger Buchführung bzw. der Anforderungen an die Ordnungsmäßigkeit und Sicherheit rechnungslegungsrelevanter Systeme[8] ermöglicht wird.

35 Im Falle einer Prüfung einer Erklärung zum IT-System darf der Wirtschaftsprüfer den Auftrag nur annehmen, wenn eine Erklärung der gesetzlichen Vertreter zum IT-System vorliegt bzw. die gesetzlichen Vertreter ihre Bereitschaft erklären, eine solche Erklärung zu erstellen.

36 Der Wirtschaftsprüfer hat vor der Auftragsannahme festzustellen, dass eine missbräuchliche Verwendung der Berichterstattung des Wirtschaftsprüfers vermieden wird (vgl. Tz. A19).

---

[8] Vgl. *IDW RS FAIT 1*, *IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)* (Stand: 11.09.2015) für Dokumentenmanagementsysteme, *IDW Stellungnahme zur Rechnungslegung: Anforderungen an die Ordnungsmäßigkeit und Sicherheit IT-gestützter Konsolidierungsprozesse (IDW RS FAIT 4)* (Stand: 08.08.2012) für die Konzernrechnungslegung, *IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen einschließlich Cloud Computing (IDW RS FAIT 5)* (Stand: 04.11.2015) für Auslagerungen einschließlich der Nutzung von Cloud Computing.

37 Der Wirtschaftsprüfer hat mit dem Auftraggeber die Auftragsbedingungen – insb. die jeweiligen Verantwortlichkeiten der gesetzlichen Vertreter und des Wirtschaftsprüfers – schriftlich zu vereinbaren (vgl. Tz. A20–A22).

38 Wird dem Wirtschaftsprüfer vor der Auftragsannahme ein Prüfungshemmnis bekannt, das nach Einschätzung des Wirtschaftsprüfers zu einer Nicht-Erteilung des Prüfungsurteils führen würde, darf er den Auftrag nicht annehmen.

39 Werden dem Wirtschaftsprüfer nach der Auftragsannahme Informationen bekannt, die – wenn sie ihm vorher bekannt geworden wären – zur Ablehnung des Auftrags geführt hätten, so hat er die ggf. erforderlichen Maßnahmen zu ergreifen (vgl. Tz. A23)[9].

40 Der Wirtschaftsprüfer darf nach der Auftragsannahme einer wesentlichen Änderung der Bedingungen des Prüfungsauftrags nicht zustimmen, wenn es dafür keine vertretbare Begründung gibt. Erfolgt eine Änderung der Bedingungen, darf der Wirtschaftsprüfer Prüfungsnachweise nicht außer Acht lassen, die vor der Änderung der Auftragsbedingungen erlangt wurden (vgl. Tz. A24).

2.2. Prüfungsplanung

41 Der Wirtschaftsprüfer hat die Prüfung in sachlicher, personeller und zeitlicher Hinsicht so zu planen, dass sie in sachgerechter Weise durchgeführt werden kann. Hierzu sind die Art, die zeitliche Einteilung und der Umfang der geplanten Prüfungshandlungen festzulegen, die erforderlich sind, um die Prüfungsziele zu erreichen.

42 Bei der Auswahl der Mitglieder des Prüfungsteams hat der Wirtschaftsprüfer darauf zu achten, dass diese insgesamt über ausreichende praktische Erfahrungen mit IT-Prüfungen sowie die notwendigen Branchen- und ggf. Rechtskenntnisse verfügen (vgl. Tz. A25), um den Auftrag ordnungsgemäß durchzuführen und ein sachgerechtes Prüfungsurteil zu erteilen.[10] Das Prüfungsteam muss ausreichende Kenntnisse der relevanten Grundsätze, Verfahren und Maßnahmen sowie der Elemente des IT-Systems besitzen. Der Wirtschaftsprüfer hat sich zu vergewissern, dass das Prüfungsteam bei der Hinzuziehung von Sachverständigen sowie von anderen Wirtschaftsprüfern, die nicht Mitglied des Prüfungsteams sind, im erforderlichen Umfang in die Tätigkeit des Sachverständigen bzw. anderen Wirtschaftsprüfers eingebunden werden kann, um die Verantwortung für sein Prüfungsurteil insgesamt übernehmen zu können.

43 Der Wirtschaftsprüfer muss die Prüfung mit einer kritischen Grundhaltung[11] planen und mit dem Bewusstsein durchführen, dass Umstände bestehen können, die dazu führen, dass das zu prüfende IT-System in Bezug auf die verwendeten Kriterien zu dem zu prüfenden Zeitpunkt bzw. in dem zu prüfenden Zeitraum nicht angemessen bzw. wirksam war.

44 Der Wirtschaftsprüfer hat für Zwecke der Prüfungsplanung und -durchführung, einschließlich der Festlegung von Art, Umfang und zeitlicher Einteilung der Prüfungshandlungen sowie bei der Auswertung der Prüfungsergebnisse, d.h. bei der Beurteilung, ob die Erklärung der gesetzlichen Vertreter zum IT-System wesentliche Fehler enthält (Prüfung einer Erklärung zum

---

[9] Vgl. *IDW QS 1*, Tz. 79.

[10] Vgl. § 38 Abs. 3 BS WP/vBP.

[11] Vgl. § 37 BS WP/vBP.

IT-System) bzw. das IT-System wesentliche Mängel aufweist (direkte IT-Prüfung), die Wesentlichkeit zu berücksichtigen.

45 Der Wirtschaftsprüfer hat sich ein ausreichendes Verständnis vom Unternehmen, dem für die Prüfung relevanten rechtlichen und wirtschaftlichen Umfeld sowie von dem zu prüfenden IT-System zu verschaffen, um die Risiken für wesentliche Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) bzw. die Risiken für wesentliche Mängel des zu prüfenden IT-Systems (direkte IT-Prüfung) festzustellen und zu beurteilen (vgl. Tz. A26). Hierzu hat sich der Wirtschaftsprüfer bei einer Prüfung einer Erklärung zum IT-System ein angemessenes Verständnis darüber zu verschaffen, dass der Prozess zur Erstellung der Erklärung der gesetzlichen Vertreter zum IT-System in ein angemessenes internes Kontrollsystem eingebettet ist. Dies schließt die Beurteilung mit ein, ob zur Erlangung der in der Erklärung der gesetzlichen Vertreter zum IT-System enthaltenen Informationen neben der Befragung der verantwortlichen Mitarbeiter auch geeignete Kontrollhandlungen durchgeführt wurden. Das erlangte Verständnis muss zudem eine angemessene Grundlage bilden für die Planung und Durchführung von Prüfungshandlungen als Reaktion auf die festgestellten und beurteilten Risiken und für die Erlangung hinreichender Sicherheit bei der Bildung des Prüfungsurteils.

46 Der Wirtschaftsprüfer hat Befragungen der gesetzlichen Vertreter sowie weiterer geeigneter Personen durchzuführen, um in Erfahrung zu bringen, ob

- diese Personen Kenntnisse über vorliegende, vermutete oder behauptete Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System oder über Mängel des IT-Systems haben,
- das Unternehmen über eine Interne Revision verfügt; falls eine solche eingerichtet ist, sind weitere Befragungen durchzuführen, um ein Verständnis von den Aktivitäten und Feststellungen der Internen Revision in Bezug auf das zu prüfende IT-System zu gewinnen, und
- das Unternehmen Sachverständige bei der Konzeption oder der Einrichtung des zu prüfenden IT-Systems oder bei der Erstellung der Erklärung der gesetzlichen Vertreter zum IT-System eingesetzt hat.

47 Auf der Grundlage des gewonnenen Verständnisses über das Unternehmen, das rechtliche und wirtschaftliche Umfeld und das zu prüfende IT-System hat der Wirtschaftsprüfer die Risiken für wesentliche Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) bzw. die Risiken für wesentliche Mängel des zu prüfenden IT-Systems (direkte IT-Prüfung) zu identifizieren und zu beurteilen (vgl. Tz. A27). Sofern der Wirtschaftsprüfer im Rahmen der Prüfungsdurchführung Nachweise erlangt, die im Widerspruch zu den Prüfungsnachweisen stehen, die Basis für seine ursprüngliche Risikobeurteilung waren, muss er die Risikobeurteilung anpassen und die weiteren geplanten Prüfungshandlungen entsprechend modifizieren.

48 Unter Ausübung seines pflichtgemäßen Ermessens hat der Wirtschaftsprüfer die Prüfungshandlungen so zu planen und durchzuführen, dass das Prüfungsrisiko (vgl. Tz. 10 l)) so weit reduziert wird, dass er mit hinreichender Sicherheit beurteilen kann, ob die Erklärung der gesetzlichen Vertreter zum IT-System wesentliche Fehler aufweist (Prüfung einer Erklärung zum IT-System) bzw. ob das zu prüfende IT-System wesentliche Mängel enthält (direkte IT-Prüfung).

49 Bei der Bestimmung von Art und Umfang der Prüfungshandlungen hat der Wirtschaftsprüfer die Art des Prüfungsauftrags (Angemessenheits- oder Wirksamkeitsprüfung) und das beurteilte Risiko wesentlicher Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) bzw. das beurteilte Risiko wesentlicher Mängel des zu prüfenden IT-Systems (direkte IT-Prüfung) zu berücksichtigen. Diese Risiken werden auch durch die verwendeten Kriterien, die Erklärung der gesetzlichen Vertreter zum IT-System und die Komplexität des zu prüfenden IT-Systems bestimmt.

50 Der Wirtschaftsprüfer hat für Zwecke der Planung und Durchführung der Prüfungshandlungen sowie der Auswertung der Prüfungsergebnisse zu bestimmen, in welchen Fällen ein Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System bzw. in welchen Fällen ein Mangel des zu prüfenden IT-Systems als wesentlich einzustufen ist (vgl. Tz. A28–A29). Bei der Bestimmung der Wesentlichkeit hat der Wirtschaftsprüfer sein pflichtgemäßes Ermessen auszuüben.

51 Bei der Prüfungsplanung sind insb. die folgenden Prüfungsgebiete zu berücksichtigen:

- Die Eignung der zur Ausgestaltung des zu prüfenden IT-Systems verwendeten Kriterien
- die Vollständigkeit und Richtigkeit der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) und das Vorliegen einer angemessenen Dokumentation des zu prüfenden IT-Systems (Prüfung einer Erklärung zum IT-System und direkte IT-Prüfung)
- die Angemessenheit der eingerichteten Grundsätze, Verfahren und Maßnahmen zur Einhaltung der Kriterien und
- die Wirksamkeit der eingerichteten Grundsätze, Verfahren und Maßnahmen (nur bei einer Wirksamkeitsprüfung).

52 Der Wirtschaftsprüfer muss die geplanten Prüfungshandlungen in einem Prüfungsprogramm zusammenfassen, das die Prüfungsanweisungen zur sachlichen und zeitlichen Auftragsabwicklung für die Mitglieder des Prüfungsteams enthält.[12]

53 Zudem hat der Wirtschaftsprüfer die übrigen auftragsbezogenen Qualitätssicherungsmaßnahmen sowie die Überwachung der Auftragsabwicklung und die Durchsicht der Prüfungsergebnisse zu planen.[13]

2.3. Prüfungsdurchführung

2.3.1. Prüfung der Ausgestaltung und Aktualität der Erklärung der gesetzlichen Vertreter zum IT-System

54 Der Wirtschaftsprüfer hat die Ausgestaltung und Aktualität der der Prüfung zugrunde liegenden Erklärung der gesetzlichen Vertreter zum IT-System zu beurteilen. Hinsichtlich der Ausgestaltung dieser Erklärung hat der Wirtschaftsprüfer zu beurteilen, ob das Prüfungsobjekt und die zur Einhaltung der Kriterien angewandten Grundsätze, Verfahren und Maßnahmen vollständig und richtig sowie in einer für die Adressaten verständlichen Art und Weise dargestellt sind.

---

[12] Vgl. § 38 Abs. 1 BS WP/vBP.

[13] Vgl. *IDW QS 1*, Tz. 107 ff.

Hierzu zählen auch die bei der Ausgestaltung des zu prüfenden IT-Systems verwendeten Kriterien. Die Prüfung der Vollständigkeit hat auch zu umfassen, ob die Erklärung der gesetzlichen Vertreter zum IT-System die erforderlichen Mindestinhalte aufweist (vgl. Tz. 24).

55 Hinsichtlich der Aktualität der Erklärung der gesetzlichen Vertreter zum IT-System ist festzustellen, ob diese dem vereinbarten Stand des zu prüfenden IT-Systems entspricht oder ob zwischenzeitlich Änderungen vorgenommen wurden, die aus Sicht des Wirtschaftsprüfers als wesentlich zu erachten sind. Soweit Letzteres der Fall ist, hat der Wirtschaftsprüfer die gesetzlichen Vertreter aufzufordern, die Erklärung entsprechend anzupassen.

56 Im Falle einer Wirksamkeitsprüfung hat der Wirtschaftsprüfer zu beurteilen, ob die Erklärung der gesetzlichen Vertreter zum IT-System auf wesentliche Veränderungen des zu prüfenden IT-Systems bezogen auf den Berichtszeitraum gesondert eingeht.

2.3.2. Prüfung der Angemessenheit des IT-Systems

57 Auf der Grundlage seines Verständnisses von dem zu prüfenden IT-System (Prüfung einer Erklärung zum IT-System und direkte IT-Prüfung) und der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) sowie den Ergebnissen seiner Risikobeurteilungen hat der Wirtschaftsprüfer im Rahmen der Prüfung der Angemessenheit zu beurteilen, ob die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Grundsätze, Verfahren und Maßnahmen (Prüfung einer Erklärung zum IT-System) bzw. ob die vom Unternehmen angewandten Grundsätze, Verfahren und Maßnahmen (direkte IT-Prüfung) geeignet sind, mit hinreichender Sicherheit die Einhaltung der Kriterien zu gewährleisten (vgl. Tz. A30–A32).

58 Der Wirtschaftsprüfer hat durch die Kombination von Befragungen mit anderen Prüfungshandlungen, einschließlich Beobachtung sowie Einsichtnahme in Aufzeichnungen und Dokumente, festzustellen, ob die Grundsätze, Verfahren und Maßnahmen, wie von den gesetzlichen Vertretern vorgesehen, zu dem zu prüfenden Zeitpunkt eingerichtet (implementiert) sind (vgl. Tz. A33–A35).

59 Stellt der Wirtschaftsprüfer fest, dass keine angemessenen Grundsätze, Verfahren und Maßnahmen zur Einhaltung der Kriterien eingerichtet sind, hat er darauf hinzuwirken, dass diese durch das Unternehmen eingerichtet werden (direkte IT-Prüfung und Prüfung einer Erklärung zum IT-System) und dementsprechend die Erklärung der gesetzlichen Vertreter zum IT-System geändert wird (Prüfung einer Erklärung zum IT-System), bevor die Prüfung fortgesetzt werden kann.

2.3.3. Prüfung der Wirksamkeit des IT-Systems

60 Die Prüfung der Wirksamkeit setzt die Prüfung der Angemessenheit voraus und zielt darauf ab, ob die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Grundsätze, Verfahren und Maßnahmen (Prüfung einer Erklärung zum IT-System) bzw. die vom Unternehmen angewandten Grundsätze, Verfahren und Maßnahmen (direkte IT-Prüfung) innerhalb des gesamten zu prüfenden Zeitraums wie vorgesehen durchgeführt wurden. Dabei hat der Wirtschaftsprüfer die Funktionsprüfungen so zu planen und durchzuführen, dass diese

ausreichende geeignete Prüfungsnachweise für die Wirksamkeit des als angemessen beurteilten, zu prüfenden IT-Systems erbringen (vgl. Tz. A36–A40). Befragungen allein reichen für die Erzielung der erforderlichen Urteilssicherheit über die Wirksamkeit der Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems nicht aus. Der Wirtschaftsprüfer hat diese für eine Verwertbarkeit als Prüfungsnachweis mit einer oder mehreren zusätzlichen Arten von Prüfungshandlungen zu kombinieren.

61 Ist eine Änderung in der Art oder Durchführung der Grundsätze, Verfahren und Maßnahmen in dem zu prüfenden Zeitraum erfolgt, hat der Wirtschaftsprüfer die Grundsätze, Verfahren und Maßnahmen sowohl vor als auch nach der Änderung auf ihre Wirksamkeit hin zu beurteilen.

62 Bei der Planung und Durchführung der Prüfungshandlungen hat der Wirtschaftsprüfer die Bedeutung und Verlässlichkeit der Informationen, die als Prüfungsnachweise dienen sollen, zu berücksichtigen. Für den Fall, dass

- die aus unterschiedlichen Quellen stammenden Prüfungsnachweise nicht im Einklang stehen oder
- der Wirtschaftsprüfer Zweifel an der Verlässlichkeit der Information hat, die als Prüfungsnachweis dienen soll,

muss der Wirtschaftsprüfer festlegen, wie die Prüfungshandlungen angepasst oder ergänzt werden müssen, um den Sachverhalt zu klären, und die etwaigen Auswirkungen des Sachverhalts auf andere Aspekte der Prüfung abwägen.

2.3.4. Weitere Prüfungshandlungen

2.3.4.1. Verwertung der Arbeit von Sachverständigen des Wirtschaftsprüfers

63 Wenn die Beurteilung bedeutsamer Sachverhalte besondere Sachkenntnisse erfordert, um ausreichende geeignete Prüfungsnachweise zu erlangen, hat der Wirtschaftsprüfer zu entscheiden, ob Sachverständige hinzuzuziehen sind (vgl. Tz. A41).

64 Eingesetzte interne Sachverständige des Wirtschaftsprüfers müssen dem Qualitätssicherungssystem der WP-Praxis unterliegen. Der Wirtschaftsprüfer hat die internen Sachverständigen angemessen anzuleiten und zu überwachen.

65 Wenn die Arbeiten eines externen Sachverständigen des Wirtschaftsprüfers verwertet werden sollen, hat der Wirtschaftsprüfer

- zu beurteilen, ob der Sachverständige über die Kompetenz, die Fähigkeiten und die Objektivität verfügt, die für die Zwecke der Prüfung des zu prüfenden IT-Systems notwendig sind. Die Beurteilung der Objektivität des Sachverständigen hat u.a. eine Befragung zu möglichen Interessen und Beziehungen zu umfassen, die eine Gefährdung der Objektivität des Sachverständigen hervorrufen können (vgl. Tz. A42),
- ein ausreichendes Verständnis von dem Fachgebiet des Sachverständigen zu erlangen,
- mit dem Sachverständigen Art, Umfang und Ziele der Arbeit für die Zwecke der Prüfung des zu prüfenden IT-Systems zu vereinbaren und
- die Angemessenheit der Arbeit des Sachverständigen für die Zwecke der Prüfung des zu prüfenden IT-Systems zu beurteilen (vgl. Tz. A43–A46).

2.3.4.2. Verwendung der Arbeit von Sachverständigen der gesetzlichen Vertreter

66 Sollen Informationen, die unter Verwendung der Tätigkeit eines Sachverständigen der gesetzlichen Vertreter erstellt wurden, als Prüfungsnachweise verwendet werden, muss der Wirtschaftsprüfer unter Berücksichtigung der Bedeutung der Tätigkeit des Sachverständigen für die Zwecke des Wirtschaftsprüfers

- die Kompetenz, Fähigkeiten und Objektivität des Sachverständigen beurteilen,
- ein ausreichendes Verständnis von der Tätigkeit des Sachverständigen gewinnen und
- die Angemessenheit der Tätigkeit des Sachverständigen als Prüfungsnachweis beurteilen (vgl. Tz. A47).

2.3.4.3. Verwendung oder Verwertung der Arbeit anderer Wirtschaftsprüfer

67 Plant der Wirtschaftsprüfer die Verwendung des Vermerks, Berichts oder der Bescheinigung eines anderen Wirtschaftsprüfers, gelten die Anforderungen in Tz. 66 sinngemäß. In Fällen, in denen der Wirtschaftsprüfer die Verwertung der Arbeit eines anderen Wirtschaftsprüfers plant, hat er die Anforderungen in Tz. 64 und 65 sinngemäß zu berücksichtigen (vgl. Tz. A47).

2.3.4.4. Verwendung der Arbeit der Internen Revision

68 Plant der Wirtschaftsprüfer, Arbeiten der Internen Revision zu verwenden, hat er zu beurteilen,

- inwieweit die organisatorische Stellung und die Arbeitsweise die notwendige Objektivität der internen Revisoren gewährleisten,
- die notwendige fachliche Kompetenz der Internen Revision,
- ob die Arbeiten der Internen Revision mit einer systematischen Vorgehensweise und mit der notwendigen berufsüblichen Sorgfalt (einschließlich qualitätssichernder Maßnahmen) durchgeführt werden und
- ob die Arbeiten der Internen Revision für die Zwecke der Prüfung des zu prüfenden IT-Systems angemessen sind (vgl. Tz. A47).

69 Für die Frage, inwieweit sich die Arbeiten der Internen Revision auf die Art, den Umfang und die zeitliche Einteilung der eigenen Prüfungshandlungen auswirken, hat der Wirtschaftsprüfer Folgendes zu berücksichtigen:

- Art und Umfang der Revisionstätigkeiten (sowohl durchgeführte als auch noch durchzuführende)
- Relevanz der Revisionstätigkeit für die eigene Prüfung
- Nachvollziehbarkeit der Revisionsergebnisse
- Art, Umfang und Ergebnisse einer ggf. durchgeführten Prüfung nach *IDW PS 983*[14].

[14] *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Internen Revisionssystemen (IDW PS 983)* (Stand: 03.03.2017).

2.3.4.5. Ereignisse nach dem zu prüfenden Zeitpunkt bzw. dem zu prüfenden Zeitraum

70 Der Wirtschaftsprüfer hat die Auswirkungen von Ereignissen nach dem Zeitpunkt bzw. Zeitraum, auf den sich die Erklärung der gesetzlichen Vertreter zum IT-System bezieht (Prüfung einer Erklärung zum IT-System) bzw. auf den sich die Prüfung des zu prüfenden IT-Systems bezieht (direkte IT-Prüfung), bis zum Datum der Berichterstattung zu würdigen (vgl. Tz. A48).

71 Der Wirtschaftsprüfer ist nicht verpflichtet, Prüfungshandlungen nach dem Datum der Berichterstattung durchzuführen oder Prüfungshandlungen durchzuführen, um Ereignisse festzustellen, die nicht den zu prüfenden Zeitpunkt bzw. zu prüfenden Zeitraum betreffen.

72 Werden dem Wirtschaftsprüfer nach dem Datum der Auslieferung der Berichterstattung Sachverhalte bekannt, die dazu führen, dass das Prüfungsurteil in der erteilten Form nicht hätte abgegeben werden dürfen, hat er angemessene Maßnahmen zu ergreifen, damit die vorgesehenen Nutzer hiervon Kenntnis erlangen.

2.3.4.6. Sonstige Angaben in der Erklärung der gesetzlichen Vertreter zum IT-System

73 Enthält die Erklärung der gesetzlichen Vertreter zum IT-System sonstige Angaben, die nicht Gegenstand der Auftragsvereinbarung sind, hat der Wirtschaftsprüfer darauf hinzuwirken, dass die gesetzlichen Vertreter diese Angaben unterlassen oder diese Angaben eindeutig von den prüfungsrelevanten Angaben dieser Erklärung abgrenzen (vgl. Tz. A49).

74 Es liegt im Ermessen des Wirtschaftsprüfers, ob die sonstigen Angaben in die Prüfung einbezogen werden. Der Wirtschaftsprüfer hat die nicht geprüften sonstigen Angaben in der Berichterstattung zu benennen und darauf hinzuweisen, dass sie nicht geprüft wurden und sich daher das Prüfungsurteil nicht darauf erstreckt.

75 Nicht in die Prüfung einbezogene sonstige Angaben hat der Wirtschaftsprüfer jedoch kritisch zu lesen, um ggf. bestehende wesentliche Unstimmigkeiten gegenüber den geprüften Aussagen in der Erklärung der gesetzlichen Vertreter zum IT-System festzustellen.

76 Falls der Wirtschaftsprüfer beim kritischen Lesen der sonstigen Angaben

- eine wesentliche Unstimmigkeit zwischen den sonstigen Angaben und den geprüften Aussagen in der Erklärung der gesetzlichen Vertreter zum IT-System oder den Aussagen in der Berichterstattung feststellt oder
- wesentliche offensichtliche Fehler in den sonstigen Angaben feststellt, die nicht mit den geprüften Aussagen in der Erklärung der gesetzlichen Vertreter zum IT-System und den Aussagen in der Berichterstattung zusammenhängen,

hat er den Sachverhalt mit den gesetzlichen Vertretern zu erörtern und, sofern angebracht, weitere angemessene Maßnahmen zu ergreifen (vgl. Tz. A50).

77 Hat der Wirtschaftsprüfer festgestellt, dass die Klarheit und Übersichtlichkeit der Erklärung der gesetzlichen Vertreter zum IT-System durch die sonstigen Angaben, die nicht Gegenstand der Prüfung sind, wesentlich beeinträchtigt ist, hat er das Prüfungsurteil einzuschränken oder zu versagen.

2.3.4.7. Schriftliche Erklärungen

78 Der Wirtschaftsprüfer hat vor Abschluss der Prüfung von den gesetzlichen Vertretern eine Vollständigkeitserklärung einzuholen, in der in Übereinstimmung mit den vereinbarten Auftragsbedingungen bestätigt wird, dass dem Wirtschaftsprüfer alle relevanten Erklärungen und Nachweise zur Angemessenheit und – soweit einschlägig – Wirksamkeit des IT-Systems erteilt worden sind. Die Vollständigkeitserklärung hat auch die Zusicherung zu enthalten, dass die gesetzlichen Vertreter dem Wirtschaftsprüfer alle relevanten Zugangsberechtigungen zu den für die Prüfung erforderlichen Informationen eingeräumt und ihm vollständig die folgenden ihnen bekannten Aspekte mitgeteilt haben:

- Vollständigkeit und Richtigkeit der Erklärung der gesetzlichen Vertreter zum IT-System auf der Grundlage der verwendeten Kriterien bei einer Prüfung einer Erklärung zum IT-System
- Mängel in Bezug auf die Angemessenheit des zu prüfenden IT-Systems
- Fälle, in denen die Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems nicht wie in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellt bzw. anders als vorgesehen, durchgeführt wurden
- geplante bedeutsame Änderungen des zu prüfenden IT-Systems und
- Ereignisse, die nach dem zu prüfenden Zeitpunkt bzw. zu prüfenden Zeitraum, aber vor dem Datum der Berichterstattung eingetreten sind und eine erhebliche Auswirkung auf die Einhaltung der Kriterien haben können (vgl. Tz. A51).

79 Wenn der Wirtschaftsprüfer feststellt, dass es notwendig ist, über die im Rahmen der Vollständigkeitserklärung angeforderten Erklärungen hinaus weitere schriftliche Erklärungen zu erlangen, um andere für das IT-System relevante Prüfungsnachweise zu stützen, hat er diese weiteren schriftlichen Erklärungen einzuholen (vgl. Tz. A52).

80 Sofern sich einzelne Aspekte der Vollständigkeitserklärung oder ggf. weitere schriftliche Erklärungen auf Sachverhalte beziehen, die wesentlich für die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Aussagen (Prüfung einer Erklärung zum IT-System) bzw. für die Einhaltung der Kriterien durch die Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems (direkte IT-Prüfung) sind, muss der Wirtschaftsprüfer

- beurteilen, ob die von den gesetzlichen Vertretern abgegebenen Erklärungen nachvollziehbar und mit anderen erlangten Prüfungsnachweisen, einschließlich anderer mündlicher oder schriftlicher Erklärungen, konsistent sind und
- abwägen, ob zu erwarten ist, dass die Personen, welche die schriftlichen Erklärungen abgeben, in Bezug auf die betreffenden Sachverhalte ausreichend informiert sind.

81 Die Vollständigkeitserklärung muss zeitnah zum Datum des Prüfungsvermerks bzw. Prüfungsberichts, darf aber nicht nach diesem datiert werden.

82 Unterbleibt die Vollständigkeitserklärung durch die gesetzlichen Vertreter oder bestehen begründete Zweifel in Bezug auf die Kompetenz oder die Integrität der Personen, welche die Vollständigkeitserklärung abgeben, bzw. bestehen andere begründete Zweifel, dass die erteilte Erklärung verlässlich ist, ist darin ein Prüfungshemmnis zu sehen. In diesem Fall hat der Wirtschaftsprüfer in der Berichterstattung darauf hinzuweisen, dass ein Prüfungsurteil nicht erteilt wird.

83 Beziehen sich die Zweifel auf andere vom Wirtschaftsprüfer angeforderte schriftliche Erklärungen, hat der Wirtschaftsprüfer den Sachverhalt mit den Verantwortlichen zu erörtern, die Auswirkungen auf die Verlässlichkeit der bereits eingeholten Prüfungsnachweise zu würdigen und, sofern angebracht, weitere Maßnahmen zu ergreifen, einschließlich der Feststellung möglicher Auswirkungen auf das Prüfungsurteil.

2.4. Auswertung der Prüfungsfeststellungen und Bildung des Prüfungsurteils

84 Der Wirtschaftsprüfer muss würdigen, ob er ausreichende geeignete Prüfungsnachweise als Grundlage für sein Prüfungsurteil erlangt hat. Ist dies nicht der Fall, hat er weitere Prüfungsnachweise einzuholen. Anderenfalls hat er die Ergebnisse der Prüfung auszuwerten und auf dieser Grundlage ein Prüfungsurteil zu treffen. Bei der Bildung eines Prüfungsurteils muss der Wirtschaftsprüfer alle relevanten Prüfungsnachweise berücksichtigen, unabhängig davon, ob sie dem Anschein nach die Aussagen in der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) bzw. die Angemessenheit und Wirksamkeit des IT-Systems (direkte IT-Prüfung) stützen oder ihnen widersprechen.

85 Bei der Bildung des Prüfungsurteils hat der Wirtschaftsprüfer zu würdigen, ob nicht korrigierte Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System bzw. festgestellte Mängel in dem in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten IT-System (Prüfung einer Erklärung zum IT-System) oder festgestellte Mängel des zu prüfenden IT-Systems (direkte IT-Prüfung) einzeln oder in der Summe wesentlich sind (vgl. Tz. A53–A54).

86 Bestehen keine wesentlichen Beanstandungen in Bezug auf die Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) bzw. die vom Unternehmen angewandten Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems, hat der Wirtschaftsprüfer ein uneingeschränktes Prüfungsurteil abzugeben. Liegen wesentliche Beanstandungen vor, ist das Prüfungsurteil einzuschränken oder zu versagen.

87 Das Prüfungsurteil ist wegen eines Fehlers in der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) oder eines Mangels in den vom Unternehmen angewandten Grundsätzen, Verfahren und Maßnahmen des zu prüfenden IT-Systems einzuschränken, wenn der Fehler oder Mangel zwar wesentlich, aber nicht umfassend ist (vgl. Tz. A55). Sind die Beanstandungen nicht auf bestimmte Teile der in der Erklärung der gesetzlichen Vertreter zum IT-System enthaltenen Aussagen (Prüfung einer Erklärung zum IT-System) oder der vom Unternehmen angewandten Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems einzugrenzen (umfassender Mangel), ist das Prüfungsurteil zu versagen (vgl. Tz. A56).

88 Ist der Wirtschaftsprüfer nicht in der Lage, ausreichende geeignete Prüfungsnachweise zu erlangen, liegt ein Prüfungshemmnis vor. In diesem Fall ist das Prüfungsurteil einzuschränken, wenn die Auswirkungen des Prüfungshemmnisses zwar die Beurteilung eines wesentlichen Teils der Aussagen in der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) bzw. der vom Unternehmen angewandten Grundsätze, Verfahren und Maßnahmen ausschließen, eine Beurteilung insgesamt aber noch möglich ist. Kann aufgrund von Prüfungshemmnissen auch nach Ausschöpfung der prüferischen Möglichkeiten ein Urteil nicht abgegeben werden, ist in der Berichterstattung zu erklären, dass ein Prüfungsurteil nicht erteilt wird.

89 Wird das Prüfungsurteil aufgrund von Prüfungshemmnissen eingeschränkt oder nicht erteilt, sind festgestellte wesentliche Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) bzw. festgestellte Mängel des zu prüfenden IT-Systems (direkte IT-Prüfung) in der Berichterstattung des Wirtschaftsprüfers zu beschreiben.

90 Falls sich im Verlauf der Prüfung herausstellt, dass sich bei einer Prüfung einer Erklärung zum IT-System diese Erklärung der gesetzlichen Vertreter zum IT-System nicht für eine Prüfung eignet oder sie unangemessene Verallgemeinerungen oder unausgewogene und verzerrende Darstellungen enthält, die eine Irreführung der Berichtsadressaten zur Folge haben können, hat der Wirtschaftsprüfer zunächst auf eine entsprechende Änderung der Erklärung der gesetzlichen Vertreter zum IT-System hinzuwirken. Unterbleibt diese, hat er abzuwägen, ob das Prüfungsurteil einzuschränken oder zu versagen ist.

91 Der Wirtschaftsprüfer hat das Prüfungsurteil zu versagen, wenn sich im Verlauf der Prüfung herausstellt, dass

- das zu prüfende IT-System irreführend abgegrenzt wurde oder
- die vereinbarten Kriterien nicht geeignet sind oder nicht angewendet wurden.

92 Einschränkungen, Versagungen oder Nichterteilungen des Prüfungsurteils sind klar durch die Verwendung des Begriffs „Einschränkung“ bzw. „Versagung“ oder „Nichterteilung“ zu kennzeichnen. Die Gründe für die Einschränkung bzw. Versagung oder die Nichterteilung eines Prüfungsurteils sind vollständig und eindeutig in der Berichterstattung darzustellen.

93 Bei einer Einschränkung des Prüfungsurteils hat der Wirtschaftsprüfer die Formulierung „…mit Ausnahme…“ zu verwenden und die Auswirkungen der Gründe darzustellen, die zu einer Einschränkung geführt haben.

94 Ist es nach Auffassung des Wirtschaftsprüfers für das Verständnis der Erklärung der gesetzlichen Vertreter zum IT-System durch die vorgesehenen Nutzer (Prüfung einer Erklärung zum IT-System) oder für das Verständnis der Beurteilung der Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems (direkte IT-Prüfung) notwendig, die vorgesehenen Nutzer der Berichterstattung auf einen besonderen Sachverhalt aufmerksam zu machen, hat er einen Absatz zur Hervorhebung des Sachverhalts in die Berichterstattung aufzunehmen. Die Hervorhebung darf sich nur auf in der Erklärung der gesetzlichen Vertreter zum IT-System angegebene Informationen (Prüfung einer Erklärung zum IT-System) bzw. Informationen i.Z.m. der Beurteilung der Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems durch den Wirtschaftsprüfer (direkte IT-Prüfung) beziehen.

95 Darüber hinaus hat der Wirtschaftsprüfer auf sonstige Sachverhalte außerhalb der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) bzw. der angewendeten Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems hinzuweisen, wenn dies nach Auffassung des Wirtschaftsprüfers für die vorgesehenen Nutzer zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis der Berichterstattung erforderlich ist.

96 Ein hinweisender Absatz nach Tz. 95 ist – ebenso wie eine Hervorhebung nach Tz. 94 – klar zu kennzeichnen und es ist klarzustellen, dass das Prüfungsurteil im Hinblick auf den entsprechenden Sachverhalt nicht eingeschränkt oder versagt wird.

2.5. Dokumentation

97 Der Wirtschaftsprüfer hat die zur Stützung seines Prüfungsurteils dienenden Prüfungsnachweise in angemessener Zeit in den Arbeitspapieren zu dokumentieren.

98 Anhand der Dokumentation muss ein erfahrener Wirtschaftsprüfer, der nicht mit der Prüfung befasst war, in angemessener Zeit Folgendes nachvollziehen können:

- Einhaltung der Berufspflichten (insb. zum Grundsatz der Unabhängigkeit einschließlich möglicher Unabhängigkeitsgefährdungen und deren Lösung)
- Art, zeitliche Einteilung und Umfang der durchgeführten Prüfungshandlungen, um diesen *IDW Prüfungsstandard*, die rechtlichen Vorschriften und die Berufspflichten einzuhalten (vgl. Tz. A57)
- die Ergebnisse der Prüfungshandlungen und die erlangten Prüfungsnachweise
- bedeutsame Sachverhalte, die während der Prüfung aufgetreten sind sowie daraus resultierende bedeutsame Schlussfolgerungen und Beurteilungen (vgl. Tz. A58).

99 Erhält der Wirtschaftsprüfer Informationen, die einer zuvor erfolgten abschließenden Beurteilung eines bedeutsamen Prüfungssachverhalts entgegenstehen, hat er die in diesem Zusammenhang ergriffenen Maßnahmen (z.B. die Durchführung zusätzlicher Prüfungshandlungen) zu dokumentieren.

100 Der Abschluss der Auftragsdokumentation hat innerhalb eines angemessenen Zeitraums nach dem Datum der Berichterstattung zu erfolgen. Der Wirtschaftsprüfer darf die Löschung bzw. das Entfernen von Dokumentationen nach der abschließenden Zusammenstellung der Arbeitspapiere und finalen Auftragsdokumentation vor dem Ablauf der Aufbewahrungsfrist nicht vornehmen.

101 Für den Fall, dass der Wirtschaftsprüfer es als notwendig erachtet, nach der abschließenden Zusammenstellung die Auftragsdokumentation zu ändern oder zu ergänzen, und dies keine Auswirkungen auf die Berichterstattung hat, ist Folgendes zu dokumentieren:

- Die Gründe für die Änderungen bzw. Ergänzungen und
- von wem sie wann durchgeführt und wie sie kontrolliert wurden.

2.6. Berichterstattung des Wirtschaftsprüfers

2.6.1. Allgemeine Anforderungen an die Berichterstattung

102 Der Wirtschaftsprüfer hat eine schriftliche Berichterstattung – entweder als Prüfungsvermerk oder als Prüfungsbericht – zu verfassen, die ein Prüfungsurteil bzw. erforderlichenfalls eine Aussage enthält, dass ein Prüfungsurteil nicht erteilt werden kann (vgl. Tz. A59).

103 Ein Prüfungsbericht des Wirtschaftsprüfers beinhaltet gegenüber einem Prüfungsvermerk zusätzlich eine zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und ggf. Funktionsprüfungen und der weiteren Prüfungshandlungen sowie Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen.

104 In der Berichterstattung ist das Prüfungsurteil von anderen Informationen und Erläuterungen (z.B. Hervorhebungen und Hinweise (Tz. 94 ff.) oder Feststellungen und Empfehlungen, die keinen Einfluss auf das Urteil haben) klar zu trennen.

105 Ein Prüfungsvermerk muss folgende Bestandteile enthalten (vgl. Tz. A60–A62):

a) Überschrift: Angabe, dass es sich um den Prüfungsvermerk eines unabhängigen Wirtschaftsprüfers handelt

b) Berichtsadressaten

c) Prüfungsauftrag einschließlich einer Angabe des zu prüfenden Zeitraums bzw. des zu prüfenden Zeitpunkts

d) Beschreibung des geprüften IT-Systems

e) Beschreibung der Verantwortlichkeiten der gesetzlichen Vertreter

f) Darstellung der oder Bezugnahme auf die vom Unternehmen verwendeten Kriterien; sofern bei der Beurteilung des Prüfungsobjekts Kriterien verwendet wurden, die nur einem eingeschränkten Nutzerkreis zugänglich sein sollen (z.B. Vertragsdaten, Preise), ist auf diesen Umstand im Prüfungsvermerk hinzuweisen. Ferner ist darauf hinzuweisen, wenn die verwendeten Kriterien für einen speziellen Zweck entwickelt wurden und dementsprechend die Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) bzw. die Darstellung des geprüften IT-Systems (direkte IT-Prüfung) für andere Zwecke möglicherweise nicht geeignet ist.

g) Beschreibung der Verantwortlichkeiten des Wirtschaftsprüfers

h) Gegenstand, Art und Umfang der Prüfung einschließlich einer Aussage, dass es sich um einen Auftrag zur Erlangung hinreichender Sicherheit handelt

i) Aussage, dass die Prüfung in Übereinstimmung mit diesem *IDW Prüfungsstandard* durchgeführt wurde; der Wirtschaftsprüfer darf nicht die Einhaltung dieses *IDW Prüfungsstandards* erklären, wenn er nicht sämtliche einschlägigen Anforderungen beachtet hat

j) 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

k) Prüfungsurteil

l) Aussage über die inhärenten Grenzen des geprüften IT-Systems und zum Risiko, die Feststellungen zum geprüften IT-System auf die Zukunft zu übertragen

m) falls relevant, bei einer Prüfung einer Erklärung zum IT-System ggf. Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter zum IT-System

n) Aussage, dass der Auftrag für einen bestimmten Zweck bzw. Adressatenkreis durchgeführt wurde und deshalb die Verwendung der Ergebnisse für andere Zwecke möglicherweise nicht geeignet ist

o) Datum des Prüfungsvermerks: Das Datum darf nicht vor dem Datum liegen, an dem der Wirtschaftsprüfer ausreichende geeignete Prüfungsnachweise als Grundlage für das Prüfungsurteil über das IT-System erlangt hat.

p) Unterschrift, Name und Ort des Wirtschaftsprüfers.

106 Wenn der Wirtschaftsprüfer auf die Arbeit eines Sachverständigen des Wirtschaftsprüfers Bezug nimmt, darf nicht der Eindruck entstehen, dass die Verantwortung des Wirtschaftsprüfers für das Prüfungsurteil durch diese Bezugnahme verringert wird.

2.6.2. Ergänzende Bestandteile der Berichterstattung bei einer Prüfung einer Erklärung zum IT-System

107 Die Erklärung der gesetzlichen Vertreter zum IT-System ist als Bestandteil in die Berichterstattung aufzunehmen. Das Datum der Erklärung der gesetzlichen Vertreter zum IT-System muss möglichst zeitnah zum Datum der Berichterstattung sein, in keinem Fall jedoch danach.

108 Sind in der Erklärung der gesetzlichen Vertreter zum IT-System auch nicht geprüfte Angaben enthalten, ist dies in der Berichterstattung zu verdeutlichen.

109 Das Prüfungsurteil bei einer Prüfung einer Erklärung zum IT-System in Form einer Angemessenheitsprüfung hat ein Urteil zu enthalten, dass

- die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet sind,
- die Erklärung der gesetzlichen Vertreter zum IT-System in allen wesentlichen Belangen frei von wesentlichen Fehlern ist,
- das in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellte IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet war, die Kriterien zu erfüllen, und
  - zum zu prüfenden Zeitpunkt implementiert war.

110 Das Prüfungsurteil bei einer Prüfung einer Erklärung zum IT-System in Form einer Wirksamkeitsprüfung hat ein Urteil zu enthalten, dass

- die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet sind,
- die Erklärung der gesetzlichen Vertreter zum IT-System in allen wesentlichen Belangen frei von wesentlichen Fehlern ist,
- das in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellte IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet war, die Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert war und
  - im geprüften Zeitraum wirksam war.

2.6.3. Ergänzende Bestandteile der Berichterstattung bei einer direkten IT-Prüfung

111 Der Prüfungsgegenstand ist in der Berichterstattung in allen wesentlichen Belangen darzustellen, damit sich die vorgesehenen Nutzer ein angemessenes Bild von dem geprüften IT-System einschließlich der angewandten Grundsätze, Verfahren und Maßnahmen verschaffen können.

112 Das Prüfungsurteil bei einer direkten IT-Prüfung in Form einer Angemessenheitsprüfung hat ein Urteil zu enthalten, dass

- die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet sind,
- das IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet war, die Kriterien zu erfüllen, und
  - zum zu prüfenden Zeitpunkt implementiert war.

113 Das Prüfungsurteil bei einer direkten IT-Prüfung in Form einer Wirksamkeitsprüfung hat ein Urteil zu enthalten, dass

- die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet sind,
- das IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet war, die Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert war und
  - im geprüften Zeitraum wirksam war.

2.6.4. Weitere Berichtspflichten

114 Wenn nach Einschätzung des Wirtschaftsprüfers bestimmte Prüfungsfeststellungen eine unmittelbare Reaktion des Unternehmens erfordern, ist darüber vorab zu berichten.

115 Der Wirtschaftsprüfer muss feststellen, ob ggf. weitere Berichtspflichten bestehen, z.B. gegenüber dem Aufsichtsorgan des Unternehmens. Im Falle einer Berichtspflicht ist diese im Prüfungsvermerk bzw. im Prüfungsbericht oder in sonstiger geeigneter Weise zu erfüllen (vgl. Tz. A21, A63).

3. Anwendungshinweise und sonstige Erläuterungen

Vorbemerkungen [Tz. 1 ff.]

A1 Beispiele für IT-gestützte Prozesse und Verfahren, für die eine Prüfung nach diesem *IDW Prüfungsstandard* durchgeführt werden kann, sind:

- Erfüllung von gesetzlichen oder regulatorischen Anforderungen außerhalb der Abschlussprüfung, z.B. Erfüllung der MaRisk[15], des IT-Sicherheitsgesetzes oder des Bundesdatenschutzgesetzes (BDSG) bzw. der EU-Datenschutz-Grundverordnung (EU-DSGVO)
- Sicherheit im Softwareentwicklungsprozess
- Konformität von IT-Systemen mit steuerlichen Vorgaben (§§ 14, 14b UStG, §§ 146, 147 AO, GoBD)
- Konformität von IT-Systemen mit Industrie-Standards, z.B. Payment Card Industry Data Security Standard (PCI DSS), Archivierungsstandards, etc.
- Konformität von IT-Systemen mit ISO- und DIN-Normen
- Konformität von IT-Systemen mit allgemein anerkannten Frameworks, z.B. COSO[16], COBIT[17], ITIL®[18],

[15] Vgl. Rundschreiben 09/2017 (BA) „Mindestanforderungen an das Risikomanagement – MaRisk“ der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) vom 27.10.2017.

[16] www.coso.org.

[17] www.isaca.org/cobit.

[18] www.axelos.com.

- Konformität von Projekten oder Prozessen mit allgemein anerkannten oder sonstigen Frameworks, z.B. PRINCE2®[19], Guide to the Project Management Body of Knowledge (PMBOK Guide)[20]
- Wirksamkeit von Kontrollen zur Personalbeschaffung und zum Personaltraining.

A2 Spezielle IDW Prüfungsstandards für die Prüfung von Systemen sind bspw.

- *IDW Prüfungsstandard: Die Prüfung von Softwareprodukten (IDW PS 880)*[21],
- *IDW Prüfungsstandard: Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen (IDW PS 951 n.F.)*[22],
- *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980)*[23],
- *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981)*[24],
- *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung des internen Kontrollsystems des internen und externen Berichtswesens (IDW PS 982)*[25],
- *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Internen Revisionssystemen (IDW PS 983)*.

Definitionen [Tz. 10 f.]

A3 Die vorgesehenen Nutzer können sich vom Adressaten der Berichterstattung unterscheiden. Unter Umständen ist es dem Wirtschaftsprüfer nicht möglich, alle Personen, Organisationen und Gruppen, die die Berichterstattung erhalten werden, zu identifizieren. In solchen Fällen können die vorgesehenen Nutzer auf die maßgeblichen Interessengruppen beschränkt werden. Die vorgesehenen Nutzer können auf unterschiedlichen Wegen festgelegt werden. Maßgeblich dafür ist in erster Linie der Vertrag zwischen dem Wirtschaftsprüfer und seinem Auftraggeber. Es kann daher sinnvoll sein, in diesen Vertrag entsprechende Regelungen aufzunehmen. Es sind jedoch auch andere Wege denkbar, wie z.B. gesetzliche Vorschriften oder Anordnungen.

A4 Für eine Prüfung nach diesem *IDW Prüfungsstandard* verwendete Kriterien können auf verschiedene Weise ausgewählt bzw. entwickelt werden:

- Gesetzliche oder sonstige regulatorische Anforderungen
- Standards und Rahmenwerke, die einen anerkannten definierten Formulierungs-, Abstimmungs- und Veröffentlichungsprozess durchlaufen haben[26]

---

19 www.axelos.com.

20 www.pmi.org.

21 Stand: 11.03.2010.

22 Stand: 16.10.2013.

23 Stand: 11.03.2011.

24 Stand: 03.03.2017.

25 Stand: 03.03.2017.

26 Ein anerkannter definierter Formulierungs-, Abstimmungs- und Veröffentlichungsprozess beinhaltet die Veröffentlichung als Entwurf und die Möglichkeit der Kommentierung durch Fachkreise oder die interessierte Öffentlichkeit.

- weitere Standards, die keinem transparenten Verfahren unterlegen haben, aus Veröffentlichungen oder Büchern entnommen, zur kommerziellen Vermarktung entwickelt oder speziell für das Prüfungsobjekt erstellt wurden.

A5 Zu den gesetzlichen Anforderungen können neben den handels- und steuerrechtlichen Anforderungen sowie den Grundsätzen ordnungsmäßiger Buchführung auch branchenspezifische Gesetze (z.B. Gesetz über das Kreditwesen, Gesetz über den Wertpapierhandel) und Verordnungen zählen. Regulatorische Anforderungen an IT-Systeme betreffen z.B. Aufbewahrungsfristen nach § 257 HGB und § 147 AO, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der für den Betrieb der kritischen Infrastrukturen erforderlichen informationstechnischen Systeme, Komponenten oder Prozesse nach § 8a BSIG, organisatorische und technische Vorgaben nach dem BDSG. Die allgemeinen Grundsätze an die Ordnungsmäßigkeit und Sicherheit IT-gestützter rechnungslegungsrelevanter Verfahren sind in *IDW RS FAIT 1* erläutert. Sachgebietsspezifische Ergänzungen und Auslegungen ergeben sich i.Z.m. Dokumentenmanagementsystemen aus *IDW RS FAIT 3*, im Rahmen der Konzernrechnungslegung aus *IDW RS FAIT 4* und bei Auslagerungen und der Nutzung von Cloud Computing aus *IDW RS FAIT 5*.

A6 Beispiele für Standards und Rahmenwerke mit Bezug zu IT, die einen anerkannten definierten Formulierungs-, Abstimmungs- und Veröffentlichungsprozess durchlaufen haben, sind

- Verwaltungsanweisungen von Aufsichtsbehörden, z.B. Mindestanforderungen an das Risikomanagement – MaRisk, Mindestanforderung an die Sicherheit von Internetzahlungen (MaSI)[27],
- *IDW RS FAIT 1*, *IDW RS FAIT 2*[28], *IDW RS FAIT 3*, *IDW RS FAIT 4* und *IDW RS FAIT 5*,
- COSO-Modell zur Gestaltung interner Kontrollsysteme (herausgegeben vom Committee of Sponsoring Organizations of the Treadway Commission),
- COBIT (herausgegeben von der Information Systems Audit and Control Association (ISACA)),
- ISO- und DIN-Normen, z.B. ISO 27001 zur Gestaltung des Informationssicherheitsmanagements.

A7 Weitere Standards sind z.B. aufgabenbezogene Anforderungen wie Good Manufacturing Practice (GMP).

A8 Hinreichende Sicherheit bedeutet nicht absolute Sicherheit: Auch ein wirksames IT-System unterliegt systemimmanenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird. Diese systemimmanenten Grenzen ergeben sich u.a. aus menschlichen Fehlleistungen (bspw. infolge von Nachlässigkeit, Ablenkungen, Beurteilungsfehlern und Missverstehen von Arbeitsanweisungen), Missbrauch oder Vernachlässigung der Verantwortung durch für bestimmte Maßnahmen verantwortliche Personen, der Umgehung

---

[27] Vgl. Rundschreiben 4/2015 (BA) „Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)“ der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) vom 05.05.2015.

[28] Vgl. *IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce (IDW RS FAIT 2)* (Stand: 29.09.2003).

oder Außerkraftsetzung von Kontrollen durch Zusammenwirken zweier oder mehrerer Personen oder dem Verzicht des Unternehmens auf bestimmte Maßnahmen, weil die Kosten dafür höher eingeschätzt werden als der erwartete Nutzen.

A9 Ein Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System kann z.B. vorliegen, wenn die Erklärung

- nicht sämtliche Mindestinhalte (vgl. Tz. 24) umfasst,
- einen vorhandenen Mangel in dem in der Erklärung dargestellten IT-System nicht erkennen lässt oder
- unangemessene Verallgemeinerungen bzw. unausgewogene und verzerrende Darstellungen enthält.

A10 Unternehmen i.S. dieses IDW Prüfungsstandards können neben Unternehmen im rechtlichen Sinne auch Gesellschaften bürgerlichen Rechts, rechtsfähige oder nicht rechtsfähige Vereine, Stiftungen, Gebietskörperschaften, sonstige Körperschaften, Eigenbetriebe, Anstalten des öffentlichen Rechts, Gemeinschaften, natürliche Personen oder sonstige wirtschaftlich abgegrenzte Geschäftstätigkeiten (z.B. Standorte, selbstständige Teilbetriebe, Sparten) oder Gruppen dieser Einheiten sein.

Gegenstand, Ziel und Umfang der Prüfung [Tz. 12 ff.]

A11 Gemäß Tz. 13 und 18 liegt die Dokumentation des zu prüfenden IT-Systems und der angewendeten Grundsätze, Verfahren und Maßnahmen in der Verantwortung der gesetzlichen Vertreter. Art und Umfang sind abhängig von den mit der Dokumentation verfolgten Zielen (z.B. Dokumentation zum Nachweis der Wirksamkeit der Grundsätze, Verfahren und Maßnahmen des IT-Systems gegenüber Dritten, etwa Aufsichtsbehörden).

A12 Bei der Beurteilung, ob ein angemessen dokumentiertes IT-System vorliegt, ist von Bedeutung, dass eine unvollständige Dokumentation des IT-Systems zu Zweifeln an der dauerhaften Funktionsfähigkeit der eingerichteten Grundsätze, Verfahren und Maßnahmen führen kann.

Auftragsannahme [Tz. 27 ff.]

A13 Damit die vorgesehenen Nutzer ein Verständnis über die Beurteilung des Prüfungsobjekts entwickeln können, ist es von Bedeutung, dass die verwendeten Kriterien verfügbar sind. Hierzu kommen folgende Wege in Betracht:

- Öffentliche Quellen
- Einbeziehung in die Darstellung des Prüfungsgegenstands bzw. die Erklärung der gesetzlichen Vertreter zum IT-System
- Abdruck in der Berichterstattung
- Kriterien, bei denen von einem allgemeinen Verständnis ausgegangen werden kann (z.B. Zeit, Längen-, Gewichtsangaben).

A14 Kriterien aus gesetzlichen und sonstigen regulatorischen Anforderungen sowie aus Standards und Rahmenwerken, die einen allgemein anerkannten, definierten Formulierungs-, Abstimmungs- und Veröffentlichungsprozess durchlaufen haben, betreffen häufig das gesamte IT-

System sowie die diesbezüglichen Kontrollaspekte. Bei einer Prüfung nach diesem *IDW Prüfungsstandard* ist es zulässig, die Prüfung auf in sich abgeschlossene Teilbereiche dieser Vorschriften bzw. Standards einzuschränken: Beispielsweise kann für eine Prüfung des IT-Servicemanagements auf Basis des COBIT-Frameworks eine Einschränkung auf die Domäne „Deliver Service and Support“ sachgerecht sein.

A15 Merkmale geeigneter Kriterien sind:

- *Relevanz:* Die Kriterien sind für die Entscheidungsfindung maßgeblich.
- *Vollständigkeit:* Kriterien sind vollständig, wenn keine für die Beurteilung des Prüfungsobjekts und die Entscheidungsfindung wesentlichen Gesichtspunkte fehlen.
- *Verlässlichkeit:* Verlässliche Kriterien ermöglichen eine konsistente Beurteilung ähnlicher Sachverhalte auch durch unterschiedliche Wirtschaftsprüfer.
- *Neutralität:* Neutrale Kriterien führen zu Informationen, die frei von irreführenden Darstellungen sind.
- *Verständlichkeit:* Verständliche Kriterien ermöglichen klare Schlussfolgerungen und vermeiden Fehlinterpretationen.

A16 Ungenaue Erwartungswerte oder Erfahrungswerte einzelner Personen sind keine geeigneten Kriterien i.S. dieses *IDW Prüfungsstandards*.

A17 Neben der beauftragenden Partei bzw. der für das Prüfungsobjekt verantwortlichen Partei und dem Wirtschaftsprüfer können ebenso die vorgesehenen Nutzer in die Bestimmung der dem Sachverhalt zugrunde zu legenden Kriterien einbezogen werden. Dies betrifft z.B. die Berücksichtigung von speziellen nationalen Regelungen oder Verordnungen bei IT-Systemen mit internationaler Dimension (bspw. Cloud Computing, europäisches IT-Dienstleistungsunternehmen). Die Eigenverantwortung des Wirtschaftsprüfers für die daraus abgeleitete Prüfungsplanung bleibt hiervon unberührt.

A18 Aufgabenbezogene Anforderungen an die Ausgestaltung von IT-Systemen können sich z.B. aus Industriestandards, wie bspw. dem Payment Card Industry Data Security Standard (PCI DSS) ergeben.

A19 Eine missbräuchliche Verwendung der Berichterstattung des Wirtschaftsprüfers kann bspw. in den folgenden Fällen gegeben sein:

- Missbräuchliche Anwendung des Kreises der vorgesehenen Nutzer
- missbräuchliche Abgrenzung des Prüfungsobjekts bei bekannten Mängeln des IT-Systems.

A20 Im Interesse des Auftraggebers und des Wirtschaftsprüfers sollten die Auftragsbedingungen vor dem Prüfungsbeginn schriftlich vereinbart werden, um Missverständnisse zwischen den involvierten Parteien zu vermeiden. Art und Inhalt der schriftlich vereinbarten Auftragsbedingungen können in Abhängigkeit von den Rahmenbedingungen des jeweiligen Auftrags variieren.

A21 Folgende Aspekte können mit dem Auftraggeber schriftlich vereinbart werden:

- Ziel und Gegenstand der Prüfung

- die Verantwortung der gesetzlichen Vertreter für das IT-System sowie im Falle einer Prüfung einer Erklärung zum IT-System auch für das Vorliegen und die Inhalte der schriftlichen Erklärung der gesetzlichen Vertreter zum IT-System
- die verwendeten Kriterien; ggf. der Umstand, dass diese nur einem eingeschränkten Nutzerkreis zugänglich sein sollen (z.B. Vertragsdaten, Preise)
- Art und Umfang der Prüfung und der Berichterstattung einschließlich einer Bezugnahme auf diesen *IDW Prüfungsstandard*; dies bezieht sich auch auf eine etwaige Berichtspflicht gegenüber Dritten (vgl. Tz. 115)
- die Tatsache, dass die Prüfung der Aussagen in der Erklärung der gesetzlichen Vertreter zum IT-System (bei einer Prüfung einer Erklärung zum IT-System) bzw. des in der Auftragsvereinbarung abgegrenzten, zu prüfenden IT-Systems risikoorientiert erfolgt und keine Vollprüfung, sondern eine Prüfung in einer Auswahl vorgenommen wird und deshalb ein unvermeidbares Risiko besteht, dass selbst wesentliche falsche Aussagen in der Erklärung der gesetzlichen Vertreter zum IT-System bzw. wesentliche Mängel im zu prüfenden IT-System unentdeckt bleiben
- ein Hinweis auf die systemimmanenten Grenzen des zu prüfenden IT-Systems und darauf, dass die Prüfung nicht darauf ausgerichtet ist, festzustellen, ob einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder durchgeführte Maßnahmen zur Einhaltung der Kriterien geeignet oder wirtschaftlich sinnvoll sind
- bei einer Angemessenheitsprüfung: Zeitpunkt, auf den sich die Prüfung der Angemessenheit beziehen soll
- bei einer Wirksamkeitsprüfung: Zeitraum, auf den sich die Prüfung der Wirksamkeit beziehen soll
- Hinweise auf die Verwertung von Arbeiten der Internen Revision, anderer Wirtschaftsprüfer sowie von Sachverständigen
- das Erfordernis eines unbeschränkten Zugangs des Wirtschaftsprüfers 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 den Auslagenersatz
- ggf. Haftungsregelungen
- die Verpflichtung der gesetzlichen Vertreter, eine Vollständigkeitserklärung abzugeben
- ggf. Verwendungsvorbehalt der Berichterstattung sowie
- ggf. Hinweis auf Berichtspflichten gegenüber dem Aufsichtsorgan.

A22 Wenn der Wirtschaftsprüfer auch mit anderen Dienstleistungen, wie bspw. der Abschlussprüfung oder der Prüfung des Compliance Management Systems beauftragt war und er in deren Rahmen für sein Urteil über den Prüfungsgegenstand evtl. relevante Informationen erlangt hat, kann es sinnvoll sein zu vereinbaren, dass er das Ergebnis der Tätigkeiten bei der Prüfung nach diesem *IDW Prüfungsstandard* berücksichtigt.

A23 Als mögliche Maßnahmen bei Bekanntwerden von Informationen nach der Auftragsannahme, die vor der Auftragsannahme zur Ablehnung des Auftrags geführt hätten, kommen z.B. bei Unabhängigkeitsrisiken die Ergreifung von Schutzmaßnahmen i.S. von § 30 BS WP/vBP oder ggf. die Niederlegung des Mandats in Betracht.

A24 Beispiele für wesentliche Änderungen der Bedingungen des Prüfungsauftrags sind:

- Die Auftragsart, d.h. Prüfung einer Erklärung zum IT-System oder direkte IT-Prüfung, wird geändert.
- Anstelle einer Wirksamkeitsprüfung soll nur eine Angemessenheitsprüfung durchgeführt werden.

Prüfungsplanung [Tz. 41 ff.]

A25 Praktische Erfahrungen mit IT-Prüfungen sowie notwendige Branchen- und ggf. Rechtskenntnisse können z.B. umfassen:

- Praktische Erfahrungen im Umgang mit Datenanalysen
- Kenntnisse über den Aufbau von ERP-Systemen, Datenbanken oder Betriebssystemen.

A26 Für die Gewinnung eines Verständnisses vom Unternehmen und dem rechtlichen und wirtschaftlichen Umfeld können insb. die folgenden Informationsquellen in Betracht kommen:

- Informationsdienste
- Auftritt des Unternehmens im Internet
- Branchenvergleichsinformationen
- Geschäftsbericht des Vorjahres.

A27 Folgende Prüfungshandlungen können im Rahmen der Risikoidentifikation und Risikobeurteilung in Betracht kommen:

- Befragung des Managements
- Ableitung aus der Erfahrung des Wirtschaftsprüfers
- Durchsicht von Dokumentationen und vorhandenen Berichten der Internen Revision.

A28 Ein wesentlicher Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System liegt z.B. dann vor, wenn

- sie einen vorhandenen wesentlichen Mangel des IT-Systems nicht erkennen lässt,
- sie falsche Angaben enthält oder Angaben fehlen, die – einzeln oder in der Summe – für die Adressaten der Erklärung entscheidungsrelevant sein können, oder
- sie unangemessene Verallgemeinerungen oder unausgewogene und verzerrende Darstellungen enthält, die eine Irreführung der Adressaten der Erklärung zur Folge haben können.

A29 Ein wesentlicher Mangel des IT-Systems liegt z.B. dann vor, wenn die Grundsätze, Verfahren und Maßnahmen nicht geeignet, nicht implementiert oder nicht wirksam sind, mit hinreichender Sicherheit die Kriterien in Bezug auf das IT-System in allen wesentlichen Belangen einzuhalten.

Prüfungsdurchführung

Prüfung der Angemessenheit des IT-Systems [Tz 57 ff.]

A30 Bei der Festlegung der Prüfungshandlungen kann der Prüfer bei wiederkehrenden Aufträgen Ergebnisse früherer Prüfungen des IT-Systems verwerten. Dies gilt vor allem für die Beurteilung der Angemessenheit des IT-Systems, die sich bei Folgeprüfungen vor allem auf Veränderungen des IT-Systems erstrecken wird.

A31 Relevante Ergebnisse von Prüfungshandlungen, die ggf. im Rahmen einer Abschlussprüfung oder einer anderen betriebswirtschaftlichen Prüfung gewonnen wurden, können für Zwecke der Prüfung der Angemessenheit nach diesem *IDW Prüfungsstandard* berücksichtigt werden. Diese Ergebnisse werden für Zwecke der Prüfung i.S. dieses *IDW Prüfungsstandards* allein jedoch nicht ausreichend sein.

A32 Bei der Beurteilung der Regelungen zum IT-Kontrollumfeld und zur IT-Organisation können die Einstellungen und das Problembewusstsein der gesetzlichen Vertreter und der mit der Überwachung des Unternehmens betrauten Mitarbeiter sowie die Aufbau- und Ablauforganisation durch die Durchsicht von Regelwerken und dokumentierten Verhaltensgrundsätzen, Befragungen, Beobachtung und Nachvollziehen des gelebten Verhaltens eingeschätzt werden. In diesem Zusammenhang ist nicht nur das formale Bestehen von Grundsätzen, Verfahren und Maßnahmen, sondern auch deren tatsächliche Umsetzung im Unternehmen von Bedeutung.

A33 Art, Umfang und zeitliche Einteilung der im Rahmen der Prüfung der Angemessenheit durchzuführenden Prüfungshandlungen (vgl. Tz. A34) können u.a. abhängig sein von

- den verwendeten Kriterien,
- den Inhalten der Erklärung der gesetzlichen Vertreter zum IT-System (bei einer Prüfung einer Erklärung zum IT-System),
- der Ausgestaltung des IT-Systems und dessen Dokumentation,
- der Art und Weise der Überwachung des IT-Systems, z.B. durch die Interne Revision oder andere unternehmensinterne Funktionen sowie
- Wesentlichkeitsüberlegungen.

A34 Im Rahmen der Prüfung der Angemessenheit können insb. die folgenden Prüfungshandlungen in Betracht kommen:

- Befragung der gesetzlichen Vertreter und anderer Mitglieder des Managements (z.B. zur Konzeption des IT-Systems, zu bekannten Schwachstellen im IT-System)
- Befragung von Personen, die für die Steuerung und Überwachung des IT-Systems und die Koordination von Aktivitäten i.Z.m. dem IT-System zuständig sind, um deren Aufgabenstellung, Kompetenz und Erfahrung und Kenntnisse über mögliche Schwachstellen im IT-System und festgestellte Verstöße sowie die Reaktionen des Unternehmens auf solche Feststellungen in Erfahrung zu bringen
- Durchsicht von Unterlagen zu Vorfällen *(incidents)*, die von Anwendern/Nutzern i.Z.m. dem Einsatz des IT-Systems gemeldet wurden
- Durchsicht von Dokumentationen des IT-Systems (z.B. Netzwerkdiagramme und Richtlinien zum IT-Betrieb, einschließlich entsprechender Anweisungen an die Mitarbeiter)
- Durchsicht von Unterlagen, die durch das IT-System generiert werden (u.a. Fehlerberichte, Logs)

- Beobachtung von Aktivitäten und Arbeitsabläufen, die mit dem IT-System in Verbindung stehen.

A35 Im Rahmen des Prozessdurchlaufs (sog. *walkthrough*) folgt der Wirtschaftsprüfer den tatsächlichen Geschäftsvorfällen und/oder Ver- und Bearbeitungsschritten durch die für das IT-System relevanten Prozessabläufe, einschließlich der IT-gestützten Prozessschritte.

Prüfung der Wirksamkeit des IT-Systems [Tz. 60 ff.]

A36 Die Prüfung der Wirksamkeit umfasst die laufende Einhaltung der Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems in dem zu prüfenden Zeitraum. Es wird geprüft, ob die Grundsätze, Verfahren und Maßnahmen wie vorgesehen und von den dafür bestimmten Personen beachtet bzw. durchgeführt wurden. Durch diese Prüfungshandlungen wird der Nachweis der laufenden Einhaltung der Kriterien erbracht.

A37 Art, Umfang und zeitliche Einteilung der im Rahmen der Prüfung der Wirksamkeit durchzuführenden Funktionsprüfungen können u.a. abhängig sein von

- den verwendeten Kriterien,
- den angewandten Grundsätzen, Verfahren und Maßnahmen,
- den Inhalten der Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System),
- der Ausgestaltung des zu prüfenden IT-Systems und dessen Dokumentation sowie
- Wesentlichkeitsüberlegungen.

A38 Folgende Prüfungshandlungen können im Rahmen der Prüfung der Wirksamkeit in Betracht kommen:

- Befragung der von den Grundsätzen, Verfahren und Maßnahmen betroffenen Personen (gesetzliche Vertreter, mit dem zu prüfenden IT-System befasste Mitarbeiter, Mitarbeiter der Internen Revision und andere relevante Mitarbeiter)
- Durchsicht und Auswertung der Dokumentation des zu prüfenden IT-Systems hinsichtlich der kontinuierlichen Anwendung der Grundsätze, Verfahren und Maßnahmen
- Beobachtung von Abläufen
- Nachvollzug von für die Einhaltung der Kriterien relevanten Kontrollen
- IT-gestützte Prüfungshandlungen (z.B. Datenanalysen).

A39 Der Umfang der durchzuführenden Prüfungshandlungen – bspw. der Stichprobenumfang – kann abhängig sein von der Frequenz der durchgeführten Kontrollen und dem eingeschätzten Risiko einer fehlerhaften Durchführung der Kontrolle.

A40 Eigene Beobachtungen sind i.d.R. aussagekräftiger als die Verwertung von Aussagen Dritter. Allerdings beziehen sich solche Beobachtungsergebnisse immer nur auf den Zeitpunkt der Prüfung. In diesen Fällen kann es daher erforderlich sein, weitere Prüfungshandlungen in Erwägung zu ziehen, um die kontinuierliche Anwendung der Grundsätze, Verfahren und Maßnahmen des IT-Systems zu prüfen.

Weitere Prüfungshandlungen

Verwertung der Arbeit von Sachverständigen des Wirtschaftsprüfers [Tz. 63 ff.]

A41 Eine Verwertung der Arbeit von Sachverständigen kann z.B. geboten sein bei der Beurteilung komplexer technischer oder rechtlicher Prozesse, z.B. im Bereich Forschung und Entwicklung, Energieerzeugung oder Lizenzmanagement.

A42 Informationen zu Kompetenz, Fähigkeiten und Objektivität eines externen Sachverständigen können aus unterschiedlichen Quellen stammen, bspw. aus

- persönlicher Erfahrung mit der bisherigen Tätigkeit des Sachverständigen,
- Gesprächen mit dem Sachverständigen,
- Gesprächen mit anderen Wirtschaftsprüfern oder anderen Personen, die mit der Arbeit des Sachverständigen vertraut sind,
- Kenntnissen über die Qualifikationen des Sachverständigen (Feststellung einer Berufszulassung bzw. Mitgliedschaft in einer Berufs- oder Branchenorganisation),
- Publikationen des Sachverständigen.

A43 Die folgenden Aspekte können bei der Beurteilung der Arbeiten externer Sachverständiger für die Zwecke des Prüfers relevant sein:

- Die Relevanz und Vertretbarkeit der Feststellungen und Schlussfolgerungen des Sachverständigen und ob diese mit anderen Prüfungsnachweisen in Einklang stehen;
- wenn den Arbeiten des Sachverständigen wesentliche Annahmen und Methoden zugrunde liegen, die Relevanz, Vollständigkeit und Vertretbarkeit dieser Annahmen und Methoden unter den gegebenen Umständen und
- wenn die Tätigkeit des Sachverständigen in der Verwendung von Ausgangsdaten besteht, die Relevanz, Vollständigkeit und Richtigkeit dieser Ausgangsdaten.

A44 Die Beurteilung der Arbeit von externen Sachverständigen kann z.B. durch Befragungen oder die Durchsicht der Berichterstattung bzw. der Arbeitspapiere des externen Sachverständigen erfolgen.

A45 Maßgebliche Faktoren bei der Beurteilung der Relevanz und Vertretbarkeit der Feststellungen und Schlussfolgerungen des Sachverständigen können die Frage einschließen, ob die Feststellungen und Schlussfolgerungen

- in einer Weise dargelegt sind, die mit Standards des Berufsstands oder der Branche des Sachverständigen in Einklang steht,
- klar ausgedrückt sind und eine Bezugnahme auf die mit dem Wirtschaftsprüfer vereinbarten Ziele, den Umfang der durchgeführten Tätigkeit sowie die angewendeten Standards enthält,
- auf einem angemessenen Zeitraum basieren und, sofern relevant, nachträglichen Ereignissen Rechnung tragen,
- Vorbehalten, Einschränkungen oder Verwendungsbeschränkungen unterliegen und, wenn ja, ob dies Konsequenzen für den Wirtschaftsprüfer hat und
- auf einer angemessenen Berücksichtigung von Irrtümern oder Abweichungen basieren, auf die der Sachverständige gestoßen ist.

A46 Zu den Faktoren, die für die Beurteilung der vom Sachverständigen verwendeten Methoden relevant sind, kann gehören, ob die Methoden

- innerhalb des Fachgebiets des Sachverständigen allgemein anerkannt sind,
- von der Anwendung spezialisierter Modelle abhängen und
- mit denjenigen des Unternehmens in Einklang stehen, z.B. Anwendung übereinstimmender Frameworks zum gleichen Sachverhalt, und, wenn nicht, die Gründe und Auswirkungen der Unterschiede.

Verwendung der Arbeit von Sachverständigen der gesetzlichen Vertreter, Verwendung oder Verwertung der Arbeit anderer Wirtschaftsprüfer sowie Verwendung der Arbeit der Internen Revision [Tz. 66 ff.]

A47 Die in Tz. A41 ff. dargestellten Anwendungshinweise können sinngemäß auch auf die Verwendung der Arbeit von Sachverständigen der gesetzlichen Vertreter, die Verwendung oder Verwertung der Arbeit eines anderen Wirtschaftsprüfers bzw. auf die Verwendung der Arbeit der Internen Revision angewandt werden. Die Verwendung der Arbeit eines anderen Wirtschaftsprüfers umfasst z.B. die Verwendung von Softwarebescheinigungen nach *IDW PS 880*.

Ereignisse nach dem Beurteilungszeitpunkt/-zeitraum [Tz. 70]

A48 Als Prüfungshandlungen zur Feststellung von Ereignissen nach dem Zeitpunkt bzw. Zeitraum, auf den sich die Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum IT-System) bzw. auf den sich die Prüfung des IT-Systems bezieht (direkte IT-Prüfung), können z.B. in Betracht kommen:

- Kritisches Lesen von Protokollen über in diesem Zeitraum stattgefundene Sitzungen der Verwaltungsorgane
- kritisches Lesen von unternehmensinternen Berichten, bspw. Berichte der Internen Revision sowie
- Befragungen der für das IT-System operativ verantwortlichen Personen und erforderlichenfalls der gesetzlichen Vertreter und des Aufsichtsorgans.

Sonstige Angaben in der Erklärung der gesetzlichen Vertreter zum IT-System [Tz. 73 ff.]

A49 Angaben, die nicht Gegenstand der Auftragsvereinbarung sind, können z.B. Angaben zur Wirksamkeit des IT-Systems bei einer Angemessenheitsprüfung sein.

A50 Als weitere angemessene Maßnahme kann der Wirtschaftsprüfer z.B. einen Hinweis in die Berichterstattung aufnehmen und darin die wesentliche Unstimmigkeit bzw. den wesentlichen offensichtlichen Fehler erläutern.

Schriftliche Erklärungen [Tz. 78 f.]

A51 Schriftliche Erklärungen sind kein Ersatz für andere nach diesem *IDW Prüfungsstandard* vorgesehene Prüfungshandlungen.

A52 Beispiele für weitere schriftliche Erklärungen sind:

- Schriftliche Erklärung bei einer Auslagerung von Teilen des IT-Systems auf ein Dienstleistungsunternehmen
- Bestätigung der gesetzlichen Vertreter, dass keine Änderungen am IT-System erfolgt sind.

Auswertung der Prüfungsfeststellungen und Bildung des Prüfungsurteils [Tz. 84 ff.]

A53 Stellt der Wirtschaftsprüfer eine Abweichung von den in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten (Prüfung einer Erklärung zum IT-System) bzw. von den vom Unternehmen angewendeten (direkte IT-Prüfung) Grundsätzen, Verfahren und Maßnahmen des zu prüfenden IT-Systems fest, kann es sinnvoll sein, durch weitere Prüfungshandlungen zu klären, ob es sich um einen Einzelfall handelt, der die Angemessenheit und Wirksamkeit des zu prüfenden IT-Systems nicht berührt, oder ob ein Mangel des zu prüfenden IT-Systems vorliegt. Als mögliche Prüfungshandlungen kommen hierbei bspw. in Betracht:

- Befragung der gesetzlichen Vertreter zur eigenen Einschätzung der Ursache der festgestellten Abweichung
- Würdigung des Umgangs des Unternehmens mit der festgestellten Abweichung
- Prüfung, ob mit der Überwachung des zu prüfenden IT-Systems beauftragte Personen vergleichbare Abweichungen identifiziert haben und welche Maßnahmen daraufhin veranlasst wurden.

A54 Bei einem festgestellten Mangel des zu prüfenden IT-Systems kann eine Beurteilung durch den Wirtschaftsprüfer sinnvoll sein, ob geeignete kompensierende Grundsätze, Verfahren und Maßnahmen vorhanden und – soweit einschlägig – wirksam sind. In diesem Fall kann bei einer Prüfung einer Erklärung zum IT-System eine entsprechende Anpassung der Erklärung der gesetzlichen Vertreter zum IT-System durch die gesetzlichen Vertreter oder bei einer Prüfung einer Erklärung zum IT-System bzw. einer direkten IT-Prüfung ein Hinweis (vgl. Tz. 95) in der Berichterstattung sinnvoll sein.

A55 Eine Einschränkung des Prüfungsurteils wird bspw. auch dann erforderlich sein, wenn der wesentliche, aber nicht umfassende Mangel des zu prüfenden IT-Systems bei einer Prüfung einer Erklärung zum IT-System angemessen in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellt ist. Dies ist bspw. der Fall, wenn die Erklärung der gesetzlichen Vertreter zum IT-System darauf hinweist, dass wesentliche Grundsätze, Verfahren und Maßnahmen noch nicht umgesetzt wurden, dies aber für die Zukunft vorgesehen ist.

A56 Ein Mangel des zu prüfenden IT-Systems, der nicht auf einzelne Teile der angewendeten Grundsätze, Verfahren und Maßnahmen einzugrenzen ist und bei dem das Prüfungsurteil zu versagen ist, kann z.B. vorliegen, wenn aufgrund von Mängeln bei der Konzeption des zu prüfenden IT-Systems oder aufgrund eines unangemessenen IT-Kontrollumfelds bzw. einer unangemessenen IT-Organisation die Grundsätze, Verfahren und Maßnahmen insgesamt als nicht angemessen anzusehen sind.

Dokumentation [Tz. 97 ff.]

A57 Die Dokumentation von Art, zeitlicher Einteilung und Umfang der Prüfungshandlungen beinhaltet bspw.,

- welche Prüfungsnachweise zur Angemessenheit und Wirksamkeit des IT-Systems erlangt wurden nebst deren eindeutiger Bezeichnung,
- von wem die Prüfungshandlungen durchgeführt und wann sie abgeschlossen wurden,
- von wem und wann die Prüfungshandlungen kontrolliert wurden sowie den Inhalt dieser Überprüfung.

A58 Soweit der Wirtschaftsprüfer bestimmte Arbeiten der Internen Revision oder von Sachverständigen verwertet, kann die Dokumentation dieser Verwertung von Bedeutung sein. Hiervon umfasst ist die Dokumentation seiner Beurteilungsergebnisse sowie seiner in diesem Zusammenhang durchgeführten Prüfungshandlungen.

Berichterstattung des Wirtschaftsprüfers

Allgemeine Anforderungen an die Berichterstattung [Tz. 102]

A59 Beispiele für die Formulierung des Prüfungsvermerks bzw. Prüfungsberichts finden sich in der Anlage 1 zu diesem *IDW Prüfungsstandard*.

A60 Die Mindestbestandteile des Prüfungsvermerks bzw. Prüfungsberichts können um weitere Angaben ergänzt werden, bspw.

- Angaben zum Datum der Beauftragung,
- Angaben zum Prüfungszeitraum.

A61 Zudem ist es zulässig, die Verwendung der Berichterstattung nur auf einen speziellen Nutzerkreis zu beschränken.

A62 Da freiwillige Prüfungen von IT-Systemen keine Vorbehaltsaufgabe i.S. des § 48 Abs. 1 Satz 1 WPO sind, besteht keine Pflicht zur Führung des Siegels.

Weitere Berichtspflichten [Tz. 114 f.]

A63 Im Zusammenhang mit der Prüfung des IT-Systems kann sich für den Wirtschaftsprüfer aus der Treuepflicht eine Pflicht zur Information des Auftraggebers über Sachverhalte ergeben, die anlässlich der Prüfung des IT-Systems festgestellt werden. Hierbei kann es sich z.B. handeln um

- beabsichtigte oder unbeabsichtigte Verstöße der gesetzlichen Vertreter oder von Mitarbeitern des Unternehmens gegen Gesetze und andere Vorschriften,
- Hinweise, dass einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder umgesetzte Maßnahmen offensichtlich nicht geeignet sind.

Anlagen

Die nachfolgenden Anlagen enthalten Beispiele für die Formulierung von Prüfungsvermerken bzw. Prüfungsberichten. Die zusätzlichen Bestandteile eines Prüfungsberichts gegenüber einem Prüfungsvermerk sind jeweils wie folgt kenntlich gemacht: [*kursiv*]

1. Prüfung einer Erklärung zum IT-System

1.1. Wirksamkeitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine IT-Prüfung nach *IDW PS 860*

An die [Gesellschaft]

Wir haben eine Prüfung der in nachstehender Anlage 1 beigefügten Erklärung der gesetzlichen Vertreter zur Beschreibung des [Beschreibung des IT-Systems] (im Folgenden das „IT-System“) sowie zur Angemessenheit und Wirksamkeit des IT-Systems (im Folgenden „Erklärung der gesetzlichen Vertreter zum IT-System“) der [Gesellschaft] (im Folgenden die „Gesellschaft“) für den Zeitraum vom [Datum] bis [Datum] durchgeführt.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der Gesellschaft sind für die Aufstellung der Erklärung zur Beschreibung des IT-Systems sowie zur Angemessenheit und Wirksamkeit des IT-Systems nach den untengenannten Kriterien verantwortlich sowie für die internen Kontrollen, die sie als notwendig erachten, um eine Erklärung zum IT-System aufzustellen, die frei von wesentlichen – beabsichtigten und unbeabsichtigten – Fehlern ist. Des Weiteren sind die gesetzlichen Vertreter für die von ihnen als notwendig erachteten Grundsätze, Verfahren und Maßnahmen zur Konzeption, Implementierung, Aufrechterhaltung, Überwachung und Dokumentation des IT-Systems verantwortlich, das in allen wesentlichen Belangen die untengenannten Kriterien zur Angemessenheit und Wirksamkeit erfüllt. Aufgrund bestehender inhärenter Grenzen von Systemen kann das IT-System diese Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Aufstellung der Erklärung der gesetzlichen Vertreter zum IT-System sowie zur Angemessenheit und Wirksamkeit des IT-Systems umfassen:

[Beschreibung der Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die Erklärung der gesetzlichen Vertreter zum IT-System frei von wesentlichen Fehlern ist.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* durchgeführt. Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Erklärung der gesetzlichen Vertreter zum IT-System in allen wesentlichen Belangen frei von wesentlichen Fehlern ist, was die Beurteilung umfasst, ob die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet sind, ob das in der Erklärung der gesetzlichen Vertreter dargestellte IT-System in allen wesentlichen Belangen geeignet war, mit hinreichender Sicherheit die Kriterien zu erfüllen, und ob dieses dargestellte IT-System in allen wesentlichen Belangen während des Zeitraums vom [Datum] bis [Datum] mit hinreichender Sicherheit implementiert war und die Kriterien wirksam erfüllt hat.

Eine Prüfung gemäß *IDW PS 860* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung von Risiken wesentlicher – beabsichtigter oder unbeabsichtigter – Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System ein. Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der Erklärung der gesetzlichen Vertreter zum IT-System angewandten Methoden und Kontrollen sowie der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens. Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der Erklärung der gesetzlichen Vertreter zum IT-System relevante interne Kontrollsystem abzugeben. Für die Beurteilung des IT-Systems ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel des IT-Systems mit hinreichender Sicherheit aufgedeckt werden. Die Prüfung des IT-Systems umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbau- und einer Funktionsprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung der Risiken des Vorhandenseins von wesentlichen Mängeln ein.

[*Prüfungshandlungen, Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen*

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen/Empfehlungen gegeben, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen und Empfehlungen dargestellten Sachverhalte keine gesonderten Prüfungsurteile ab.

a) sonstige Feststellungen, u.a.

- *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der Erklärung oder des IT-Systems*
- *nicht wesentliche falsche Angaben in der Erklärung*
- *nicht wesentliche Mängel in der Angemessenheit oder Wirksamkeit des IT-Systems*

*b) Empfehlungen***]**

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- sind die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- ist die Erklärung der gesetzlichen Vertreter zum IT-System in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- war das in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellte IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert und
  - im geprüften Zeitraum wirksam.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- sind die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- ist die Erklärung der gesetzlichen Vertreter zum IT-System in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- war das in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellte IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert und
  - im geprüften Zeitraum wirksam.]

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften IT-Systems

Auch ein wirksames IT-System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Erklärung der gesetzlichen Vertreter zum IT-System wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit des IT-Systems erstrecken sich auf den Zeitraum vom [Datum] bis [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen des IT-Systems falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter]

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Das IT-System wurde durch die Gesellschaft abgegrenzt und beinhaltet daher möglicherweise nicht jeden Aspekt eines IT-Systems, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte. Folglich ist die Erklärung der gesetzlichen Vertreter zum IT-System möglicherweise für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an die Gesellschaft gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Erklärung der gesetzlichen Vertreter zum IT-System

Allgemeine Auftragsbedingungen

1.2. Angemessenheitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine IT-Prüfung nach *IDW PS 860*

An die [Gesellschaft]

Wir haben eine Prüfung der in nachstehender Anlage 1 beigefügten Erklärung der gesetzlichen Vertreter zur Beschreibung des [Beschreibung des IT-Systems] (im Folgenden das „IT-System“) sowie zur Angemessenheit des IT-Systems (im Folgenden „Erklärung der gesetzlichen Vertreter zum IT-System“) der [Gesellschaft] (im Folgenden die „Gesellschaft“) zum [Datum] durchgeführt.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der Gesellschaft sind für die Aufstellung der Erklärung zur Beschreibung des IT-Systems sowie zur Angemessenheit des IT-Systems nach den untengenannten Kriterien verantwortlich sowie für die internen Kontrollen, die sie als notwendig erachten, um eine Erklärung zum IT-System aufzustellen, die frei von wesentlichen – beabsichtigten und unbeabsichtigten – Fehlern ist. Des Weiteren sind die gesetzlichen Vertreter für die von ihnen als notwendig erachteten Grundsätze, Verfahren und Maßnahmen zur Konzeption, Implementierung, Aufrechterhaltung, Überwachung und Dokumentation des IT-Systems verantwortlich, das in allen wesentlichen Belangen die untengenannten Kriterien zur Angemessenheit erfüllt. Aufgrund bestehender inhärenter Grenzen von Systemen kann das IT-System diese Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Aufstellung der Erklärung der gesetzlichen Vertreter zum IT-System sowie zur Angemessenheit des IT-Systems umfassen:

[Beschreibung der Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die Erklärung der gesetzlichen Vertreter zum IT-System frei von wesentlichen Fehlern ist.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* durchgeführt. Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Erklärung der gesetzlichen Vertreter zum IT-System in allen wesentlichen Belangen frei von wesentlichen Fehlern ist, was die Beurteilung umfasst, ob die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet sind, ob das in der Erklärung der gesetzlichen Vertreter dargestellte IT-System in allen wesentlichen Belangen geeignet war, mit hinreichender Sicherheit die Kriterien zu erfüllen, und ob dieses dargestellte IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit zum [Datum] implementiert war.

Eine Prüfung gemäß *IDW PS 860* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung von Risiken wesentlicher – beabsichtigter oder unbeabsichtigter – Fehler in der Erklärung der gesetzlichen Vertreter zum IT-System ein. Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der Erklärung der gesetzlichen Vertreter zum IT-System angewandten Methoden und Kontrollen sowie der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens. Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der Erklärung der gesetzlichen Vertreter zum IT-System relevante interne Kontrollsystem abzugeben. Für die Beurteilung des IT-Systems ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel des IT-Systems mit hinreichender Sicherheit aufgedeckt werden. Die Prüfung des IT-Systems umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbauprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung der Risiken des Vorhandenseins von wesentlichen Mängeln ein.

[*Prüfungshandlungen, Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen*

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen/Empfehlungen gegeben, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen und Empfehlungen dargestellten Sachverhalte keine gesonderten Prüfungsurteile ab.

a) *sonstige Feststellungen, u.a.*
   - *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der Erklärung oder des IT-Systems*
   - *nicht wesentliche falsche Angaben in der Erklärung*
   - *nicht wesentliche Mängel in der Angemessenheit des IT-Systems*

b) *Empfehlungen***]**

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- sind die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- ist die Erklärung der gesetzlichen Vertreter zum IT-System in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- war das in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellte IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen und
  - zum zu prüfenden Zeitpunkt implementiert.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- sind die in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- ist die Erklärung der gesetzlichen Vertreter zum IT-System in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- war das in der Erklärung der gesetzlichen Vertreter zum IT-System dargestellte IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen und
  - zum zu prüfenden Zeitpunkt implementiert.]

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften IT-Systems

Die Erklärung der gesetzlichen Vertreter zum IT-System wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Angemessenheit des IT-Systems erstrecken sich auf den Zeitpunkt zum [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen des IT-Systems falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter]

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Das IT-System wurde durch die Gesellschaft abgegrenzt und beinhaltet daher möglicherweise nicht jeden Aspekt eines IT-Systems, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte. Folglich ist die Erklärung der gesetzlichen Vertreter zum IT-System möglicherweise für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an die Gesellschaft gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Erklärung der gesetzlichen Vertreter zum IT-System

Allgemeine Auftragsbedingungen

2. Direkte IT-Prüfung

2.1. Wirksamkeitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen *Wirtschaftsprüfers* über eine IT-Prüfung nach *IDW PS 860*

An die [Gesellschaft]

Wir haben eine Prüfung der Angemessenheit und Wirksamkeit des [Bezeichnung des IT-Systems] der [Gesellschaft] (im Folgenden die „Gesellschaft“) für den Zeitraum vom [Datum] bis [Datum] durchgeführt. Zur Darstellung des [Bezeichnung des IT-Systems] verweisen wir auf nachstehende Anlage 1.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der Gesellschaft sind für die von ihnen als notwendig erachteten Grundsätze, Verfahren und Maßnahmen zur Konzeption, Implementierung, Aufrechterhaltung, Überwachung und Dokumentation des IT-Systems verantwortlich, das in allen wesentlichen Belangen die untengenannten Kriterien zur Angemessenheit und Wirksamkeit erfüllt. Aufgrund bestehender inhärenter Grenzen von Systemen kann das IT-System diese Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Angemessenheit und Wirksamkeit des IT-Systems umfassen:

[Beschreibung der Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit über die Angemessenheit und Wirksamkeit des IT-Systems abzugeben.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* durchgeführt. Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob das IT-System in allen wesentlichen Belangen geeignet war, mit hinreichender Sicherheit die Kriterien zu erfüllen und ob das IT-System in allen wesentlichen Belangen während des Zeitraums vom [Datum] bis [Datum] mit hinreichender Sicherheit implementiert war und die Kriterien wirksam erfüllt hat.

Eine Prüfung gemäß *IDW PS 860* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil

abgeben zu können. Für die Beurteilung des IT-Systems ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel des IT-Systems mit hinreichender Sicherheit aufgedeckt werden. Die Prüfung des IT-Systems umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbau- und einer Funktionsprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung der Risiken des Vorhandenseins von wesentlichen Mängeln ein.

**[*Prüfungshandlungen, Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen*

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen/Empfehlungen gegeben, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen und Empfehlungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

a) *sonstige Feststellungen, u.a.*
   - ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des IT-Systems
   - nicht wesentliche Mängel in der Angemessenheit oder Wirksamkeit des IT-Systems

b) *Empfehlungen***]**

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- sind die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- war das IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert und
  - im geprüften Zeitraum wirksam.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- sind die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- war das IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert und
  - im geprüften Zeitraum wirksam.]

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften IT-Systems

Auch ein wirksames IT-System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit des IT-Systems erstrecken sich auf den Zeitraum vom [Datum] bis [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen des IT-Systems falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Das IT-System wurde durch die Gesellschaft abgegrenzt und beinhaltet daher möglicherweise nicht jeden Aspekt eines IT-Systems, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte. Folglich ist die beigefügte Darstellung des IT-Systems möglicherweise für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an die Gesellschaft gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Darstellung des IT-Systems

Allgemeine Auftragsbedingungen

2.2. Angemessenheitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine IT-Prüfung nach *IDW PS 860*

An die [Gesellschaft]

Wir haben eine Prüfung der Angemessenheit des [Bezeichnung des IT-Systems] der [Gesellschaft] (im Folgenden die „Gesellschaft“) zum [Datum] durchgeführt. Zur Darstellung des [Bezeichnung des IT-Systems] verweisen wir auf nachstehende Anlage 1.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der Gesellschaft sind für die von ihnen als notwendig erachteten Grundsätze, Verfahren und Maßnahmen zur Konzeption, Implementierung, Aufrechterhaltung, Überwachung und Dokumentation des IT-Systems verantwortlich, das in allen wesentlichen Belangen die untengenannten Kriterien zur Angemessenheit erfüllt. Aufgrund bestehender inhärenter Grenzen von Systemen kann das IT-System diese Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Angemessenheit des IT-Systems umfassen:

[Beschreibung der Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit über die Angemessenheit des IT-Systems abzugeben.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* durchgeführt. Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis*

(IDW QS 1) angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob das IT-System in allen wesentlichen Belangen geeignet war, mit hinreichender Sicherheit die Kriterien zu erfüllen und ob das IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit zum [Datum] implementiert war.

Eine Prüfung gemäß *IDW PS 860* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Für die Beurteilung des IT-Systems ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel des IT-Systems mit hinreichender Sicherheit aufgedeckt werden. Die Prüfung des IT-Systems umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbauprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung der Risiken des Vorhandenseins von wesentlichen Mängeln ein.

**[*Prüfungshandlungen, Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen*

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen/Empfehlungen gegeben, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen und Empfehlungen dargestellten Sachverhalte keine gesonderten Prüfungsurteile ab.

a) *sonstige Feststellungen, u.a.*
   - *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des IT-Systems*
   - *nicht wesentliche Mängel in der Angemessenheit des IT-Systems*

b) *Empfehlungen***]**

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- sind die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet,

- war das IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen und
  - zum zu prüfenden Zeitpunkt implementiert.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- sind die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- war das IT-System in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen und
  - zum zu prüfenden Zeitpunkt implementiert.]

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften IT-Systems

Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Angemessenheit des IT-Systems erstrecken sich auf den Zeitpunkt zum [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen des IT-Systems falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Das IT-System wurde durch die Gesellschaft abgegrenzt und beinhaltet daher möglicherweise nicht jeden Aspekt eines IT-Systems, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte. Folglich ist die beigefügte Darstellung des IT-Systems möglicherweise für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an die Gesellschaft gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Darstellung des IT-Systems

Allgemeine Auftragsbedingungen

IDW Prüfungshinweis: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)

(Stand: 19.06.2018)

IDW Prüfungshinweis: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)

Stand: 19.06.2018[1]

1. Vorbemerkungen

1 Der *IDW PS 860*[2] legt die Grundsätze fest, nach denen IT-Prüfungen außerhalb der Abschlussprüfung durchzuführen sind. Der vorliegende *IDW Prüfungshinweis* konkretisiert

[1] Verabschiedet vom Fachausschuss für Informationstechnologie (FAIT) am 17.05.2018. Billigende Kenntnisnahme durch den Hauptfachausschuss (HFA) am 19.06.2018.

[2] *IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* (Stand: 02.03.2018).

die für eine Prüfung nach der EU-Datenschutz-Grundverordnung (DS-GVO)[3] und dem BDSG[4] zugrunde zu legenden Kriterien. Er enthält geeignete Grundsätze, Verfahren und Maßnahmen zur Einhaltung der Kriterien und Beispiele für Prüfungshandlungen zur Beurteilung der Angemessenheit und Wirksamkeit der Grundsätze, Verfahren und Maßnahmen. Der in Anlage 1 enthaltene Anforderungskatalog ist eine vom IDW als sachgerecht angesehene Anwendung der Kriterien zur Einrichtung geeigneter Grundsätze, Verfahren und Maßnahmen, die bei einer Prüfung nach diesem *IDW Prüfungshinweis* beurteilt werden. Gleichwohl kann er auch als Grundlage für eine Würdigung der getroffenen Maßnahmen zur Vorbereitung einer datenschutzspezifischen Zertifizierung dienen.

2 Dieser *IDW Prüfungshinweis* gilt sowohl für die Auftragsart „Prüfung einer Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG“ als auch für die Auftragsart „direkte Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG“.

3 Dieser *IDW Prüfungshinweis* findet Anwendung bei der Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG im Zusammenhang mit der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen.

2. Ziel und Umfang der Prüfung

4 Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) hat mit dem *IDW PS 860* die Berufsauffassung dargelegt, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit die Prüfung von IT-Systemen außerhalb der Abschlussprüfung planen, durchführen sowie darüber Bericht erstatten.[5]

5 Eine nach *IDW PS 860* durchgeführte Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG kann als Angemessenheitsprüfung und ggf. zusätzlich als Wirksamkeitsprüfung erfolgen.

6 Bei der Auftragsart „Prüfung einer Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG“ ist Ziel der Angemessenheitsprüfung, dem Wirtschaftsprüfer ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob[6]

- die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Kriterien den in Abschn. 4 genannten Kriterien entsprechen und somit für den vorgesehenen Anwendungszweck geeignet sind,
- die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen frei von wesentlichen Fehlern ist,

---

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU Nr. L 119 v. 04.05.2016, S. 1.

[4] Artikel 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30.06.2017, BGBl I S. 2097.

[5] Vgl. *IDW PS 860*, Tz. 3.

[6] Vgl. *IDW PS 860*, Tz. 15.

- die in der Erklärung der gesetzlichen Vertreter dargestellten Grundsätze, Verfahren und Maßnahmen des Datenschutzes in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet sind, die in Abschn. 4 genannten Kriterien einzuhalten, und
  - zu dem zu prüfenden Zeitpunkt implementiert sind.

7 Ziel der Wirksamkeitsprüfung bei dieser Auftragsart ist – über die Angemessenheitsprüfung hinaus – zu beurteilen, ob die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Grundsätze, Verfahren und Maßnahmen des Datenschutzes in dem zu prüfenden Zeitraum wirksam gewesen sind.[7]

8 Bei der Auftragsart „direkte Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG“ ist Ziel der Angemessenheitsprüfung, dem Wirtschaftsprüfer ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob[8]

- die verwendeten Kriterien den in Abschn. 4 genannten Kriterien entsprechen und somit für den vorgesehenen Anwendungszweck geeignet sind,
- die vom Unternehmen angewandten Grundsätze, Verfahren und Maßnahmen des Datenschutzes in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet sind, die in Abschn. 4 genannten Kriterien einzuhalten, und
  - zu dem zu prüfenden Zeitpunkt implementiert sind.

9 Ziel der Wirksamkeitsprüfung bei dieser Auftragsart ist – über die Angemessenheitsprüfung hinaus – zu beurteilen, ob die vom Unternehmen angewandten Grundsätze, Verfahren und Maßnahmen des Datenschutzes in dem zu prüfenden Zeitraum wirksam gewesen sind.[9]

10 Die Prüfung wird für Zwecke des Unternehmens durchgeführt und der Prüfungsvermerk bzw. Prüfungsbericht ist zur Information des Unternehmens über das Ergebnis der Prüfung bestimmt. Darüber hinaus dient der Prüfungsvermerk bzw. Prüfungsbericht dem Unternehmen dazu, den vorgesehenen Nutzer über die Durchführung und die Ergebnisse der Prüfung zu informieren.

3. Gegenstand der Prüfung

11 Gegenstand der Auftragsart „Prüfung einer Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG“ nach diesem *IDW Prüfungshinweis* ist die Erklärung der gesetzlichen Vertreter des Unternehmens über die Einhaltung der in Abschn. 4 genannten Kriterien in Bezug auf die zu prüfenden Grundsätze, Verfahren und Maßnahmen des Datenschutzes.

12 Gegenstand der Auftragsart „direkte Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG“ nach diesem *IDW Prüfungshinweis* sind die in der Auftragsvereinbarung abgegrenzten Grundsätze, Verfahren und Maßnahmen des Datenschutzes.

---

[7] Vgl. *IDW PS 860*, Tz. 16.

[8] Vgl. *IDW PS 860*, Tz. 21.

[9] Vgl. *IDW PS 860*, Tz. 22.

13 Die Grundsätze, Verfahren und Maßnahmen des Datenschutzes umfassen die Grundsätze, Verfahren und Maßnahmen eines Unternehmens, die auf die Einhaltung der Anforderungen der DS-GVO und des BDSG bei der Verarbeitung personenbezogener Daten gerichtet sind. Das Zusammenwirken dieser Grundsätze, Verfahren und Maßnahmen wird durch das Datenschutzmanagement i.S. eines internen Kontrollsystems bestimmt, das vom Datenschutzumfeld sowie der Datenschutzaufbau- und Datenschutzablauforganisation abhängt. Die Ausgestaltung der Grundsätze, Verfahren und Maßnahmen des Datenschutzes erfolgt unternehmensindividuell in Abhängigkeit von Art und Umfang der Geschäftstätigkeit sowie der Art der verarbeiteten personenbezogenen Daten.

14 Personenbezogene Daten sind gemäß Artikel 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

15 Verarbeitung bezeichnet gemäß Artikel 4 Nr. 2 DS-GVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Reihe von solchen Vorgängen im Zusammenhang mit personenbezogenen Daten. Hierzu gehören gemäß Artikel 4 Nr. 2 DS-GVO z.B. das Erheben, die Speicherung, die Veränderung, die Verwendung, die Offenlegung durch Übermittlung, das Löschen und die Vernichtung der personenbezogenen Daten.

16 Die Prüfung i.S. dieses *IDW Prüfungshinweises* kann auf die Prüfung einzelner Verarbeitungstätigkeiten begrenzt werden. Die Verarbeitungstätigkeit betrifft die Tätigkeit der Verarbeitung i.S. von Artikel 4 Nr. 2 DS-GVO (vgl. Tz. 15) und bezieht sich auf konkrete Abwicklungen und Vorgänge, die personenbezogene Daten verwenden. Hierbei handelt es sich i.d.R. um (Teil-) Geschäftsprozesse, wie z.B. die Lohn- und Gehaltsabrechnung, das Bewerbermanagement oder das Customer-Relationship-Management. Die Prüfung i.S. dieses *IDW Prüfungshinweises* umfasst hierbei aber stets die Verarbeitung von sämtlichen personenbezogenen Daten innerhalb der Verarbeitungstätigkeit. Eine isolierte Prüfung der Verarbeitung einzelner Kategorien von personenbezogenen Daten liegt nicht im Anwendungsbereich dieses *IDW Prüfungshinweises*.

4. Kriterien

17 Die ab dem 25.05.2018 anzuwendende DS-GVO regelt die Verarbeitung personenbezogener Daten in den EU-Mitgliedstaaten. Mit dem am 25.05.2018 in Kraft getretenen reformierten BDSG werden die nationalen datenschutzrechtlichen Regelungen an die DS-GVO angepasst und die Richtlinie (EU) 2016/680[10] umgesetzt.

18 Der in Anlage 1 enthaltene Anforderungskatalog ist an den Anforderungen ausgerichtet, welche sich aus der DS-GVO und dem BDSG für nicht-öffentliche Stellen ergeben. Der Anforderungskatalog konkretisiert die Regelungen der DS-GVO und des BDSG im Zusammenhang mit der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen und stellt geeignete Kriterien für die Beurteilung der vom Unternehmen getroffenen datenschutzspezifischen Maßnahmen dar. Sind weitere gesetzliche oder sonstige regulatorische daten-

[10] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. EU Nr. L 119 v. 04.05.2016, S. 89.

schutzrechtliche Anforderungen einschlägig, richtet sich deren Anwendung nach der in der Auftragsvereinbarung getroffenen Abgrenzung. Der Anforderungskatalog ist in diesem Fall ggf. entsprechend zu erweitern.

5. Besonderheiten bei der Auftragsannahme

5.1. Prüfung einer Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG

19 Die angemessene Dokumentation der Grundsätze, Verfahren und Maßnahmen des Datenschutzes ist Voraussetzung für deren konsistente Anwendung und personenunabhängige Funktion im Zeitablauf. Die Verantwortung für diese Dokumentation liegt bei den gesetzlichen Vertretern des Unternehmens. Art und Umfang der Dokumentation hängen wesentlich von der Ausgestaltung der Grundsätze, Verfahren und Maßnahmen des Datenschutzes ab. Aus der Dokumentation muss auch die tatsächliche Durchführung der Grundsätze, Verfahren und Maßnahmen einschließlich der durchführenden Personen und des Zeitpunkts der Durchführung erkennbar sein.

20 Die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG hat eine Darstellung aller Grundsätze, Verfahren und Maßnahmen des Datenschutzes zu enthalten, die zur Einhaltung der in Abschn. 4 genannten Kriterien erforderlich sind. Hierbei ist von Bedeutung, dass sämtliche der in Abschn. 4 genannten Kriterien durch entsprechende Grundsätze, Verfahren und Maßnahmen abgedeckt werden.

5.2. Direkte Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG

21 Die angemessene Dokumentation der Grundsätze, Verfahren und Maßnahmen des Datenschutzes ist Voraussetzung für deren konsistente Anwendung und personenunabhängige Funktion im Zeitablauf. Die Verantwortung für diese Dokumentation liegt bei den gesetzlichen Vertretern des Unternehmens. Art und Umfang der Dokumentation hängen wesentlich von der Ausgestaltung der Grundsätze, Verfahren und Maßnahmen des Datenschutzes und dem rechtlichen und wirtschaftlichen Umfeld des Unternehmens ab.

22 Die Dokumentation dient dem Wirtschaftsprüfer als Grundlage für die Planung und Durchführung seiner Prüfungshandlungen. Sie muss so beschaffen sein, dass sie die Grundsätze, Verfahren und Maßnahmen des Datenschutzes klar, verständlich, vollständig und aktuell darstellt. Aus der Dokumentation muss auch die tatsächliche Durchführung der Grundsätze, Verfahren und Maßnahmen einschließlich der durchführenden Personen und des Zeitpunkts der Durchführung erkennbar sein.

6. Besonderheiten bei der Prüfungsdurchführung

23 Bei einer Prüfung nach der DS-GVO und dem BDSG sind die in Abschn. 4 genannten Kriterien vollständig zu berücksichtigen. Die von den gesetzlichen Vertretern des Unternehmens eingerichteten Grundsätze, Verfahren und Maßnahmen des Datenschutzes sind nach

diesen Kriterien hinsichtlich ihrer Angemessenheit und – sofern einschlägig – Wirksamkeit zu beurteilen.

24 Geeignete Grundsätze, Verfahren und Maßnahmen zur Einhaltung der Kriterien sowie Hinweise zur Durchführung der Prüfung können der Anlage 1 entnommen werden. Diese gelten sowohl für die Auftragsart „Prüfung einer Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG“ als auch für die Auftragsart „direkte Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG“.

25 Die in der Anlage 1 aufgeführten Grundsätze, Verfahren und Maßnahmen sind als Mindestanforderungen und nicht als abschließende Aufzählung zu verstehen, da ihre Festlegung in der Verantwortung der gesetzlichen Vertreter des Unternehmens liegt.

26 Der *IDW PS 860* legt die Grundsätze für die Planung und Durchführung von Prüfungshandlungen für eine Prüfung nach der DS-GVO und dem BDSG fest. Die in der Anlage 1 aufgeführten Prüfungshandlungen sind ergänzend zu den zur Erfüllung der Anforderungen des *IDW PS 860* notwendigen Prüfungshandlungen als Beispiele und nicht als abschließende Aufzählung zu verstehen, da die Festlegung der durchzuführenden Prüfungshandlungen in der Eigenverantwortlichkeit des Wirtschaftsprüfers liegt.

27 Weitere beispielhafte Prüfungshandlungen ergänzend zu den in der Anlage 1 aufgeführten beispielhaften Prüfungshandlungen sind jeweils auch

- zur Prüfung der Angemessenheit der Grundsätze, Verfahren und Maßnahmen die Durchsicht von Unterlagen und Dokumentationen, wie bspw. Richtlinien, Arbeitsanweisungen, Verfahrensanweisungen, Prozessdokumentationen, Verzeichnissen oder Schulungskonzepten, in denen zentrale Vorgaben zur Durchführung, zum Ablauf und zu den Verantwortlichkeiten schriftlich geregelt sind,
- zur Prüfung der Angemessenheit und Wirksamkeit der Grundsätze, Verfahren und Maßnahmen die Beurteilung der Unterlagen und Dokumentationen im Hinblick auf ihre Vollständigkeit und regelmäßige Aktualisierung.

7. Besonderheiten bei der Berichterstattung des Wirtschaftsprüfers

28 Der Wirtschaftsprüfer verfasst eine schriftliche Berichterstattung als Prüfungsbericht. Der Prüfungsbericht beinhaltet eine zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und ggf. Funktionsprüfungen und der weiteren Prüfungshandlungen sowie Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen. Der Prüfungsbericht muss für die vorgesehenen Nutzer zugänglich sein.

29 In einem Prüfungsvermerk hat der Wirtschaftsprüfer auf den Prüfungsbericht hinzuweisen.

Anlagen

Anlage 1: Darstellung der Grundsätze, Verfahren und Maßnahmen zur Einhaltung der in Abschnitt 4 genannten Kriterien sowie beispielhafte Prüfungshandlungen

Anforderung: Das Unternehmen stellt mit der Einrichtung eines geeigneten Umfelds und einer geeigneten Aufbau- und Ablauforganisation mit hinreichender Sicherheit die Einhaltung der einschlägigen datenschutzrechtlichen Vorgaben sicher. (Artikel 5 Abs. 1 und 2, Artikel 24 Abs. 1 DS-GVO, Artikel 29 DS-GVO).

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
1	Es wurden Datenschutzziele festgelegt, die sich nachvollziehbar aus der Unternehmensstrategie ableiten, besondere datenschutzrechtliche Faktoren, die sich aus dem Geschäftsmodell ergeben, berücksichtigen und die dokumentiert sind. Der angestrebte Zielzustand/Reifegrad der Datenschutzmaßnahmen wurde bestimmt und dokumentiert.	Prüfung der Angemessenheit: ● Durchsicht relevanter Dokumente zu den Datenschutzzielen ● Prüfung der Datenschutzziele auf Ausrichtung an der Unternehmensstrategie. Die Unternehmensstrategie und die Datenschutzziele sollten sich ergänzen und nicht widersprechen. Prüfung der Wirksamkeit: ● Einsichtnahme in Berichte/Auswertungen bezogen auf die Zielerreichung/-abweichung und die regelmäßige Überprüfung und Anpassung der Datenschutzziele
2	Es wurden Maßnahmen ergriffen und dokumentiert, um eine nachhaltige Datenschutz-Kultur im Unternehmen zu etablieren. Diese Maßnahmen ermöglichen, dass sich Mitarbeiter der Relevanz des Datenschutzes nachhaltig bewusst sind.	Prüfung der Angemessenheit: ● Durchsicht des Awareness Plans und der Verpflichtung der Mitarbeiter zur Vertraulichkeit und Prüfung dieser auf Aktualität und Ableitung aus den Datenschutzzielen Prüfung der Wirksamkeit: ● Befragung des Managements und Einsichtnahme in Protokolle von Sitzungen des Managements, um die Grundeinstellung („tone from the top“) zum Datenschutz und die Kommunikation der Bedeutung von datenschutzkonformem Verhalten im Unternehmen nachzuvollziehen. ● Befragung von Mitarbeitern, um festzustellen, ob diesen die Relevanz des Datenschutzes bewusst ist

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
3	Das in Bezug auf den Datenschutz für das Unternehmen relevante rechtliche und regulatorische Umfeld wurde bei der Ausgestaltung der Aufbau- und Ablauforganisation sowie bei der Festlegung der Datenschutzmaßnahmen berücksichtigt. Es erfolgt eine anlassbezogene sowie regelmäßige Prüfung im Hinblick auf Änderungen des rechtlichen und regulatorischen Umfelds sowie bei Bedarf die Ableitung von Anpassungsmaßnahmen.	Prüfung der Angemessenheit: ● Durchsicht der Dokumentation bezogen auf das rechtliche und regulatorische Umfeld ● Befragung des Managements sowie des Datenschutzbeauftragten zur Berücksichtigung des rechtlichen und regulatorischen Umfelds Prüfung der Wirksamkeit: ● Einsichtnahme in die Dokumentation über die Durchführung der Prüfung von Änderungen des rechtlichen und regulatorischen Umfelds sowie der daraus abgeleiteten Anpassungsmaßnahmen
4	Es ist ein Rahmenwerk (Dokumentenpyramide) vorhanden, das den Umgang mit dem Datenschutz detailliert regelt und mindestens folgende Bereiche umfasst: ● Datenschutzorganisation ● Stellung und Aufgaben des Datenschutzbeauftragten ● Datenschutzrechtliches Risikomanagement und Datenschutzfolgenabschätzung ● Zulässigkeit der Verarbeitung personenbezogener Daten ● Datenschutz durch Technikgestaltung ● Verzeichnis von Verarbeitungstätigkeiten ● Technisch organisatorische Maßnahmen ● Löschung von Daten ● Betroffenenrechte ● Datenschutzverletzungen und Meldung ● Auftragsverarbeitung und Zulässigkeit der Übermittlung von Daten ● Übermittlung von Daten in Drittländer ● Sensibilisierung und Kommunikation ● Nachweis- und Rechenschaftspflichten Die im Rahmenwerk enthaltenen Regelungen sind durch ein Dokumenten-Management nachvollziehbar dokumentiert und allen Mitarbeitern zugänglich.	Prüfung der Angemessenheit: ● Durchsicht der Inhalte von Richtlinien und Anweisungen zum Datenschutz ● Prüfung der Zugänglichkeit der Richtlinien und Anweisungen für Mitarbeiter durch Beobachtung, Befragung oder Nachvollzug Prüfung der Wirksamkeit: ● Prüfung auf vollständige Berücksichtigung der Kriterien ● Prüfung der Aktualität des Rahmenwerks ● Einsichtnahme in Freigaben des Managements zur Inkraftsetzung der Richtlinien und Anweisungen ● Prüfung auf Vollständigkeit der Freigaben in Bezug auf das Rahmenwerk

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	Folgende Aspekte werden bei der Erstellung des Rahmenwerks berücksichtigt: ● Es sind Richtlinien und Anweisungen zum Datenschutz vorhanden, die die Grundsätze gemäß Artikel 5 DS-GVO berücksichtigen und den Anforderungen der Kriterien gemäß Abschn. 4 dieses IDW Prüfungshinweises entsprechen. ● Die Richtlinien und Anweisungen wurden vom Management freigegeben. ● Die Richtlinien und Anweisungen wurden kommuniziert und können von den Mitarbeitern jederzeit eingesehen werden. ● Abhängigkeiten zu weiteren Policies, Richtlinien und Anweisungen im Unternehmen wurden betrachtet und dokumentiert. ● Die Richtlinien und Anweisungen werden regelmäßig aktualisiert.	
5	Die Regelungen des Rahmenwerks zu den Nachweis- und Rechenschaftspflichten umfassen neben allgemeinen Vorgaben zur nachvollziehbaren Dokumentation der Einhaltung der datenschutzrechtlichen Anforderungen sowie Vorgaben zur Aufbewahrung der Dokumentation auch explizite Anforderungen an die Dokumentation von Einzelsachverhalten, z.B.: ● Dokumentation von Datenschutzverletzungen gemäß Artikel 33 Abs. 5 DS-GVO ● gesonderte oder allgemeine schriftliche Genehmigung bei Unterauftragsverhältnissen von Auftragsverarbeitern gemäß Artikel 28 Abs. 2 DS-GVO ● Nachweis über die Einhaltung der Pflichten als Auftragsverarbeiter (Artikel 28 Abs. 3 DS-GVO) ● Nachweis für unbegründete Anträge (Artikel 12 Abs. 5 DS-GVO) bzw. über eine Auskunftsverweigerung gemäß § 34 Abs. 2 BDSG ● Nachweispflicht über erteilte Einwilligungen in die Verarbeitung gemäß Arti-	Prüfung der Angemessenheit: ● Durchsicht der zentralen Vorgaben bezogen auf Vollständigkeit und Aktualität

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	kel 7 Abs. 1 DS-GVO ● unterlassene Informationen an Betroffene gemäß § 32 Abs. 2 bzw. § 33 Abs. 2 BDSG ● Unterrichtung des Betroffenen gemäß § 31 Abs. 1 Nr. 4 BDSG bei Anwendung des Scoring-Verfahrens.	
6	Es existiert eine Datenschutzorganisation mit einer klaren Festlegung von Rollen und Verantwortlichkeiten. Die Zusammenarbeit der verschiedenen Rollen innerhalb der Datenschutzorganisation sowohl untereinander als auch mit der Geschäftsführung (Verantwortlicher) ist festgelegt. Die definierte Datenschutzorganisation ist durch die Geschäftsführung abgenommen, dokumentiert und an alle relevanten Mitarbeiter kommuniziert worden.	Prüfung der Angemessenheit: ● Durchsicht der Dokumentation der Aufbau- und Ablauforganisation (z.B. Ressourcenplanung, Rollen- und Stellenbeschreibungen, Liste der Datenschutzkoordinatoren, Kontaktdaten des Datenschutzbeauftragten), insb. bezogen auf folgende Aspekte: - Definition von Rollen und Verantwortlichkeiten - Zuweisung angemessener Ressourcen - Benennung von Datenschutzkoordinatoren in den Fachbereichen in einem angemessenen Umfang im Verhältnis zur Organisationsgröße - klare Definition der Zusammenarbeit zwischen dem Datenschutzbeauftragten und den Datenschutzkoordinatoren/Fachbereichen (einschließlich Festlegung der Berichtswege) - Definition von Schnittstellen zu relevanten internen Stakeholdern, wie z.B. zur Compliance Organisation Prüfung der Wirksamkeit: ● Prüfung der Aktualität der Dokumentation der Aufbau- und Ablauforganisation ● Einsichtnahme in die Dokumentation von regelmäßigen Abstimmungen zwischen dem Datenschutzbeauftragten und den Datenschutzkoordinatoren/Fachbereichen
7	Sofern das Unternehmen mit einem anderen Unternehmen für bestimmte Verarbeitungen gemeinsam die Zwecke und die	Prüfung der Angemessenheit: ● Durchsicht der Vereinbarung und Prü-

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	Mittel zur Verarbeitung festlegt (gemeinsam Verantwortliche gemäß Artikel 26 DS-GVO), wird eine Vereinbarung mit folgenden Inhalten getroffen: ● Rollen und Verantwortlichkeiten zur Erfüllung der Vorgaben der Kriterien ● Festlegung, welches Unternehmen den Informationspflichten gemäß Artikel 13 und 14 DS-GVO nachkommt ● Berücksichtigung der tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber der betroffenen Person Wesentliche Inhalte der Vereinbarung werden der betroffenen Person zur Verfügung gestellt.	fung auf Vollständigkeit und Aktualität Prüfung der Wirksamkeit: ● Prüfung auf Einhaltung der abgestimmten Aufgabenverteilung ● Prüfung der Erfüllung der Informationspflichten nach Artikel 13 und 14 DS-GVO, die dem Unternehmen zugewiesen wurden ● Prüfung der Zurverfügungstellung der wesentlichen Inhalte der Vereinbarung gegenüber der betroffenen Person
8	Es ist ein Schulungskonzept vorhanden, welches die Kommunikation der datenschutzrelevanten Grundsätze, Verfahren und Maßnahmen an die beteiligten Mitarbeiter sicherstellt und dafür sorgt, dass die Mitarbeiter ihre Rolle und Bedeutung im jeweiligen Prozess und deren Abhängigkeiten von vor- und nachgelagerten Prozessschritten bzw. Kontrollen kennen. (Artikel 39 Abs. 1 Buchst. a) DS-GVO)	Prüfung der Angemessenheit: ● Durchsicht der Schulungsunterlagen
9	Das Unternehmen führt geeignete Nachweise zu regelmäßig durchgeführten Schulungen, zur Teilnahme an den Schulungen und zur Überprüfung des Wissensstands der Mitarbeiter. Die beteiligten Mitarbeiter werden zur Teilnahme an Datenschutzschulungen vertraglich verpflichtet. Die vollständige Teilnahme wird nachgehalten. Die Informationsmaterialien werden den Schulungsteilnehmern zur dauerhaften Einsicht zur Verfügung gestellt. (Artikel 39 Abs. 1 Buchst. b) DS-GVO).	Prüfung der Angemessenheit: ● Durchsicht der entsprechenden vertraglichen Regelungen (z. B. Betriebsvereinbarungen oder Arbeitsverträge) bezogen auf die Verpflichtung zur Teilnahme an Datenschutzschulungen Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über die Teilnahme an Schulungen ● Einsichtnahme in Nachweise über die Überprüfung des Wissensstands der Mitarbeiter („Erfolgskontrolle“)
10	Das Unternehmen hat einen Überarbeitungsprozess implementiert, der sicherstellt, dass die Schulungsinhalte regelmäßig auf Aktualität und Angemessenheit	Prüfung der Angemessenheit: ● Durchsicht der Prozessvorgaben Prüfung der Wirksamkeit: ● Einsichtnahme in die Dokumentation

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	überprüft und bei Bedarf korrigiert werden.	über die regelmäßige Aktualisierung der Schulungsunterlagen.
11	Die Interne Revision überwacht als prozessunabhängige Institution die Einhaltung der datenschutzrechtlichen Grundsätze, Verfahren und Maßnahmen und entwickelt bei Bedarf Verbesserungsvorschläge. Hierbei ist die angemessene Kommunikation mit dem Datenschutzbeauftragten sichergestellt.	Prüfung der Angemessenheit: ● Befragung von Mitarbeitern der Internen Revision und Durchsicht der Prozessvorgaben Prüfung der Wirksamkeit: ● Einsichtnahme in Dokumentationen über durchgeführte Prüfungen der Internen Revision

Anforderung: Die eingerichteten Verfahren und Kontrollen stellen mit hinreichender Sicherheit sicher, dass der Datenschutzbeauftragte die Anforderungen an seine Tätigkeiten nachweisbar erfüllt.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
12	Die Tätigkeiten des Datenschutzbeauftragten sind schriftlich in einer Stellen- bzw. Aufgabenbeschreibung bzw. bei einem externen Datenschutzbeauftragten in dessen Beauftragung festgehalten. (Artikel 39 Abs. 1, Artikel 38 Abs. 6, Artikel 5 Abs. 2 DS-GVO) Soweit ein Benennungsschreiben bzw. eine Bestellungsurkunde vorliegt, sind die aufgeführten Aufgaben und Tätigkeiten konsistent zur Stellen- bzw. Aufgabenbeschreibung. Die Stellen- bzw. Aufgabenbeschreibung wird mindestens jährlich auf ihre Aktualität überprüft und vom Management bestätigt. Die Stellen- bzw. Aufgabenbeschreibung bzw. die Beauftragung berücksichtigen die Verpflichtung zur Verschwiegenheit gegenüber Dritten und unternehmensintern gem. Artikel 38 Abs. 5 DS-GVO i.V.m. § 6 Abs. 5 Satz 2 BDSG sowie die folgenden Anforderungen gemäß Artikel 39 Abs. 1 und 2 DS-GVO und beschreibt angemessen die jeweiligen Ausprägungen der Aktivitäten:	Prüfung der Angemessenheit: ● Durchsicht der Stellen- bzw. Aufgabenbeschreibung und Beurteilung hinsichtlich Vollständigkeit und Aktualität Prüfung der Wirksamkeit: ● Abgleich der Stellen- bzw. Aufgabenbeschreibung mit der Unternehmensorganisation sowie dem Benennungsschreiben bzw. der Bestellungsurkunde und den Nachweisen über die Tätigkeit des Datenschutzbeauftragten

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	● Unterrichtung und Beratung des Unternehmens (sowie ggf. der Auftragsverarbeiter) und der Beschäftigten ● Überwachung der Einhaltung der Vorgaben der DS-GVO sowie anderer relevanter Datenschutzvorschriften und Strategien des Unternehmens ● Beratung im Rahmen der Datenschutz-Folgenabschätzung (auf Anfrage) ● Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für diese ● Beratung und Stellungnahmen gegenüber betroffenen Personen ● Vorgaben zur frühzeitigen Einbindung des Datenschutzbeauftragten in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen ● Durchführung einer eigenen Risikoeinschätzung durch den Datenschutzbeauftragten (auch „Gefährdungsanalyse“ oder „Abwägungsentscheidung“) gemäß Artikel 39 Abs. 2 DS-GVO zur Berücksichtigung des mit den Verarbeitungsvorgängen verbundenen Risikos bei der Erfüllung seiner Aufgaben.	
13	Soweit dem Datenschutzbeauftragten neben seinen gesetzlichen Aufgaben weitere Aufgaben gemäß Artikel 38 Abs. 6 DS-GVO in Bezug auf die Datenschutzorganisation (z.B. Führung des Verzeichnisses von Verarbeitungstätigkeiten, Durchführung von Schulungen, Koordination von Lösch-/Auskunftsersuchen bzw. von Meldeprozessen) übertragen werden, sind auch diese in entsprechenden Stellen-/Aufgabenbeschreibungen bzw. Arbeitsanweisungen festgehalten. Es wird seitens des Unternehmens durch entsprechende Maßnahmen sichergestellt, dass die Unabhängigkeit des Datenschutzbeauftragten aufgrund seiner erweiterten Aufgaben nicht beeinträchtigt wird. Dies kann z.B. durch die externe Überwachung der erweiterten Aufgaben des Datenschutzbeauftragten erfolgen.	Prüfung der Angemessenheit: ● Durchsicht der Stellen-/Aufgabenbeschreibungen bzw. Arbeitsanweisungen und Beurteilung in Bezug auf mögliche Interessenkonflikte. Prüfung der Wirksamkeit: ● Abgleich der Stellen-/Aufgabenbeschreibung bzw. Arbeitsanweisungen mit der Unternehmensorganisation und den Nachweisen über die Tätigkeit des Datenschutzbeauftragten. ● Durchsicht der Ergebnisse einer externen Überwachung der erweiterten Aufgaben des Datenschutzbeauftragten

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
14	Die Verantwortlichkeiten des Datenschutzbeauftragten sind gemäß Artikel 38 DS-GVO klar geregelt. Dies betrifft insb. auch Schnittstellen bzw. die Abgrenzung zur Rechtsabteilung und zum Management bzw. zu – soweit vorhanden – dezentralen Datenschutzkoordinatoren oder anderen Datenschutzbeauftragten in einem Konzern. Dem Datenschutzbeauftragten ist der Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen gewährt. Es ist eindeutig festgelegt, dass die Verantwortung für die Einhaltung der datenschutzrechtlichen Anforderungen nicht beim Datenschutzbeauftragten liegt.	Prüfung der Angemessenheit: ● Durchsicht der Dokumentation der Verantwortlichkeiten, Organigramme, Stellenbeschreibungen Prüfung der Wirksamkeit: ● Abgleich mit der tatsächlichen Organisationsstruktur des Unternehmens
15	Es ist schriftlich festgehalten, dass der Datenschutzbeauftragte gemäß Artikel 38 Abs. 3 DS-GVO bei der konkreten Ausführung seiner Tätigkeit weisungsfrei agieren kann.	Prüfung der Angemessenheit: ● Durchsicht der Dokumentation. Prüfung der Wirksamkeit: ● Befragung des Datenschutzbeauftragten und ggf. des Managements und Einsicht in Nachweise über Berichtslinien
16	Der Datenschutzbeauftragte ist gemäß Artikel 38 Abs. 5 DS-GVO i.V.m. § 6 Abs. 5 Satz 2 BDSG gesetzlich zur Verschwiegenheit verpflichtet. Die Mitarbeiter des Datenschutzbeauftragten sind schriftlich zur Verschwiegenheit verpflichtet worden.	Prüfung der Angemessenheit und Wirksamkeit: ● Einsichtnahme in die Verpflichtungserklärung der Mitarbeiter des Datenschutzbeauftragten
17	Die Erreichbarkeit des Datenschutzbeauftragten als unternehmensinterner Ansprechpartner gemäß Artikel 37 Abs. 2 DS-GVO sowie als Ansprechpartner gegenüber Betroffenen gemäß Artikel 38 Abs. 4 DS-GVO ist gewährleistet. Die Erreichbarkeit berücksichtigt nicht nur eine Stellvertreterregelung, sondern auch die Frage, inwieweit der Datenschutzbeauftragte (ggf. unter Hinzuziehung von Hilfspersonen) die relevanten Sprachen für die Korrespondenz mit der Aufsicht oder betroffenen Personen abdecken kann.	Prüfung der Angemessenheit: ● Befragung des Datenschutzbeauftragten und Durchsicht der Vorgaben Prüfung der Wirksamkeit: ● Durchführung eines Funktionstests der Erreichbarkeit ● Einsichtnahme in Nachweise über die Kommunikation des Datenschutzbeauftragten mit Mitarbeitern des Unternehmens bzw. Betroffenen

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
18	Die Kontaktdaten des Datenschutzbeauftragten sind gemäß Artikel 37 Abs. 7 DS-GVO im Unternehmen bekannt gemacht worden bzw. für Betroffene veröffentlicht (z.B. auf der Homepage des Unternehmens). Die zuständige Aufsichtsbehörde wurde identifiziert und dieser wurden die Kontaktdaten des Datenschutzbeauftragten gemeldet.	Prüfung der Angemessenheit und Wirksamkeit: ● Einsichtnahme in die Kommunikation im Intranet bzw. auf der Homepage des Unternehmens Prüfung der Wirksamkeit: ● Einsichtnahme in die Meldung der Kontaktdaten an die zuständige Aufsichtsbehörde (i.d.R. am Hauptsitz des Unternehmens)
19	Zur Erfüllung der Rechenschaftspflicht gemäß Artikel 5 Abs. 2 DS-GVO dokumentiert der Datenschutzbeauftragte wesentliche Tätigkeiten seiner Person bzw. seiner Mitarbeiter, z.B. in einem zentralen Dokumentations-Tool. Die Dokumentation umfasst u.a. ● die erfolgte Unterrichtung und Beratung des Unternehmens (sowie ggf. der Auftragsverarbeiter) und der Beschäftigten ● die Tätigkeit zur Überwachung der Einhaltung der Vorgaben der DS-GVO sowie anderer relevanter Datenschutzvorschriften und Strategien des Unternehmens ● den Umfang und das Ergebnis der Beratung im Rahmen der Datenschutz-Folgenabschätzung ● die Zusammenarbeit mit der Aufsichtsbehörde ● die Beratung und Stellungnahmen gegenüber betroffenen Personen oder unternehmensinternen Bereichen ● das Ergebnis der eigenen Risikoeinschätzung des Datenschutzbeauftragten (auch „Gefährdungsanalyse“ oder „Abwägungsentscheidung“) gemäß Artikel 39 Abs. 2 DS-GVO zur Berücksichtigung des mit den Verarbeitungsvorgängen verbundenen Risikos bei der Erfüllung seiner Aufgaben. Soweit dem Datenschutzbeauftragten weitere Aufgaben i.S. der DS-GVO übertragen wurden, ist auch deren Durchführung entsprechend zu dokumentieren.	Prüfung der Angemessenheit: ● Befragung des Datenschutzbeauftragten und Durchsicht der Dokumentationsvorgaben Prüfung der Wirksamkeit: ● Prüfung der Dokumentation auf Einhaltung der Dokumentationsvorgaben ● Abgleich der Risikoeinschätzung des Datenschutzbeauftragten mit Ergebnissen der Datenschutz-Folgenabschätzung oder Angaben im Verzeichnis von Verarbeitungstätigkeiten

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
20	Die operative Ausgestaltung der Aufgaben des Datenschutzbeauftragten ist gemäß Artikel 39 Abs. 2 DS-GVO grundsätzlich risikoorientiert geplant. Hierfür hat der Datenschutzbeauftragte – ggf. zusammen mit dem Unternehmen und auf Basis des Verzeichnisses von Verarbeitungstätigkeiten – eine Risikoeinschätzung („Gefährdungsanalyse“ oder „Abwägungsentscheidung“) durchgeführt und das Ergebnis nachvollziehbar dokumentiert. Die Risikoeinschätzung ist regelmäßig bzw. anlassbezogen vom Datenschutzbeauftragten auf ihre Angemessenheit zu überprüfen und ggf. anzupassen.	Prüfung der Angemessenheit: ● Durchsicht der entsprechenden Vorgaben für den Datenschutzbeauftragten Prüfung der Wirksamkeit: ● Nachvollzug der Risikoeinschätzung des Datenschutzbeauftragten ● Abgleich der Risikoeinschätzung des Datenschutzbeauftragten mit dem vorliegenden Verzeichnis von Verarbeitungstätigkeiten ● Prüfung der regelmäßigen Aktualisierung auf Basis der Freigabebestätigung
21	Es erfolgt eine regelmäßige Kommunikation des Datenschutzbeauftragten mit dem Management bzw. der Geschäftsführung. Die Berichtswege, der Rhythmus und die Formate, die Inhalte und der Adressatenkreis der Kommunikation sind klar geregelt. Die Kommunikation umfasst auch die Berichterstattung des Datenschutzbeauftragten über seine Tätigkeit. Hierbei ist gemäß Artikel 38 Abs. 3 DS-GVO die unmittelbare Berichterstattung an die höchste Managementebene des Unternehmens sichergestellt.	Prüfung der Angemessenheit: ● Durchsicht der Kommunikationsplanung, der Stellenbeschreibungen und des Organigramms Prüfung der Wirksamkeit ● Einsichtnahme in die erstellten Berichte und Stellungnahmen
22	Für die Tätigkeit des Datenschutzbeauftragten und seiner Mitarbeiter ist eine nachvollziehbare und angemessene Budgetierung erfolgt. Dem Datenschutzbeauftragten werden gemäß Artikel 38 Abs. 2 DS-GVO die für die Erfüllung seiner Aufgaben erforderlichen Ressourcen bzw. die erforderliche Ausstattung zur Verfügung gestellt. Das Budget ermöglicht die Hinzuziehung externer Unterstützung bzw. Beratung oder die Beschaffung von spezifischen Hilfsmitteln.	Prüfung der Angemessenheit: ● Durchsicht der Budget- und Ressourcenplanung Prüfung der Wirksamkeit: ● Abgleich der Budget- und Ressourcenplanung mit vorhandenen Ressourcen und Ausstattungen ● Beurteilung, ob Anhaltspunkte für nicht ausreichende Budgets und Ressourcen vorliegen, z.B. lange Bearbeitungszeiten bei Anfragen, Verstöße gegen Datenschutzvorschriften, mangelnde fachliche Qualifikation des Datenschutzbeauftragten

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
23	Der Datenschutzbeauftragte verfügt gemäß Artikel 37 Abs. 5 DS-GVO über eine ausreichende Qualifikation bzw. Fachkenntnis. Es sind gemäß Artikel 38 Abs. 2 DS-GVO regelmäßige Schulungs- und Fortbildungsmaßnahmen für den Datenschutzbeauftragten und seine Mitarbeiter vorgesehen. Die jeweilige Teilnahme wird dokumentiert. Notwendige Fachliteratur oder externe Beratung können bei Bedarf in Anspruch genommen werden.	Beurteilung der Angemessenheit und Wirksamkeit: ● Befragung des Datenschutzbeauftragten ● Einsichtnahme in Zertifikate des Datenschutzbeauftragten bzw. Nachweise über die Teilnahme an Schulungen ● Einsichtnahme in den Prozess zur Auswahl des Datenschutzbeauftragten und Beurteilung der an den Datenschutzbeauftragten gestellten Qualifikationsanforderungen sowie Beurteilung, ob der Datenschutzbeauftragte diese Anforderungen erfüllt
24	Der Datenschutzbeauftragte ist gemäß Artikel 38 Abs. 1 DS-GVO so in Entscheidungs- und Informationsprozesse eingebunden, dass er ordnungsgemäß und frühzeitig bei allen Fragen in Bezug auf den Umgang und den Schutz personenbezogener Daten involviert wird. Der Datenschutzbeauftragte ist in die Qualitätssicherung von Arbeitsanweisungen und Arbeitshilfen bzw. Templates mit Bezug zum Datenschutz eingebunden.	Beurteilung der Angemessenheit: ● Durchsicht der Richtlinien und der Dokumentation von Informations- und Kommunikationsprozessen bezogen auf die Einbindung des Datenschutzbeauftragten, bspw. bei - Projektanträgen oder Einsicht in eine Projektdatenbank, - Incident- bzw. Change-Prozessen, - dem regelmäßigen Austausch zwischen Geschäftsführung, Interner Revision oder dem IT-Sicherheitsbeauftragten, etc. - dem Austausch mit dezentralen Datenschutzkoordinatoren (soweit vorhanden) Prüfung der Wirksamkeit: ● Befragung des Datenschutzbeauftragten und von Mitarbeitern der IT-Abteilung ● Einsichtnahme in Anfragen, Projektanträge, Protokolle, Berichte etc.
25	Der Datenschutzbeauftragte unterrichtet und berät gemäß Artikel 39 Abs. 1 DS-GVO das Unternehmen (i.d.R. das Management) und die Beschäftigten bezogen auf datenschutzrechtliche Anforderungen.	Prüfung der Angemessenheit: ● Durchsicht der Stellen- bzw. Aufgabenbeschreibung des Datenschutzbeauftragten. Diesbezügliche Vorgaben berücksichtigen z.B. - die regelmäßige Information des Managements sowie der Beschäf-

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
		tigten im Hinblick auf einschlägige datenschutzrechtliche Anforderungen sowie aktuelle Entwicklungen, - die Durchführung von ad hoc Beratungen auf Anfrage der Fachbereiche oder des Managements, - die Qualitätssicherung des Schulungsmaterials Prüfung der Wirksamkeit: ● Einsichtnahme in die Nachweise über die Tätigkeit des Datenschutzbeauftragten, wie bspw. einen Tätigkeitsbericht
26	Die Prozesse zur Datenschutz-Folgenabschätzung stellen gemäß Artikel 39 Abs. 1 Buchst. c) DS-GVO die Konsultation des Datenschutzbeauftragten sicher. Die Beratung zur Datenschutz-Folgenabschätzung erfolgt auf Anfrage des verantwortlichen Fachbereichs und bedarf insb. einer abgestimmten Methodik sowie einer klaren Aufgabenverteilung. Die Beratungsleistung wird vom Datenschutzbeauftragten dokumentiert.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben/Prozessdokumentation Prüfung der Wirksamkeit: ● Nachvollzug ausgewählter Datenschutz-Folgenabschätzungen bezogen auf die Einbindung des Datenschutzbeauftragten, bspw. im Hinblick auf folgende Fragestellungen: - Ist das methodische Vorgehen korrekt? - Sind die ergriffenen Schutzmaßnahmen sachgerecht? - Welche Gesamtwürdigung ergibt sich? ● Einsichtnahme in den Tätigkeitsbericht bzw. andere Nachweise über die Tätigkeit des Datenschutzbeauftragten
27	Für die allgemeine Zusammenarbeit mit der Aufsichtsbehörde und die Wahrnehmung der Funktion als Anlaufstelle für die Aufsichtsbehörde sind Verhaltensregeln sowie die Verantwortlichkeiten und Kontaktpersonen definiert. Diese werden regelmäßig aktualisiert. Zu den Aufgaben des Datenschutzbeauftragten gemäß Artikel 39 Abs. 1 DS-GVO gehören in diesem Zusammenhang: ● Kommunikation mit der Aufsichtsbehörde (Bearbeitung von Anfragen der Aufsichtsbehörde sowie Zugehen auf die	Beurteilung der Angemessenheit: ● Durchsicht der Verhaltensregeln und Festlegungen von Verantwortlichkeiten und Kontaktpersonen Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise zur Zusammenarbeit mit der Aufsichtsbehörde bezogen auf die Einhaltung der Vorgaben ● Prüfung auf regelmäßige Aktualisierung der Kontaktliste

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	Aufsichtsbehörde bei datenschutzrechtlichen Fragestellungen oder Beratungsanliegen) ● Konsultation im Rahmen der Datenschutz-Folgenabschätzung ● Anlaufstelle für die Aufsichtsbehörde (u.a. in Bezug auf Rückfragen aus der Konsultation, Anfragen zum Verzeichnis von Verarbeitungstätigkeiten, Bearbeitung von Betroffenenbeschwerden). Für diese Fälle sind Regelungen für die interne Kommunikation mit dem Management getroffen.	
28	Für die Entgegennahme und die Bearbeitung der Anfragen eines Betroffenen gemäß Artikel 38 Abs. 4 DS-GVO sind ein Kommunikationsprozess sowie eine nachweisbare Ablagesystematik (Fallakte) definiert. Bei der Bearbeitung von Beschwerden Betroffener wird bei Bedarf die Rechtsabteilung des Unternehmens eingebunden.	Prüfung der Angemessenheit: ● Durchsicht der Prozessvorgaben Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über bearbeitete Anfragen Betroffener bezogen auf den Aussagegehalt, die Zeitnähe der Bearbeitung sowie die Dokumentation
29	Der Datenschutzbeauftragte überwacht gemäß Artikel 39 Abs. 1 DS-GVO die Einhaltung der Anforderungen der DS-GVO und des BDSG sowie der im Rahmenwerk (Dokumentenpyramide) ggf. ergänzend definierten unternehmensinternen datenschutzrechtlichen Regelungen. Der Überwachung durch den Datenschutzbeauftragten liegt ein Überwachungskonzept zugrunde, welches folgende Aspekte berücksichtigt: ● Die Planung der Überwachung erfolgt gemäß Artikel 39 Abs. 2 DS-GVO risikoorientiert. Hierzu hat der Datenschutzbeauftragte eine sog. „Risikolandkarte“ erstellt und die Risiken der einzelnen Themen bzw. Verarbeitungstätigkeiten berücksichtigt. Die Risikoeinschätzung wird regelmäßig und anlassbezogen überprüft und in der Änderungs-/Versionshistorie dokumentiert. ● Die Überwachungstätigkeit deckt über	Prüfung der Angemessenheit: ● Durchsicht des Überwachungskonzepts Prüfung der Wirksamkeit: ● Abstimmung der sog. „Risikolandkarte“ mit dem vorliegenden Verzeichnis von Verarbeitungstätigkeiten ● Abgleich der Ergebnisse der Überwachung durch den Datenschutzbeauftragten mit Ergebnissen der Tätigkeit der Internen Revision ● Prüfung der regelmäßigen Aktualisierung des Überwachungskonzepts auf Basis der Freigabebestätigung.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	einen definierten Zeitraum alle datenschutzrechtlichen Aspekte des Unternehmens ab. ● Der Berichterstattung über die Ergebnisse der Überwachungstätigkeit liegt ein Berichtsmuster zugrunde. ● Beanstandungen werden zeitnah an das Management berichtet und unterliegen einem Follow-up-Prozess. Die Prüfungshandlungen sowie die Ergebnisse werden vom Datenschutzbeauftragten zur Erfüllung der Rechenschaftspflicht gemäß Artikel 5 Abs. 2 DS-GVO dokumentiert.	
30	Die Tätigkeit des Datenschutzbeauftragten wird durch eine unabhängige Stelle überwacht (z.B. durch die Interne Revision oder eine externe Prüfung).	Prüfung der Angemessenheit: ● Durchsicht des Prüfungsplans der Internen Revision bzw. Durchsicht (externer) Prüfungsberichte Prüfung der Wirksamkeit: ● Einsichtnahme in die Ergebnisse von Prüfungen der Internen Revision bzw. von externen Prüfungen

Anforderung: Das Unternehmen stellt mit der Einrichtung eines geeigneten datenschutzrechtlichen Risikomanagements die Einhaltung der einschlägigen datenschutzrechtlichen Vorgaben sicher.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
31	Es ist gemäß Artikel 32, Artikel 35, Artikel 24 Abs. 1 und Artikel 25 Abs. 1 DS-GVO ein geregelter Prozess zum Management von Datenschutzrisiken für die Rechte und Freiheiten von Betroffenen eingerichtet, der folgende Aspekte abbildet: ● Identifikation potentieller Risiken ● Bewertung der identifizierten Risiken in Bezug auf die Auswirkungen auf Rechte und Freiheiten von Betroffenen ● Festlegung von Maßnahmen zur Risi-	Prüfung der Angemessenheit: ● Durchsicht der Prozessdokumentation zum Management von Datenschutzrisiken Prüfung der Wirksamkeit: ● Prüfung der zutreffenden Risikobewertung in Bezug auf die Vorgaben ● Prüfung der zutreffenden Risikobehandlung in Bezug auf die Vorgaben

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	kobehandlung ● Überwachung der Umsetzung der Maßnahmen zur Risikobehandlung ● Kommunikation der Risiken an den Verantwortlichen und alle relevanten Einheiten in der Organisation. Das Risikomanagement berücksichtigt Risiken für die Rechte und Freiheiten von Betroffenen aus Projekten, Risiken aus dem Regelbetrieb, Risiken im Rahmen von Datenschutzvorfällen, Risiken aus Prozessen für datenschutzfreundliche Technik und Voreinstellungen und Risiken aus Datenschutz-Folgenabschätzungen. Die Durchführung und die Ergebnisse des Prozesses werden dokumentiert. Der Prozess wird regelmäßig auf seine Aktualität hin geprüft.	
32	Es ist ein geregelter Prozess zur Datenschutz-Folgenabschätzung eingerichtet. Durch ein zweistufiges Prüfungsverfahren ist sichergestellt, dass für Verarbeitungstätigkeiten mit einem hohen Risiko eine Datenschutz-Folgenabschätzung durchgeführt wird. 1. Erforderlichkeitsprüfung: Prüfung, ob ein hohes Risiko für die Rechte und Freiheiten von Betroffenen besteht bzw. die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 Abs. 3 DS-GVO gegeben ist. 2. Durchführung der Datenschutz-Folgenabschätzung bei voraussichtlich hohem Risiko für die Rechte und Freiheiten von Betroffenen bzw. bei Vorliegen der Voraussetzungen gemäß Artikel 35 Abs. 3 DS-GVO. Die Methode zur Durchführung und Dokumentation einer Datenschutz-Folgenabschätzung erfüllt die formalen Anforderungen gemäß Artikel 35 DS-GVO. Die Ergebnisse der Erforderlichkeitsprüfung und der Datenschutz-Folgenabschätzung werden dokumentiert.	Prüfung der Angemessenheit: ● Durchsicht der Prozessdokumentation zur Datenschutz-Folgenabschätzung. Hierbei können die von der Aufsichtsbehörde veröffentlichten Listen von Verarbeitungsvorgängen berücksichtigt werden, für die eine Datenschutz-Folgenabschätzung durchzuführen ist bzw. für die diese nicht erforderlich ist. Prüfung der Wirksamkeit: ● Prüfung, ob Verarbeitungstätigkeiten mit einem hohen Risiko entsprechend der Prozessvorgaben identifiziert wurden und ob eine Datenschutz-Folgenabschätzung durchgeführt wurde

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	Der Prozess wird regelmäßig auf seine Aktualität hin geprüft.	
33	Es ist ein geregelter Prozess zur Konsultation mit der relevanten Aufsichtsbehörde gemäß Artikel 36 DS-GVO eingerichtet für den Fall, dass trotz getroffener Maßnahmen nach erfolgter Datenschutz-Folgenabschätzung ein hohes Risiko für die Rechte und Freiheiten von Betroffenen besteht.	Prüfung der Angemessenheit: ● Durchsicht der Prozessdokumentation zur Konsultation mit der relevanten Aufsichtsbehörde. Prüfung der Wirksamkeit: ● Einsichtnahme in die Dokumentation der Ergebnisse der Konsultation mit der relevanten Aufsichtsbehörde und der abgeleiteten Maßnahmen
34	Die Verantwortlichkeiten im Rahmen des Managements von Datenschutzrisiken und der Datenschutz-Folgenabschätzung sind eindeutig geregelt. Der Datenschutzbeauftragte ist in das Management von Datenschutzrisiken, insb. in den Prozess der Datenschutz-Folgenabschätzung eingebunden.	Prüfung der Angemessenheit: ● Durchsicht der Prozessdokumentation zum Management von Datenschutzrisiken und zur Datenschutz-Folgenabschätzung Prüfung der Wirksamkeit: ● Befragungen und Abgleich mit den Rollen- und Stellenbeschreibungen ● Einsichtnahme in die Dokumentation zur Einbindung des Datenschutzbeauftragten
35	Es ist ein geregelter Prozess eingerichtet, der sicherstellt, dass auf der Grundlage der Risikobewertung angemessene technische und organisatorische Maßnahmen für Verarbeitungstätigkeiten abgeleitet und dokumentiert werden.	Prüfung der Angemessenheit: ● Durchsicht der Prozessdokumentation Prüfung der Wirksamkeit: ● Einsichtnahme in die Risikobewertung der Verarbeitungstätigkeiten und die Dokumentation der abgeleiteten technischen und organisatorischen Maßnahmen

Anforderung: Das Unternehmen hat Maßnahmen ergriffen, die mit hinreichender Sicherheit die Rechtmäßigkeit (Zulässigkeit) der Verarbeitung personenbezogener Daten sicherstellen.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
36	Es ist ein geregelter Prozess einschließlich	Prüfung der Angemessenheit:

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	der Festlegung von Rollen und Verantwortlichkeiten zur Klärung der Zulässigkeit bzw. zur Bestimmung des Erlaubnistatbestands jeder Verarbeitungstätigkeit gemäß Artikel 6 DS-GVO eingerichtet. Der Erlaubnistatbestand jeder Verarbeitungstätigkeit wird nachvollziehbar dokumentiert und die fortwährende Zulässigkeit der Verarbeitung wird regelmäßig überprüft.	● Durchsicht der Prozessdokumentation und Beurteilung der Vollständigkeit hinsichtlich der Berücksichtigung folgender Erlaubnistatbestände: - Einwilligung des Betroffenen - Vertragserfüllung - Rechtliche Verpflichtung - Lebenswichtige Interessen - Öffentliches Interesse - Berechtigtes Interesse - „Erforderlichkeit“ im Arbeitsverhältnis gemäß § 26 BDSG (z.B. zur Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses, zur Ausübung von Rechten aus dem nationalen Arbeits- und Sozialrecht, zur Aufdeckung von Straftaten, zu Zwecken der Arbeitsmedizin) ● Durchsicht der Prozessdokumentation und Beurteilung, ob z.B. in Zweifelsfällen die Einbindung des Datenschutzbeauftragten oder die Einholung rechtlichen Rats vorgesehen ist Prüfung der Wirksamkeit: ● Befragung relevanter Mitarbeiter der Fachbereiche und des Datenschutzbeauftragten und Beurteilung einzelner Verfahren aus dem Verzeichnis von Verarbeitungstätigkeiten hinsichtlich der Einhaltung der Vorgaben
37	In Bezug auf die ggf. erforderliche Einwilligung des Betroffenen zur Herstellung der Rechtmäßigkeit der Verarbeitung gemäß Artikel 7 und 8 DS-GVO sind folgende Aspekte geregelt: ● Der Text der Einwilligungsformulare entspricht einer internen Mustervorgabe oder es ist ein Prozess eingerichtet, der sicherstellt, dass Betroffene transparent über die vorgesehenen Zwecke der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten im Einzelnen informiert werden und somit ihre Einwilligung informiert erteilen.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben zur Herbeiführung von Einwilligungen einschließlich der Bearbeitung von Widerrufen. Die Vorgaben sollten insb. folgende Punkte berücksichtigen: - Freiwilligkeit einschließlich Belehrung dazu - Belehrung zur Widerrufbarkeit keine Nachteile für Betroffene bei Verweigerung oder Widerruf der Einwilligung - transparente Darstellung

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	● Erteilte Einwilligungen werden nachvollziehbar dokumentiert (Rechenschaftspflicht), dies beinhaltet auch den konkreten Wortlaut bzw. Referenz auf eine versionierte Standardformulierung. ● Es sind prozessuale Vorgaben zum Umgang mit einem Widerruf einer erteilten Einwilligung definiert. Ein Widerruf wird dokumentiert und ist ebenso einfach gestaltet wie die zugehörige Einwilligung. ● Auf die Besonderheiten spezifischer Gruppen Betroffener (z.B. Beschäftigte oder Minderjährige) wird in angemessener Weise eingegangen.	- keine Erforderlichkeit einer Schriftform - nachvollziehbare Beschreibung der Verarbeitungszwecke - Bestätigungshandlung (z.B. ankreuzbare Checkbox) - erweitertes Kopplungsverbot gemäß Artikel 7 Abs. 4 und Erwägungsgrund 43 DS-GVO - Einfachheit der Einwilligung und des Widerrufs Prüfung der Wirksamkeit: ● Einsichtnahme in erteilte Einwilligungen und Durchsicht der Bearbeitung von Widerrufen
38	Es bestehen Vorgaben für die Durchführung und Dokumentation einer Interessenabwägung im Fall der Anwendung des Erlaubnistatbestands des berechtigten Interesses gemäß Artikel 6 Abs. 1 Buchst. f) DS-GVO. Diese beinhalten die bei einer Interessenabwägung anzuwendenden Kriterien und deren Gewichtung (Kriterienkatalog) und sehen die besondere Berücksichtigung der Interessen von Minderjährigen/Kindern vor.	Prüfung der Angemessenheit: ● Durchsicht der dokumentierten Vorgaben Prüfung der Wirksamkeit: ● Befragung der mit der Interessenabwägung betrauten Mitarbeiter und Beurteilung durchgeführter Interessenabwägungen anhand deren Dokumentation
39	Es ist ein geregelter Prozess für den Umgang mit einer Zweckänderung der Verarbeitung eingerichtet, der folgende Vorgaben enthält: ● Kriterienkatalog für die Feststellung der Zulässigkeit einer Zweckänderung ● Berücksichtigung der Anforderungen gemäß Artikel 6 Abs. 4 DS-GVO und Dokumentation der Einhaltung dieser Anforderungen ● Anpassung des Verzeichnisses von Verarbeitungstätigkeiten im Hinblick auf die Zweckänderung	Prüfung der Angemessenheit: ● Durchsicht der entsprechenden Prozessvorgaben Prüfung der Wirksamkeit: ● Befragung der mit dem Prozess betrauten Mitarbeiter sowie Beurteilung durchgeführter Zweckänderungen anhand deren Dokumentation

Anforderung: Die eingerichteten Verfahren und Kontrollen stellen mit hinreichender Sicherheit sicher, dass gemäß Artikel 30 DS-GVO das Verzeichnis von Verarbeitungstätigkeiten im Unternehmen geführt und gepflegt wird und auf Anfrage bereitgestellt werden kann.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
40	Das Unternehmen führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO, um seiner Dokumentationspflicht nachzukommen. Das Verzeichnis von Verarbeitungstätigkeiten gibt für jede Verarbeitungstätigkeit Auskunft über ● den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten, ● die Zwecke der Verarbeitung, ● eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, ● die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen, ● gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Abs. 1 Unterabs. 2 DS-GVO genannten Datenübermittlungen die Dokumentation geeigneter Garantien, ● die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien, ● eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DS-GVO. Das Verzeichnis der Verarbeitungstätigkei-	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben zum Inhalt des Verzeichnisses von Verarbeitungstätigkeiten und Beurteilung, ob diese den Anforderungen von Artikel 30 Abs. 1 DS-GVO entsprechen Prüfung der Wirksamkeit: ● Einsichtnahme in Verzeichniseinträge hinsichtlich vollständiger Bearbeitung, Nachvollziehbarkeit und Einhaltung von Qualitätskontrollen

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	ten wird gemäß Artikel 30 Abs. 3 DS-GVO in schriftlicher Form oder elektronisch geführt.	
41	Soweit das Unternehmen auch als Auftragsverarbeiter tätig ist, führt es gemäß Artikel 30 Abs. 2 DS-GVO ein Verzeichnis zu allen Kategorien von den im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung. Das Verzeichnis gibt Auskunft über ● den Namen und die Kontaktdaten des Verantwortlichen, des/r von ihm beauftragten Auftragsverarbeiter/s, sowie ggf. der jeweiligen Vertreter; soweit der/die Auftragsverarbeiter einen Datenschutzbeauftragten benannt hat/haben auch die Daten des Datenschutzbeauftragten, ● die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden, ● ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Abs. 1 Unterabs. 2 DS-GVO genannten Datenübermittlungen die Dokumentation geeigneter Garantien ● eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DS-GVO. Mindestens sind die bei der Auftragsvergabe zugrunde gelegten technischen und organisatorischen Maßnahmen zu dokumentieren; ● die vorgesehenen Fristen der Löschung der verschiedenen Datenkategorien. Das Verzeichnis zu allen Kategorien von den im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung wird gemäß Artikel 30 Abs. 3 DS-GVO in schriftlicher Form oder elektronisch geführt.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben zum Inhalt des Verzeichnisses und Beurteilung, ob diese den Anforderungen von Artikel 30 Abs. 2 DS-GVO entsprechen Prüfung der Wirksamkeit: ● Einsichtnahme in Verzeichniseinträge hinsichtlich vollständiger Bearbeitung, Nachvollziehbarkeit und Einhaltung von Qualitätskontrollen

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
42	Die Verantwortlichkeiten für die Erfassung und Pflege bzw. die Qualitätssicherung der Verzeichniseinträge sind eindeutig definiert.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben, z.B. Verantwortlichkeiten-Matrix (RACI Matrix) Prüfung der Wirksamkeit: ● Beurteilung, ob die Maßnahmen von den dafür vorgesehenen Mitarbeitern durchgeführt wurden durch Befragung der Mitarbeiter und Abgleich der Vorgaben mit der tatsächlichen Organisations-Struktur bzw. durch Einsichtnahme in die erfassten Verarbeitungstätigkeiten
43	Das Unternehmen hat Verfahren und Maßnahmen eingerichtet, die die fortlaufende und ordnungsgemäße Pflege des Verzeichnisses sowie die Erfassung aller relevanten Verarbeitungstätigkeiten sicherstellen.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben, wie z.B. eines zentralen Templates, das den Fachbereichen zur Verfügung steht Prüfung der Wirksamkeit: ● Prüfung des Verzeichnisses auf Vollständigkeit und Beurteilung einzelner Verzeichniseinträge bezogen auf die fortlaufende und ordnungsmäßige Pflege
44	Die Änderungen im Verzeichnis werden versioniert, so dass die Neuaufnahme, die inhaltliche Veränderung oder das Löschen einer Verarbeitungstätigkeit nachvollziehbar sind.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben Prüfung der Wirksamkeit: ● Nachvollzug ausgewählter Änderungen und deren Historisierung
45	Auf Anfrage der Aufsichtsbehörde ist der Verantwortliche bzw. der Auftragsverarbeiter in der Lage, das Verzeichnis gemäß Artikel 30 Abs. 4 DS-GVO zur Verfügung zu stellen. Diesbezüglich ist vom Unternehmen ein Prozess einschließlich klarer Verantwortlichkeiten definiert.	Prüfung der Angemessenheit: ● Durchsicht der Prozessvorgaben sowie der Vereinbarung mit dem Auftragsverarbeiter Prüfung der Wirksamkeit: ● Nachvollzug bzw. Einsichtnahme in das an die Aufsicht übermittelte Verzeichnis
46	Es erfolgt eine regelmäßige Überprüfung der Vollständigkeit und Richtigkeit des Verzeichnisses (mindestens einmal jährlich) durch den Verantwortlichen. Das Ergebnis wird dokumentiert (sign-off).	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben Prüfung der Wirksamkeit: ● Nachvollzug / Einsichtnahme in die

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
		Sign-Off Dokumentation

Anforderung: Das Unternehmen hat gemäß Artikel 25 DS-GVO bereits bei der Programmierung, Konzeption und Entwicklung der Datenverarbeitungsvorgänge und -technik die Datenschutzgrundsätze berücksichtigt (Datenschutz durch Technikgestaltung (privacy by design)). Durch datenschutzfreundliche Voreinstellungen unterstützt das Unternehmen, dass grundsätzlich nur personenbezogene Daten verarbeitet werden, die für den Verarbeitungszweck erforderlich sind (privacy by default).

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
47	Es ist ein geregelter Prozess eingerichtet, der sicherstellt, dass bei der Konzeption und Entwicklung neuer bzw. bei der Anpassung bestehender Datenverarbeitungsvorgänge und -technik, bei der Beschaffung von Datenverarbeitungstechnik sowie im laufenden Betrieb die Berücksichtigung der Datenschutzgrundsätze erfolgt. Der Prozess enthält Vorgaben, dass sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung unter Berücksichtigung ● des Stands der Technik, ● der Implementierungskosten und der Art, des Umfangs, der Umstände und ● der Zwecke der Verarbeitung sowie ● der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen gemäß Artikel 25 Abs. 1 DS-GVO getroffen werden, um die Datenschutzgrundsätze umzusetzen.	Prüfung der Angemessenheit: ● Durchsicht der Soll-Vorgaben für Fachkonzepte und Programmierrichtlinien bzw. für Beschaffungsvorgänge im Hinblick auf die Berücksichtigung der Anforderungen des Datenschutzes bei der Softwareentwicklung und -anpassung bzw. bei der Beschaffung von Datenverarbeitungstechnik. Mögliche Sollvorgaben betreffen: - die Menge der erhobenen personenbezogenen Daten, z.B. Konzipierung der Anwendungen unter Berücksichtigung der Datenminimierung gemäß Artikel 25 Abs. 1 i.V.m. Artikel 5 Abs. 1 Buchst. c) DS-GVO - den Umfang der Verarbeitung personenbezogener Daten, z.B. die Berücksichtigung der Nichtverkettbarkeit bei der Anwendungsentwicklung - die Speicherfrist, z.B. geeignete technische Maßnahmen, die eine regelmäßige fristgerechte Löschung personenbezogener Daten gewährleisten sowie die zeitnahe Umsetzung von Löschanfragen Betroffener gemäß Artikel 17 DS-GVO - die Sicherheit der Verarbeitung personenbezogener Daten gemäß Artikel 32 DS-GVO, z.B. durch

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
		Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung Prüfung der Wirksamkeit: ● Einsichtnahme in Projektdokumentationen, Fachkonzepte, Programmdokumentationen bzw. Beschaffungsdokumentationen im Hinblick auf die Berücksichtigung der Vorgaben bei der Konzeption, Entwicklung bzw. Anpassung von Datenverarbeitungsvorgängen und -technik bzw. bei der Beschaffung von Datenverarbeitungstechnik ● soweit die Datenverarbeitungstechnik i.S.d. Artikel 42 DS-GVO zertifiziert ist, Beurteilung, ob die Zertifizierung aktuell ist und der Umfang der Zertifizierung den Anforderungen des Unternehmens an die Berücksichtigung der Datenschutzgrundsätze und an die datenschutzfreundlichen Voreinstellungen gerecht wird
48	Durch geeignete technische und organisatorische Maßnahmen wird sichergestellt, dass gemäß Artikel 25 Abs. 2 DS-GVO durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Dies betrifft ● die Menge der erhobenen personenbezogenen Daten, ● den Umfang der Verarbeitung, ● die Speicherfrist, ● die Zugänglichkeit, insb. die Sicherstellung, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.	Prüfung der Angemessenheit: ● Durchsicht von Sollvorgaben für Fachkonzeptionen bezogen auf die angemessene Planung von Einstellungsmöglichkeiten zum Schutz personenbezogener Daten, z.B. ob - die erforderlichen Pflichteingaben klar von optionalen Eingaben abgegrenzt werden und dem Grundsatz der Datensparsamkeit entsprechen, - durch geeignete Voreinstellungen Maßnahmen getroffen werden, welche eine mögliche Verkettung personenbezogener Daten unterbinden, - voreingestellte Aufbewahrungsfristen dem Gebot der Speicherbegrenzung genügen, - die vorgesehenen Standardvoreinstellungen nicht ohne Eingreifen der betroffenen Person geändert

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
		werden können Prüfung der Wirksamkeit: ● Einsichtnahme in umgesetzte Einstellungen betreffend den Schutz personenbezogener Daten ● Auswertung der programmierten Eingabefelder bezogen auf die Abgrenzung von Pflichteingaben und optionalen Eingaben und der Umsetzung des Grundsatzes der Datensparsamkeit ● Einsichtnahme in die Programmablauflogik hinsichtlich der Nutzung personenbezogener Daten für verschiedene Zwecke (Sicherstellung der Nichtverkettbarkeit) ● Prüfung der implementierten Speicherfristen für personenbezogene Daten ● Einsichtnahme in die umgesetzten Voreinstellungen im Standard hinsichtlich der Zugänglichmachung von personenbezogenen Daten an eine unbestimmte Zahl von natürlichen Personen. ● Prüfung, dass die Voreinstellungen nicht ohne Eingreifen der betroffenen Person geändert werden können.

Anforderung: Es sind gemäß Artikel 32 DS-GVO geeignete technische und organisatorische Maßnahmen eingerichtet, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Hierbei wurden der Stand der Technik, die Implementierungskosten, die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt. Die Maßnahmen umfassen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit[11] der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

[11] **Belastbarkeit (= Resilience)** stellt die Absicherung der Dienste und Systeme gegen ungewollte und gewollte, zufällige und geplante Störungen dar. Die Systeme werden in angemessener Zeit wieder in den Normalbetrieb überführt.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
49	Das Unternehmen hat Maßnahmen eingerichtet, um vollständig alle Systeme und Anwendungen zu erfassen, welche personenbezogene Daten verarbeiten. Dies umfasst auch die unterstützende IT-Infrastruktur.	Prüfung der Angemessenheit: ● Durchsicht der Richtlinien, Anweisungen, Erfassungsvorlagen, Templates etc. zur Erfassung der Systeme und Anwendungen und Beurteilung der angemessenen Ausgestaltung Prüfung der Wirksamkeit: ● Verifizierung der erfassten Systeme und Anwendungen und Beurteilung der Erfassung hinsichtlich Vollständigkeit und Aktualität
50	Es sind Richtlinien zur Sicherheit der Verarbeitung gemäß Artikel 32 DS-GVO vorhanden, die für alle Systeme und Anwendungen gelten, die personenbezogene Daten verarbeiten. Die Richtlinien umfassen klare Vorgaben, Rollen und Verantwortlichkeiten sowie Dokumentationsanforderungen und werden regelmäßig auf Aktualität geprüft.	Prüfung der Angemessenheit: ● Durchsicht des Frameworks (Richtlinienpyramide) in Bezug auf die vollständige Berücksichtigung der relevanten Systeme und Anwendungen, ● Durchsicht des Frameworks (Richtlinienpyramide) in Bezug auf das Vorhandensein und die Aktualität von Richtlinien zu - Business Continuity und IT-Desaster Recovery - Zugriffsmanagement - Kryptographischen Maßnahmen - Malware und Virenschutz Prüfung der Wirksamkeit: ● Befragung der relevanten Mitarbeiter und Abgleich mit entsprechenden Systemparametern bzw. mit systemseitig generierten Unterlagen oder Protokollen in Bezug auf die Umsetzung der Vorgaben
51	Das Unternehmen hat gemäß Artikel 32 Abs. 1 Buchst. b) und c) DS-GVO Business Continuity- und IT-Desaster Recovery-Pläne zur Wiederherstellung der Systeme und Anwendungen im Störungs- oder Katastrophenfall definiert, dokumentiert und implementiert. Die Pläne werden gemäß Artikel 32 Abs. 1 Buchst. d) DS-GVO mit einer definierten Häufigkeit auf ihre Wirk-	Prüfung der Angemessenheit: ● Durchsicht der Business Continuity- und IT-Desaster Recovery-Pläne hinsichtlich Vollständigkeit, Aktualität und Aufbau der Kontrollen. Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise zur sachgerechten Umsetzung und Durchführung der Kontrollen. Die Kontrollen

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	samkeit getestet.	können umfassen: - Pläne und Wiederherstellungsverfahren, die beschreiben, wie das Unternehmen mit disruptiven Ereignissen umgeht und seine Informationssicherheitsanforderungen auf einem vorgegebenen Niveau hält. - Verfahren zur Aufrechterhaltung der bestehenden Informationssicherheitskontrollen während einer widrigen Situation - Kompensierende Kontrollen für Informationssicherheitskontrollen, die in widrigen Situationen nicht aufrechterhalten werden können (z.B. werden für vorgesehene automatische Kontrollen während des Zeitraums einer Störung kompensierende manuelle Kontrollen durchgeführt)
52	Das Unternehmen hat gemäß Artikel 32 Abs. 1 Buchst. b) DS-GVO Verfahren und Maßnahmen eingerichtet, um das Zugriffsmanagement sicherzustellen.	Prüfung der Angemessenheit: ● Durchsicht der Dokumentation hinsichtlich Vollständigkeit, Aktualität und Aufbau der Verfahren und Maßnahmen Prüfung der Wirksamkeit: - Einsichtnahme in Dokumentationen und systemseitig generierte Unterlagen in Bezug auf die Übereinstimmung der definierten Verfahren und Maßnahmen mit den tatsächlichen Abläufen. Die Verfahren und Maßnahmen können umfassen: - Formale Richtlinien für die Zugriffsverwaltung (Zugriffsbereitstellung, -änderung und -entfernung) einschließlich privilegierter Zugriffsrechte und physischer Sicherheit - Verwendung von eindeutigen Benutzeranmeldeinformationen - Überprüfung der Benutzerrechte mit definierter Häufigkeit - Mechanismus zum Aufzeichnen des Zugriffs auf Daten, z.B. Logs, Aufzeichnungen, Tickets etc.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
		- Benutzerzugriffssteuerung für den Zugriff auf die persönlichen Daten bzw. spezielle Kategorien von Daten - Bereitstellung und Aufhebung des Zugriffs auf personenbezogene Daten bzw. spezielle Datenkategorien - Überprüfung der Zugriffsrechte für Benutzer, die auf personenbezogene Daten bzw. spezielle Datenkategorien zugreifen
53	Das Unternehmen hat gemäß Artikel 32 Abs. 1 Buchst. b) DS-GVO geeignete Test- und Freigabeverfahren eingerichtet, die neben Funktionstrennungen insb. die Trennung von Entwicklungs- und Testsystemen von den produktiv genutzten Systemen vorsehen, um sicherzustellen, dass nur freigegebene Systeme und Anwendungen produktiv zum Einsatz kommen.	Prüfung der Angemessenheit: ● Durchsicht von Richtlinien und Arbeitsanweisungen zum Test- und Freigabeverfahren bezogen auf die Nachvollziehbarkeit und Eignung der Vorgaben Prüfung der Wirksamkeit: ● Einsichtnahme in Test- und Freigabeprotokolle bezogen auf die tatsächliche Umsetzung der Vorgaben
54	Das Unternehmen verfügt gemäß Artikel 32 Abs. 1 Buchst. a) DS-GVO über eine Richtlinie für den Umgang mit kryptographischen Maßnahmen zum Schutz von Informationen einschließlich personenbezogener Daten.	Prüfung der Angemessenheit: ● Durchsicht der Richtlinie hinsichtlich Vollständigkeit und Aktualität in Bezug auf das Schutzniveau, die Schlüsselverwaltung, Rollen und Verantwortlichkeiten, sowie den aktuellen Stand der Technik. Mögliche Regelungen der Richtlinie können sein: - Ermittlung des erforderlichen Schutzniveaus unter Berücksichtigung von Art, Stärke und Qualität des erforderlichen Verschlüsselungsalgorithmus - Beschreibung der Herangehensweise an die Schlüsselverwaltung, einschließlich der Methoden zum Schutz kryptografischer Schlüssel und zur Wiederherstellung verschlüsselter Informationen bei verlorenen, kompromittierten oder beschädigten Schlüsseln - Verwendung von dem Stand der Technik entsprechenden Verschlüsselungstechnologien für defi-

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
		nierte Verbindungspunkte und für den Schutz der Kommunikation zwischen dem Verarbeitungszentrum und den mit dem Verarbeitungszentrum verbundenen Datensubjekten innerhalb oder außerhalb von Kundennetzwerken. Die Speicherung der Daten erfolgt in einem verschlüsselten Format, wobei eine Software verwendet wird, die dem aktuellen Stand der Technik entspricht. - Rückgriff auf die einschlägigen technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zur Beurteilung des aktuellen Stands der Technik Prüfung der Wirksamkeit: ● Einsichtnahme in die Dokumentation der Umsetzung der Maßnahmen (z.B. systemseitig erzeugte Auswertungen und Protokolle) und Prüfung der Berücksichtigung der kryptographischen Vorgaben
55	Das Unternehmen hat Verfahren und Maßnahmen eingerichtet, um gemäß Artikel 32 Abs. 1 Buchst. b) DS-GVO die Belastbarkeit der Systeme sicherzustellen. Dies betrifft insb. den Schutz vor Malware und Viren.	Prüfung der Angemessenheit: ● Durchsicht von Richtlinien, Anweisungen und weiteren Unterlagen hinsichtlich Vollständigkeit und Aktualität in Bezug auf die Berücksichtigung der Systeme und Anwendungen, welche personenbezogene Daten verarbeiten. ● Beurteilung der Geeignetheit der Verfahren und Maßnahmen. Mögliche Verfahren und Maßnahmen können sein: - Formale Richtlinien, die die Verwendung nicht autorisierter Software verbieten und Anti-Malware-Software aktualisieren - Kontrollen, die die Verwendung von nicht autorisierter Software verhindern oder aufdecken - Kontrollen, die die Verwendung von Websites verhindern oder aufdecken, z.B. automatisch Cookies

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
		auslesen oder Applets installieren - Malware-Erkennungs- und Reparatursoftware, die regelmäßig mit Signatur-Updates aktualisiert wird Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über die Durchführung der Verfahren und Maßnahmen ● Einsichtnahme in die Ergebnisse regelmäßig durchgeführter Penetrationstests sowie in die Dokumentation zur Umsetzung der daraus abgeleiteten Maßnahmen
56	Das Unternehmen hat Verfahren und Maßnahmen eingerichtet, um gemäß Artikel 32 Abs. 1 Buchst. a) DS-GVO Daten zu pseudonymisieren.	Prüfung der Angemessenheit: ● Durchsicht von Richtlinien, Anweisungen und weiteren Unterlagen hinsichtlich Vollständigkeit und Aktualität in Bezug auf die Berücksichtigung der Systeme und Anwendungen, welche personenbezogene Daten verarbeiten, sowie hinsichtlich der Geeignetheit der Verfahren und Maßnahmen. Mögliche Verfahren und Maßnahmen können sein: - Formale Richtlinien, die die Verwendung von Pseudonymisierung regeln. Hierbei können bestimmte Algorithmen oder Verfahren vorgeben werden. Insbesondere der Zugriff auf Entschlüsselungstabellen und Verfahren zur Entpseudonymisierung sollten geregelt sein. - Software zur Pseudonymisierung Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über die Durchführung der Verfahren und Maßnahmen ● Prüfung, ob die Daten pseudonymisiert sind
57	Das Unternehmen hat gemäß Artikel 32 Abs. 1 Buchst. d) DS-GVO Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Angemessenheit und Wirksamkeit der technischen und organisatori-	Prüfung der Angemessenheit: ● Befragung der für die Überprüfung, Bewertung und Evaluierung verantwortlichen Mitarbeiter

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	schen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung implementiert. Diese schließen die Evaluierung ein, ob die Maßnahmen dem Stand der Technik entsprechen. Das Ergebnis ist zu dokumentieren.	● Durchsicht der Richtlinien und Anweisungen bezogen auf die Vorgehensweise, die Verantwortlichkeiten und den Umgang mit festgestellten Schwächen Prüfung der Wirksamkeit: ● Einsichtnahme in Dokumentationen durchgeführter Überprüfungen, Bewertungen und Evaluierungen bezogen auf die Einhaltung der Vorgaben und ergriffene Maßnahmen zur Behebung von Schwächen

Anforderung: Die eingerichteten Verfahren und Kontrollen stellen mit hinreichender Sicherheit sicher, dass personenbezogene Daten gemäß Artikel 17 i.V.m. Artikel 5 DS-GVO regelmäßig nach Zweckbindung (bzw. nach Ablauf der Aufbewahrungsfrist) gelöscht bzw. anderweitig unbrauchbar gemacht werden.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
58	Das Unternehmen hat ein schriftlich dokumentiertes Verfahren eingerichtet, dass die folgenden Aspekte beinhaltet: ● Neben einer übergreifenden Richtlinie zur Löschung und Sperrung personenbezogener Daten sind spezifische Lösch- und Sperrkonzepte je Verarbeitungstätigkeit vorhanden, die den Grundsätzen der Zweckbindung, Datenminimierung und Speicherbegrenzung gemäß Artikel 5 DS-GVO Rechnung tragen. ● Die jeweiligen Verantwortlichkeiten sind eindeutig geregelt. ● Die Erstellung der anwendungsbezogenen Löschkonzepte sieht eine Einbindung der IT-Abteilung und der Fachbereiche vor. Soweit sich Zweckänderungen ergeben, werden die Löschkonzeptionen entsprechend überprüft. ● Die Einschätzung der Aufbewahrungsfristen sowie der Lösch- und Sperrfristen wird regelmäßig aktualisiert.	Prüfung der Angemessenheit: ● Durchsicht der Richtlinie sowie der Lösch- und Sperrkonzepte bezogen auf die Eignung der Maßnahmen. Der implementierte Prozess kann z.B. folgende Schritte enthalten: - Bestimmung von Datenkategorien - Festlegung von Aufbewahrungsfristen - Festlegung von Löschtriggern - Festlegung der Lösch- und Sperrfristen - Festlegung der Art des Löschverfahrens und der Zeitpunkte für die Löschung - Definition der Verantwortlichkeiten - Nachweise der erfolgten Löschung (Protokolle) • Einsicht in die Verantwortlichkeiten-Matrix (RACI Matrix) • Bestimmung, ob die Aufbewahrungsfristen alle einschlägigen regulatori-

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	● Eine zentrale Qualitätssicherung stellt eine unternehmensübergreifende Umsetzung der Vorgaben sicher. ● Die produktive Implementierung von technischen Löschroutinen erfolgt durch ein ordnungsgemäßes Test- und Freigabeverfahren (einschließlich der Berücksichtigung von Funktionstrennungen). ● Die Löschverfahren werden auf logische sowie physische Daten (z.B. Akten) angewandt. Hierbei werden auch ausgelagerte Daten, vor- und nachgelagerte Systeme und Datenextrakte berücksichtigt.	schen und gesetzlichen Vorschriften berücksichtigen. Prüfung der Wirksamkeit: ● Abgleich der in den Lösch- und Sperrkonzepten festgelegten Vorgaben mit Systemeinstellungen und Parametern. Hierbei können Löschklassen bzw. Löschfristen übergreifend für verschiedene Zwecke und Daten definiert werden. ● Einsichtnahme in Nachweise über die vom Unternehmen durchgeführte regelmäßige Prüfung der Umsetzung der Vorgaben ● Einsichtnahme in Verträge mit Dienstleistern bei einer Auslagerung von Prozessen bezogen auf das Vorhandensein entsprechender Regelungen.
59	Für jede Verarbeitungstätigkeit sind automatisierte (bspw. in Form einer Batchverarbeitung) oder nicht automatisierte Löschmechanismen/-prozesse implementiert, die eine vollständige Löschung der personenbezogenen Daten ermöglichen. Hierbei werden auch vor- und nachgelagerte Systeme und Datenextrakte berücksichtigt. Das Intervall der Löschung ist festgelegt. Die Löschung wird protokolliert. Die Vorgaben sind konsistent zum Verzeichnis von Verarbeitungstätigkeiten.	Prüfung der Angemessenheit: ● Durchsicht der entsprechenden Vorgaben Prüfung der Wirksamkeit: ● Abgleich der Vorgaben mit den Systemeinstellungen und Parametern ● Einsichtnahme in die Protokolle über die Durchführung der Löschung ● Abgleich der Vorgaben mit den Angaben im Verzeichnis von Verarbeitungstätigkeiten oder den Informationsblättern für Betroffene ● Prüfung der Einhaltung der Löschvorgaben für ausgewählte Datenbestände
60	Können personenbezogene Daten aus bestimmten Gründen (bspw. aufgrund von gesetzlichen Aufbewahrungsfristen) trotz Wegfalls der Zweckbindung nicht gelöscht werden (Artikel 17 Abs. 3 DS-GVO), erfolgt eine Sperrung der personenbezogenen Daten bzw. werden andere Schutzmaßnahmen vorgenommen. Die Vorgehensweise wird entsprechend dokumentiert.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben Prüfung der Wirksamkeit: ● Einsichtnahme in die Dokumentation über durchgeführte Sperrungen bezogen auf die Einhaltung der Vorgaben ● Prüfung der Umsetzung und Wirksamkeit der Sperrung für ausgewählte Datenbestände

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
61	Die fristgerechte und tatsächliche Löschung bzw. Sperrung personenbezogener Daten wird protokolliert und überwacht.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben Prüfung der Wirksamkeit: ● Einsichtnahme in Protokolle über durchgeführte Löschungen bzw. Sperrungen

Anforderung: Das Unternehmen stellt mit der Einrichtung von Prozessen für Betroffenenrechte mit hinreichender Sicherheit die Einhaltung der einschlägigen datenschutzrechtlichen Vorgaben sicher.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
62	Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person gemäß Artikel 13 DS-GVO ● Es ist ein Prozess eingerichtet, der sicherstellt, dass der betroffenen Person - zum Zeitpunkt der Erhebung der Daten die Informationen gemäß Artikel 13 Abs. 1 und 2 DS-GVO mitgeteilt werden. - bei einer beabsichtigten Änderung des Zwecks der Verarbeitung die Zweckänderung sowie die Informationen gemäß Artikel 13 Abs. 2 DS-GVO mitgeteilt werden.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben des Prozesses zur Erfüllung der Informationspflicht Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über die der betroffenen Person zur Verfügung gestellten Informationen
63	Informationspflicht gemäß Artikel 14 DS-GVO bei der Erhebung von personenbezogenen Daten, die nicht bei der betroffenen Person selbst erfolgt ● Es ist ein Prozess eingerichtet, der sicherstellt, dass - der betroffenen Person die Informationen gemäß Artikel 14 Abs. 1 und 2 DS-GVO mitgeteilt werden - die in Artikel 14 Abs. 3 DS-GVO genannten Fristen für die Mitteilung	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben des Prozesses zur Erfüllung der Informationspflicht bei indirekter Erhebung Prüfung der Wirksamkeit: ● Einsichtnahme in die Nachweise über die der betroffenen Person zur Verfügung gestellten Informationen

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	der Informationen eingehalten werden - bei einer beabsichtigten Änderung des Zwecks der Verarbeitung die Zweckänderung sowie die Informationen gemäß Artikel 14 Abs. 2 DS-GVO mitgeteilt werden	
64	Auskunftsrecht gemäß Artikel 12 und 15 DS-GVO ● Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zur Auskunft eingerichtet. ● Die Prozesse stellen sicher, dass die Auskunft gemäß Artikel 12 Abs. 1 und 6 DS-GVO nur an den rechtmäßigen Betroffenen gesendet wird bzw. dieser einwandfrei identifiziert wird. ● Auskünfte entsprechen inhaltlich den Anforderungen von Artikel 15 Abs. 1 DS-GVO. ● Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Beantwortung der Betroffenenanfragen sind den Mitarbeitern bekannt und werden eingehalten. ● Es sind Prozesse eingerichtet und technische Voraussetzungen implementiert, die es ermöglichen, dem Betroffenen auf Anfrage gemäß Artikel 15 Abs. 3 DS-GVO eine Kopie seiner personenbezogenen Daten bereitzustellen, die Gegenstand der Verarbeitung sind.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben zu dem Prozess der Auskunftserteilung ● Prüfung auf Vollständigkeit der Informationen im Template für die Beantwortung von Auskunftsersuchen ● Prüfung, ob Datenschutzhinweise bzw. Informationsschreiben des Unternehmens in Bezug auf Betroffenenrechte klar verständlich und vollständig sind Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über erteilte Auskünfte bezogen auf die Einhaltung der Vorgaben
65	Recht auf Berichtigung gemäß Artikel 16 DS-GVO ● Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zur Berichtigung eingerichtet. ● Die Berichtigung erfolgt technisch in allen Systemen bzw. an allen Speicherorten. ● Die Prozesse stellen sicher, dass die Identität des anfragenden Betroffenen gemäß Artikel 12 Abs. 1 und 6 DS-GVO eindeutig bestimmt werden kann. ● Prozesse zur Kommunikation einer	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben zu den Prozessen der Berichtigung von personenbezogenen Daten auf Anfrage von Betroffenen Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über durchgeführte Berichtigungen bezogen auf die Einhaltung der Vorgaben

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	Berichtigung an weitere Empfänger der relevanten Daten und an Betroffene gemäß Artikel 19 DS-GVO sind definiert und werden konsequent angewendet. ● Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Beantwortung der Betroffenenanfragen sind den Mitarbeitern bekannt und werden eingehalten.	
66	Recht auf Löschung gemäß Artikel 17 DS-GVO ● Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zur Löschung eingerichtet. ● Die Prozesse stellen sicher, dass die Identität des anfragenden Betroffenen gemäß Artikel 12 Abs. 1 und 6 DS-GVO eindeutig bestimmt werden kann. ● Die Prozesse stellen sicher, dass gemäß Artikel 17 Abs. 3 DS-GVO durch die Löschung keine höhergeordneten Rechte eingeschränkt werden, wie z.B. gesetzliche Vorhaltepflichten, vertragliche Grundlagen, Recht der freien Meinungsäußerung. ● Die Prozesse stellen sicher, dass – bei Vorliegen der Voraussetzungen – die relevanten personenbezogenen Daten des Betroffenen gelöscht werden. ● Prozesse zur Kommunikation einer Löschung an weitere Empfänger der relevanten Daten und an Betroffene gemäß Artikel 19 DS-GVO sind eingerichtet und werden konsequent angewendet. Dies gilt ebenso bei einer Offenlegung der Daten gemäß Artikel 17 Abs. 2 DS-GVO. ● Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Beantwortung der Betroffenenanfragen sind den Mitarbeitern bekannt und werden eingehalten.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben zu den Prozessen der Löschung von personenbezogenen Daten auf Anfrage von Betroffenen. Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über durchgeführte Löschungen bezogen auf die Einhaltung der Vorgaben ● Prüfung der Löschung für ausgewählte Datenbestände
67	Recht auf Einschränkung der Verarbeitung gemäß Artikel 18 DS-GVO ● Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zur Ein-	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben zu den Prozessen der Einschränkung der Verarbeitung auf Anfrage von Betroffenen

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	schränkung der Verarbeitung eingerichtet. ● Die Prozesse stellen sicher, dass gemäß Artikel 12 Abs. 1 und 6 DS-GVO die Identität des anfragenden Betroffenen eindeutig bestimmt werden kann. ● Die Prozesse stellen sicher, dass die Einschränkung der Verarbeitung umgesetzt wird. ● Prozesse zur Kommunikation einer Einschränkung an weitere Empfänger der relevanten Daten und an Betroffene gemäß Artikel 19 DS-GVO sind definiert und werden konsequent angewendet. ● Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Beantwortung der Betroffenenanfragen sind den Mitarbeitern bekannt und werden eingehalten.	Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über durchgeführte Einschränkungen der Verarbeitung bezogen auf die Einhaltung der Vorgaben
68	Recht auf Datenübertragbarkeit gemäß Artikel 20 DS-GVO ● Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zur Datenübertragbarkeit eingerichtet. Diese beinhalten gemäß Artikel 20 Abs. 4 DS-GVO die Überprüfung der Beeinträchtigung der Rechte Dritter vor Übertragung der Daten. ● Die Prozesse stellen sicher, dass gemäß Artikel 12 Abs. 1 und 6 DS-GVO die Identität des anfragenden Betroffenen eindeutig bestimmt werden kann. ● Prozesse zur Bereitstellung aller personenbezogenen Daten eines Betroffenen in einem strukturierten, gängigen, maschinenlesbaren Format sind definiert und werden konsequent angewendet. ● Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Beantwortung der Betroffenenanfragen sind den Mitarbeitern bekannt und werden eingehalten.	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben zu den Prozessen der Datenübertragbarkeit auf Anfrage von Betroffenen. Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über die den Betroffenen zur Verfügung gestellten Daten bezogen auf - deren Vollständigkeit - die erfolgte Überprüfung, ob durch die Herausgabe eines Datensatzes keine Rechte von Dritten eingeschränkt werden
69	Recht auf Widerspruch gegen die Verarbeitung personenbezogener Daten gemäß Artikel 21 DS-GVO ● Es sind Prozesse für die Bearbeitung	Prüfung der Angemessenheit: ● Durchsicht der Prozessvorgaben zum Widerspruchsrecht gegen die Verarbeitung

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	von Betroffenenanfragen zum Widerspruch gegen die Verarbeitung eingerichtet. Diese stellen sicher, dass bei einem begründeten Widerspruch keine weitere Verarbeitung der personenbezogenen Daten des Betroffenen vorgenommen wird bzw. anderenfalls eine begründete Ablehnung des Widerspruchs erfolgt sowie die Übermittlung der Begründung an den Betroffenen. ● Betroffene werden gemäß Artikel 21 Abs. 4 DS-GVO rechtzeitig auf das Recht hingewiesen. ● Die Prozesse stellen sicher, dass gemäß Artikel 12 Abs. 1 und 6 DS-GVO die Identität des anfragenden Betroffenen eindeutig bestimmt werden kann. ● Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Bearbeitung der Betroffenenanfragen zum Widerspruch sind den Mitarbeitern bekannt und werden eingehalten.	Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über die Bearbeitung von Widersprüchen gegen die Verarbeitung
70	Es ist ein Prozess eingerichtet, der sicherstellt, dass gemäß Artikel 22 DS-GVO die betroffene Person nicht einer Entscheidung unterworfen wird, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, soweit diese Entscheidung ausschließlich auf einer automatisierten Verarbeitung (einschließlich Profiling) beruht und keine Ausnahme gemäß Artikel 22 Abs. 2 DS-GVO gilt.	Prüfung der Angemessenheit: ● Befragung der für die Genehmigung entsprechender Entscheidungen verantwortlichen Mitarbeiter und Durchsicht der Prozessvorgaben Prüfung der Wirksamkeit: ● Befragung der zuständigen Mitarbeiter und Beobachtung von Arbeitsabläufen ● Einsichtnahme in Nachweise zu Entscheidungsfindungsprozessen und Beurteilung der Entscheidungsgrundlage

Anforderung: Die eingerichteten Verfahren und Maßnahmen stellen mit hinreichender Sicherheit sicher, dass gemäß Artikel 33 DS-GVO Datenschutzverletzungen im Unternehmen identifiziert und bewertet werden sowie bei Vorliegen eines Risikos für die Rechte und Freiheiten des Betroffenen eine Meldung an die Aufsichtsbehörde erfolgt und dass darüber hinaus gemäß Artikel 34 DS-GVO bei Vorliegen eines voraussichtlich hohen Risikos für die Rechte und Freiheiten des Betroffenen eine Benachrichtigung des Betroffenen erfolgt.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
71	Es ist ein schriftlich dokumentierter Prozess eingerichtet, der mindestens jährlich auf seine Aktualität überprüft wird, eindeutige Regelungen zu Verantwortlichkeiten (einschließlich Stellvertreterregelungen) Kommunikationswegen und Berichtslinien, der Einbindung des Datenschutzbeauftragten sowie zu folgenden Aktivitäten enthält: ● Identifikation von Datenschutzverletzungen, dies schließt die unverzügliche Meldung des Auftragsverarbeiters an den Auftraggeber ein, wenn dem Auftragsverarbeiter eine Datenschutzverletzung bekannt wird ● Bewertung der Risiken (Risikoassessment/Risikoanalyse) ● Aufarbeitung des Sachverhalts ● Auswahl geeigneter Maßnahmen (ad-hoc Behebung sowie Vermeidung einer Wiederholung) ● Entscheidung über eine Meldung und Meldung an die Aufsichtsbehörde (< 72h) ● Unverzügliche Benachrichtigung des Betroffenen bei voraussichtlich hohem Risiko ● Nachgelagerte Überprüfung auf mögliche Prozessschwächen. Es sind zudem Vorgaben für eine Dokumentation der einzelnen Aspekte vorhanden.	Prüfung der Angemessenheit: ● Durchsicht der Prozessdokumentation und Beurteilung der Vorgaben Prüfung der Wirksamkeit: ● Befragung von Mitarbeitern und Einsichtnahme in Nachweise über identifizierte und bewertete Datenschutzverletzungen bezogen auf die Einhaltung der hier genannten Vorgaben der Melde- und Benachrichtigungsprozesse
72	Es sind Kommunikationswege im Unternehmen definiert, über die (auch anonym) Datenschutzverletzungen gemeldet werden können. Dies beinhaltet, dass die Anlaufstellen im Unternehmen zur Meldung einer Datenschutzverletzung bekannt und für alle Mitarbeiter erreichbar sind. Die Kommunikationswege berücksichtigen auch die Einbindung der Abteilung Unternehmenskommunikation bzw. einer PR-Agentur. Diesbezüglich ist eine Vorabauswahl möglicher Kooperationspartner erfolgt, um die unverzügliche Information sicherzustellen.	Prüfung der Angemessenheit: ● Befragung von Mitarbeitern zu Kenntnissen über die Kommunikationswege ● Durchsicht der jeweiligen Prozessanweisungen und Beurteilung des Vorhandenseins von Absprungpunkten zum datenschutzrechtlichen Meldeprozess Prüfung der Wirksamkeit: ● Validierung durch eine eigene Testmeldung

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	● Alle anderen relevanten Prozesse, bei denen Datenschutzverletzungen identifiziert oder registriert werden können, sind mit dem datenschutzrechtlichen Meldeprozess des Unternehmens verknüpft.	
73	Die Risikobewertung gemäß Artikel 33 Abs. 1 und Artikel 34 Abs. 1 DS-GVO fokussiert auf die Risiken für die persönlichen Rechte und Freiheiten des Betroffenen. Hierbei werden Eintrittswahrscheinlichkeit und Schwere des Risikos (z.B. im Hinblick auf die Kategorie von betroffenen Daten) berücksichtigt sowie die ergriffenen technischen und organisatorischen Maßnahmen.	Prüfung der Angemessenheit: ● Durchsicht der entsprechenden Vorgaben und Beurteilung der Angemessenheit unter Berücksichtigung des rechtlichen und wirtschaftlichen Umfelds des Unternehmens Prüfung der Wirksamkeit: ● Nachvollzug der Risikobewertung für ausgewählte Datenschutzverletzungen
74	Jede identifizierte bzw. gemeldete Datenschutzverletzung wird zur Erfüllung der Rechenschaftspflicht gemäß Artikel 5 Abs. 2 und Artikel 24 Abs. 1 DS-GVO in einem zentralen Verzeichnis dokumentiert. Die Dokumentation beinhaltet u.a. ● den Zeitpunkt der Identifikation (Bekanntwerden), ● betroffene Auftragsverarbeiter, IT-Systeme, Datenkategorien, ● das Ergebnis der Risikobewertung. Sofern aus der Datenschutzverletzung ein Risiko für die Rechte und Freiheiten des Betroffenen resultiert, ist Folgendes zu dokumentieren: ● Art der Datenschutzverletzung, Kategorien und Umfang betroffener Datensätze sowie Kategorien und Anzahl betroffener Personen ● wahrscheinliche Folgen bzw. Auswirkungen der Datenschutzverletzung ● durch das Unternehmen ergriffene bzw. vorgeschlagene Maßnahmen zur Behebung der Datenschutzverletzung sowie zur Verhinderung erneuter Fehler ● Zeitpunkt und Schriftsatz einer Kommunikation mit der Aufsichtsbehörde (falls >72 Stunden auch die entsprechende	Prüfung der Angemessenheit: ● Durchsicht der entsprechenden Vorgaben Prüfung der Wirksamkeit: ● Einsichtnahme in das zentrale Verzeichnis und Prüfung dokumentierter Datenschutzverletzungen bezogen auf die Einhaltung der Dokumentationsvorgaben

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	Begründung für die Verzögerung) ● Zeitpunkt und Inhalt der Benachrichtigung des Betroffenen	
75	Die Mindestinhalte der Meldung an die Aufsichtsbehörde sind in Form einer Anweisung oder eines Musterschreibens definiert und berücksichtigen die Anforderungen gemäß Artikel 33 Abs. 3 DS-GVO.	Prüfung der Angemessenheit: ● Durchsicht der Anweisung oder des Musterschreibens Prüfung der Wirksamkeit: ● Einsichtnahme in erfolgte Meldungen an die Aufsichtsbehörde bezogen auf die Einhaltung der Mindestinhalte
76	Die Mindestinhalte der Benachrichtigung des Betroffenen sind in Form einer Anweisung oder eines Musterschreibens definiert und berücksichtigen die Anforderungen gemäß Artikel 34 Abs. 2 DS-GVO.	Prüfung der Angemessenheit: ● Durchsicht der Anweisung oder des Musterschreibens Prüfung der Wirksamkeit: ● Einsichtnahme in erfolgte Benachrichtigungen bezogen auf die Einhaltung der Mindestinhalte
77	Die Verfahren und Maßnahmen zur Identifikation, Bewertung und Meldung von Datenschutzverletzungen sind so ausgestaltet, dass die gemäß Artikel 33 Abs. 1 DS-GVO vorgegebene Frist von 72 Stunden eingehalten werden kann. Um den Anforderungen an die Reaktionszeit von 72 Stunden bei einer Meldung an die Aufsichtsbehörde gerecht zu werden, sehen die Prozesse auch Kommunikationswege und Eskalationsmaßnahmen vor, die außerhalb der Geschäftszeiten ergriffen werden.	Prüfung der Angemessenheit: ● Durchsicht der entsprechenden Vorgaben Prüfung der Wirksamkeit: ● Einsichtnahme in die Dokumentation erfolgter Meldungen von Datenschutzverletzungen bezogen auf die Einhaltung der Meldefrist
78	Die Verfahren und Maßnahmen zur Identifikation und Bewertung von Datenschutzverletzungen sowie zur Benachrichtigung des Betroffenen gemäß Artikel 34 Abs. 1 DS-GVO sind so ausgestaltet, dass – unter Berücksichtigung der Ausnahmen gemäß Artikel 34 Abs. 3 DS-GVO – eine unverzügliche Benachrichtigung des Betroffenen erfolgt. Soweit eine Weisung der Aufsichtsbehörde oder einer Strafverfolgungsbehörde hin-	Prüfung der Angemessenheit: ● Durchsicht der entsprechenden Vorgaben. So sieht die Benachrichtigung des Betroffenen bspw. die vorherige Rücksprache mit der Aufsichtsbehörde bzw. die Abstimmung mit der Rechtsabteilung und der Geschäftsführung vor. Prüfung der Wirksamkeit: ● Einsichtnahme in die Dokumentation erfolgter Benachrichtigungen von Be-

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	sichtlich des Zeitpunkts der Benachrichtigung vorliegt, wird diese berücksichtigt.	troffenen bezogen auf die Einhaltung der Benachrichtigungsfrist und die zutreffende Anwendung der Ausnahmetatbestände gemäß Artikel 34 Abs. 3 DS-GVO
79	Soweit gemäß Artikel 34 Abs. 3 Buchst. c) DS-GVO eine individuelle Benachrichtigung des Betroffenen mit einem unverhältnismäßigen Aufwand verbunden ist, sind Regelungen vorgesehen, die eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme ermöglichen. Hierfür sind entsprechende Kooperationspartner (z.B. PR-Agenturen) identifiziert, um eine zeitnahe Umsetzung zu ermöglichen.	Prüfung der Angemessenheit: ● Durchsicht der entsprechenden Vorgaben Prüfung der Wirksamkeit: ● Einsichtnahme in Testfälle des Unternehmens im Rahmen des Business Continuity Managements
80	Es sind Prozesse, Verantwortlichkeiten und Schnittstellen definiert, die es dem Unternehmen ermöglichen, auch Datenschutzverletzungen seiner Auftragsverarbeiter zu identifizieren, zu bewerten, nachweisbar zu dokumentieren und ggf. der Aufsichtsbehörde zu melden bzw. den Betroffenen zu benachrichtigen. Auftragsverarbeiter sind vertraglich verpflichtet, regelmäßig zu berichten, auch wenn keine Datenschutzverletzungen vorliegen (Null-Meldung) (Artikel 28 Abs. 3 Buchst. f) und Artikel 33 Abs. 2 DS-GVO).	Prüfung der Angemessenheit: ● Durchsicht der entsprechenden Vorgaben bzw. Musterverträge etc. Prüfung der Wirksamkeit: ● Einsichtnahme in ausgewählte Verträge zur Auftragsverarbeitung sowie in die regelmäßige Berichterstattung der Auftragsverarbeiter
81	Die Verantwortlichen der Fachbereiche und Stäbe bestätigen regelmäßig (mindestens jährlich), dass alle Datenschutzverletzungen in den zentralen Prozess gemeldet wurden bzw. keine Datenschutzverletzungen vorlagen (Null-Meldung).	Prüfung der Angemessenheit: ● Durchsicht der Vorgaben Prüfung der Wirksamkeit: ● Nachvollzug/Einsichtnahme in die Meldungen

Anforderung: Die eingerichteten Verfahren und Maßnahmen bieten hinreichende Sicherheit dafür, dass die Verarbeitung personenbezogener Daten durch Auftragsverarbeiter nur in Übereinstimmung mit einem entsprechenden Vertrag oder einem anderen rechtlich verbindlichen Dokument (Verarbeitungsvereinbarung) erfolgt und dass die Verarbeitung nur durch die vom Unternehmen zugelassenen Auftragsverarbeiter durchgeführt wird.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
82	Das Unternehmen hat vom Auftragsverarbeiter gemäß Artikel 28 Abs. 1 DS-GVO geeignete Garantien erhalten und geprüft, in denen zugesichert wird, dass die Verfahren, Maßnahmen und Kontrollen den Anforderungen der DS-GVO entsprechen.	Prüfung der Angemessenheit: ● Durchsicht der Garantien Prüfung der Wirksamkeit: ● Einsichtnahme in die Dokumentation zu durchgeführten Prüfungen der Garantien
83	Das Unternehmen hat gemäß Artikel 28 i.V.m. Artikel 29 DS-GVO Anweisungen für die Verarbeitung und den Schutz personenbezogener Daten an den Auftragsverarbeiter erteilt, einschließlich der Verarbeitung durch andere Auftragsverarbeiter (Unterbeauftragung). Diese Anweisungen sind Gegenstand eines schriftlichen Vertrags, der die Mindestbestandteile gemäß Artikel 28 Abs. 3 DS-GVO enthält.	Prüfung der Angemessenheit: ● Durchsicht der Anweisungen Prüfung der Wirksamkeit: ● Einsichtnahme in Verträge bezogen auf die vollständige Berücksichtigung der Anweisungen bzw. Mindestbestandteile gemäß Artikel 28 Abs. 3 DS-GVO
84	Die Inanspruchnahme weiterer Auftragsverarbeiter durch den Auftragsverarbeiter (Unterbeauftragung) erfordert gemäß Artikel 28 Abs. 2 DS-GVO die vorherige Zustimmung durch das Unternehmen.	Prüfung der Angemessenheit: ● Durchsicht der Verträge Prüfung der Wirksamkeit: ● Prüfung der Liste der weiteren Auftragsverarbeiter auf Vollständigkeit und Aktualität (z.B. durch Einholung einer schriftlichen Bestätigung vom Auftragsverarbeiter) und Abgleich mit erfolgten Zustimmungen
85	Das Unternehmen überwacht regelmäßig die Einhaltung der vertraglichen Regelungen durch den Auftragsverarbeiter und stellt sicher, dass die Verarbeitung und Gewährleistung der Sicherheit der personenbezogenen Daten bei dem Auftragsverarbeiter nach seinen Vorgaben durchgeführt wird.	Prüfung der Angemessenheit: ● Durchsicht der Verträge mit dem Auftragsverarbeiter Prüfung der Wirksamkeit: ● Befragung der für die Überwachung des Auftragsverarbeiters verantwortlichen Mitarbeiter und Einsichtnahme in die Dokumentation durchgeführter Überwachungsmaßnahmen

Anforderung: Die eingerichteten Verfahren und Maßnahmen bieten hinreichende Sicherheit dafür, dass die Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation in Übereinstimmung mit den Artikeln 44 bis 49 DS-GVO erfolgt und somit das durch die DS-GVO vorgegebene Schutzniveau eingehalten wird.

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
86	Es ist ein schriftlich dokumentierter Prozess eingerichtet, der sicherstellt, dass die Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation durch das Unternehmen oder den Auftragsverarbeiter nur erfolgt, sofern ● die EU-Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet oder ● das Unternehmen oder der Auftragsverarbeiter geeignete Garantien gemäß Artikel 46 DS-GVO vorgesehen hat oder ● ein Ausnahmetatbestand gemäß Artikel 49 DS-GVO vorliegt. Der Prozess beinhaltet ● die regelmäßige Überprüfung der Aktualität der Beschlüsse der EU-Kommission in Bezug auf Drittländer und internationale Organisationen ● die Überprüfung des Vorliegens und der Zulässigkeit geeigneter Garantien gemäß Artikel 46 DS-GVO ● die regelmäßige Überprüfung, ob die Garantien noch ausreichend, durchsetzbar und wirksam sind ● die Prüfung und Genehmigung von Ausnahmetatbeständen gemäß Artikel 49 DS-GVO ● die Berücksichtigung entsprechender vertraglicher Regelungen mit dem Auftragsverarbeiter, die diesen ebenfalls	Prüfung der Angemessenheit: ● Durchsicht der Prozessvorgaben Prüfung der Wirksamkeit: ● Einsichtnahme in - Nachweise über durchgeführte Beurteilungen der Aktualität der Beschlüsse der EU-Kommission und Abgleich mit der Internetseite der EU-Kommission[12] - Nachweise über die Beurteilung der Zulässigkeit und Wirksamkeit von Garantien - Genehmigungen von Ausnahmetatbeständen - Verträge mit Auftragsverarbeitern

[12] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en (Stand: 12.06.2018).

Nr.	Grundsätze, Verfahren und Maßnahmen	Beispielhafte Prüfungshandlungen
	zur Einhaltung der vorgenannten Anforderungen verpflichten	

Die nachfolgenden Anlagen enthalten Beispiele für die Formulierung von Prüfungsvermerken bzw. Prüfungsberichten. Die zusätzlichen Bestandteile eines Prüfungsberichts gegenüber einem Prüfungsvermerk sind jeweils wie folgt kenntlich gemacht: [*kursiv*]

Anlage 2: Auftragsart „Prüfung einer Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Wirksamkeitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG

An die [Gesellschaft]

Wir haben eine Prüfung der in nachstehender Anlage 1 beigefügten Erklärung der gesetzlichen Vertreter zur Beschreibung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG sowie zur Angemessenheit und Wirksamkeit dieser Grundsätze, Verfahren und Maßnahmen (im Folgenden „Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG“) der [Gesellschaft] (im Folgenden die „Gesellschaft“) für den Zeitraum vom [Datum] bis [Datum] durchgeführt.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der Gesellschaft sind für die Aufstellung der Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG nach den untengenannten Kriterien verantwortlich sowie für die internen Kontrollen, die sie als notwendig erachten, um eine Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG aufzustellen, die frei von wesentlichen – beabsichtigten und unbeabsichtigten – Fehlern ist. Des Weiteren sind die gesetzlichen Vertreter für die Konzeption, Implementierung, Aufrechterhaltung, Überwachung und Dokumentation der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG verantwortlich, die in allen wesentlichen Belangen die untengenannten Kriterien zur Angemessenheit und Wirksamkeit erfüllen. Aufgrund bestehender inhärenter Grenzen von Systemen können die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG diese Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Aufstellung der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG sowie zur Angemessenheit und Wirksamkeit dieser Grundsätze, Verfahren und Maßnahmen umfassen die im *IDW Prüfungshinweis: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)* konkretisierten Regelungen der EU-Datenschutz-Grundverordnung (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG) im Zusammenhang mit der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen. [ggf. Beschreibung weiterer Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG frei von wesentlichen Fehlern ist.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)* durchgeführt. Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen frei von wesentlichen Fehlern ist, was die Beurteilung umfasst, ob die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet sind, ob die in der Erklärung der gesetzlichen Vertreter dargestellten Grundsätze, Verfahren und Maßnahmen des Datenschutzes in allen wesentlichen Belangen geeignet waren, mit hinreichender Sicherheit die Kriterien zu erfüllen, und ob diese dargestellten Grundsätze, Verfahren und Maßnahmen des Datenschutzes in allen wesentlichen Belangen während des Zeitraums vom [Datum] bis [Datum] mit hinreichender Sicherheit implementiert waren und die Kriterien wirksam erfüllt haben.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.1* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung von Risiken wesentlicher – beabsichtigter oder unbeabsichtigter – Fehler in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG ein. Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG angewandten Methoden und Kontrollen sowie der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens. Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG relevante interne Kontrollsystem abzugeben. Für die Beurteilung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Grundsätze, Verfahren und Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Die Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbau- und einer Funktionsprüfung zur Erlangung ausreichender geeigneter

Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung der Risiken des Vorhandenseins von wesentlichen Mängeln ein.

[***Prüfungshandlungen, Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen***

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen/Empfehlungen gegeben, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen und Empfehlungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

a) *Sonstige Feststellungen, u.a.*
   - *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der Erklärung oder der Grundsätze, Verfahren und Maßnahmen,*
   - *nicht wesentliche falsche Angaben in der Erklärung,*
   - *nicht wesentliche Mängel in der Angemessenheit oder Wirksamkeit der Grundsätze, Verfahren und Maßnahmen,*

b) *Empfehlungen.*]

Eine zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen und der weiteren Prüfungshandlungen sowie Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen sind in unserem Prüfungsbericht vom [Datum] enthalten. Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- sind die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- ist die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- waren die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Grundsätze, Verfahren und Maßnahmen in allen wesentlichen Belangen mit hinreichender Sicherheit

  - geeignet, die o.g. Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert und
  - im geprüften Zeitraum wirksam.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- sind die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- ist die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- waren die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Grundsätze, Verfahren und Maßnahmen in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert und
  - im geprüften Zeitraum wirksam.]

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit der Grundsätze, Verfahren und Maßnahmen erstrecken sich auf den Zeitraum vom [Datum] bis [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter]

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG wurden durch die Gesellschaft abgegrenzt und beinhalten daher möglicherweise nicht jeden Aspekt, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte. Folglich ist die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG möglicherweise für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an die Gesellschaft gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG

Allgemeine Auftragsbedingungen

Anlage 3: Auftragsart „Prüfung einer Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Angemessenheitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG

An die [Gesellschaft]

Wir haben eine Prüfung der in nachstehender Anlage 1 beigefügten Erklärung der gesetzlichen Vertreter zur Beschreibung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG sowie zur Angemessenheit dieser Grundsätze, Verfahren und Maßnahmen (im Folgenden „Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG“) der [Gesellschaft] (im Folgenden die „Gesellschaft“) zum [Datum] durchgeführt.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der Gesellschaft sind für die Aufstellung der Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG nach den untengenannten Kriterien verantwortlich sowie für die internen Kontrollen, die sie als notwendig erachten, um eine Erklärung zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG aufzustellen, die frei von wesentlichen – beabsichtigten und unbeabsichtigten – Fehlern ist. Des Weiteren sind die gesetzlichen Vertreter für die Konzeption, Implementierung, Aufrechterhaltung, Überwachung und Dokumentation der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG verantwortlich, die in allen wesentlichen Belangen die untengenannten Kriterien zur Angemessenheit erfüllen. Aufgrund bestehender inhärenter Grenzen von Systemen können die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG diese Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Aufstellung der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG sowie zur Angemessenheit dieser Grundsätze, Verfahren und Maßnahmen umfassen die im *IDW Prüfungshinweis: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)* konkretisierten Regelungen der EU-Datenschutz-Grundverordnung (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG) im Zusammenhang mit der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen. [ggf. Beschreibung weiterer Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG frei von wesentlichen Fehlern ist.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)* durchgeführt. Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen frei von wesentlichen Fehlern ist, was die Beurteilung umfasst, ob die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet sind, ob die in der Erklärung der gesetzlichen Vertreter dargestellten Grundsätze, Verfahren und Maßnahmen des Datenschutzes in allen wesentlichen Belangen geeignet waren, mit hinreichender Sicherheit die Kriterien zu erfüllen, und ob diese dargestellten Grundsätze, Verfahren und Maßnahmen des Datenschutzes in allen wesentlichen Belangen mit hinreichender Sicherheit zum [Datum] implementiert waren.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.1* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung von Risiken wesentlicher – beabsichtigter oder unbeabsichtigter – Fehler in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG ein. Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG angewandten Methoden und Kontrollen sowie der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens. Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG relevante interne Kontrollsystem abzugeben. Für die Beurteilung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Grundsätze, Verfahren und Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Die Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbauprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung der Risiken des Vorhandenseins von wesentlichen Mängeln ein.

[***Prüfungshandlungen, Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen***

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen über-

wiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen/Empfehlungen gegeben, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen und Empfehlungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

a) *sonstige Feststellungen, u.a.*
   - *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der Erklärung oder der Grundsätze, Verfahren und Maßnahmen*
   - *nicht wesentliche falsche Angaben in der Erklärung*
   - *nicht wesentliche Mängel in der Angemessenheit der Grundsätze, Verfahren und Maßnahmen*

b) *Empfehlungen*]

Eine zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen und der weiteren Prüfungshandlungen sowie Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen sind in unserem Prüfungsbericht vom [Datum] enthalten. Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- sind die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- ist die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- waren die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Grundsätze, Verfahren und Maßnahmen in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen und
  - zum zu prüfenden Zeitpunkt implementiert.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- sind die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- ist die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- waren die in der Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG dargestellten Grundsätze, Verfahren und Maßnahmen in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen und
  - zum zu prüfenden Zeitpunkt implementiert.**]**

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften Systems

Die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Angemessenheit der Grundsätze, Verfahren und Maßnahmen erstrecken sich auf den Zeitpunkt zum [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter]

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG wurden durch die Gesellschaft abgegrenzt und beinhalten daher möglicherweise nicht jeden Aspekt, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte. Folglich ist die Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG möglicherweise für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an die Gesellschaft gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Erklärung der gesetzlichen Vertreter zu den Grundsätzen, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG

Allgemeine Auftragsbedingungen

Anlage 4: Auftragsart „Direkte Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Wirksamkeitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG

An die [Gesellschaft]

Wir haben eine Prüfung der Angemessenheit und Wirksamkeit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG der [Gesellschaft] (im Folgenden die „Gesellschaft“) für den Zeitraum vom [Datum] bis [Datum] durchgeführt. Zur Darstellung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG verweisen wir auf nachstehende Anlage 1.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der Gesellschaft sind für die Konzeption, Implementierung, Aufrechterhaltung, Überwachung und Dokumentation der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG verantwortlich, die in allen wesentlichen Belangen die untengenannten Kriterien zur Angemessenheit und Wirksamkeit erfüllen. Aufgrund bestehender inhärenter Grenzen von Systemen können die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG diese Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Angemessenheit und Wirksamkeit der Grundsätze, Verfahren und Maßnahmen umfassen die im *IDW Prüfungshinweis: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)* konkretisierten Regelungen der EU-Datenschutz-Grundverordnung (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG) im Zusammenhang mit der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen. [ggf. Beschreibung weiterer Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit über die Angemessenheit und Wirksamkeit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG abzugeben.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)* durchgeführt. Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen geeignet waren, mit hinreichender Sicherheit die Kriterien zu erfüllen und ob die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen während des Zeitraums vom [Datum] bis [Datum] mit hinreichender Sicherheit implementiert waren und die Kriterien wirksam erfüllt haben.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.1* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Für die Beurteilung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Grundsätze, Verfahren und Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Die Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbau- und einer Funktionsprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung der Risiken des Vorhandenseins von wesentlichen Mängeln ein.

[***Prüfungshandlungen, Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen***

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen/Empfehlungen gegeben, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen und Empfehlungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

a) *Sonstige Feststellungen, u.a.*
   - *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der Grundsätze, Verfahren und Maßnahmen*
   - *nicht wesentliche Mängel in der Angemessenheit oder Wirksamkeit der Grundsätze, Verfahren und Maßnahmen*

b) *Empfehlungen.*]

Eine zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen und der weiteren Prüfungshandlungen sowie Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen sind in unserem Prüfungsbericht vom [Datum] enthalten. Wir sind der Auffassung, dass die von uns erlangten

Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- sind die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- waren die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert und
  - im geprüften Zeitraum wirksam.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- sind die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- waren die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert und
  - im geprüften Zeitraum wirksam.]

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG erstrecken sich auf den Zeitraum vom [Datum] bis [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG wurden durch die Gesellschaft abgegrenzt und beinhalten daher möglicherweise nicht jeden Aspekt, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte. Folglich ist die beigefügte Darstellung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG möglicherweise für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an die Gesellschaft gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Darstellung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG

Allgemeine Auftragsbedingungen

Anlage 5: Auftragsart „Direkte Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Angemessenheitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG

An die [Gesellschaft]

Wir haben eine Prüfung der Angemessenheit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG der [Gesellschaft] (im Folgenden die „Gesellschaft“) zum [Datum] durchgeführt. Zur Darstellung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG verweisen wir auf nachstehende Anlage 1.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der Gesellschaft sind für die Konzeption, Implementierung, Aufrechterhaltung, Überwachung und Dokumentation der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG verantwortlich, die in allen wesentlichen Belangen die untengenannten Kriterien zur Angemessenheit erfüllen. Aufgrund bestehender inhärenter Grenzen von Systemen können die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG diese Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Angemessenheit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG umfassen die im *IDW Prüfungshinweis: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)* konkretisierten Regelungen der EU-Datenschutz-Grundverordnung (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG) im Zusammenhang mit der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen. [ggf. Beschreibung weiterer Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit über die Angemessenheit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG abzugeben.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)* durchgeführt. Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen geeignet waren, mit hinreichender Sicherheit die Kriterien zu erfüllen und ob die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen mit hinreichender Sicherheit zum [Datum] implementiert waren.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.1* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Für die Beurteilung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG mit hinreichender Sicherheit aufgedeckt werden. Die Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbauprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung der Risiken des Vorhandenseins von wesentlichen Mängeln ein.

[***Prüfungshandlungen, Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen***

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen/Empfehlungen gegeben, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen und Empfehlungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

a) *Sonstige Feststellungen, u.a.*
   - *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG*
   - *nicht wesentliche Mängel in der Angemessenheit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG*

b) Empfehlungen.]

Eine zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen und der weiteren Prüfungshandlungen sowie Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen sind in unserem Prüfungsbericht vom [Datum] enthalten. Wir sind der Auffassung, dass die von uns erlangten

Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- sind die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- waren die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen und
  - zum zu prüfenden Zeitpunkt implementiert.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- sind die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- waren die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o.g. Kriterien zu erfüllen und
  - zum zu prüfenden Zeitpunkt implementiert.]

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften Systems

Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Angemessenheit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG erstrecken sich auf den Zeitpunkt zum [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG wurden durch die Gesellschaft abgegrenzt und beinhalten daher möglicherweise nicht

jeden Aspekt, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte. Folglich ist die beigefügte Darstellung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG möglicherweise für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an die Gesellschaft gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Darstellung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG

Allgemeine Auftragsbedingungen

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)

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[1]

1. Vorbemerkungen

1 Dieser *IDW Prüfungshinweis* basiert auf dem *IDW PS 860*[2], der die Grundsätze und Vorgehensweise festlegt, nach denen IT-Prüfungen außerhalb der Abschlussprüfung durchzuführen sind.

---

[1] Verabschiedet vom Fachausschuss für Informationstechnologie (FAIT) am 21.06.2019 und billigende Kenntnisnahme durch den Hauptfachausschuss (HFA) am 10.07.2019. Redaktionelle Anpassung der Anlage 1 an den Anforderungskatalog der BSI Veröffentlichung „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ (Stand: 28.02.2020).

[2] *IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* (Stand: 02.03.2018).

Er konkretisiert die Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Abs. 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)[3] umzusetzenden Maßnahmen und legt die Berufsauffassung dar, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit bei der Prüfung der gemäß § 8a BSIG umzusetzenden Maßnahmen vorgehen.

2 Betreiber Kritischer Infrastrukturen sind privatwirtschaftliche oder öffentlich-rechtliche Organisationen aus den Branchen der Kritischen Infrastrukturen, die Anlagen betreiben, mit Einfluss auf die Erbringung der kritischen Dienstleistung.[4] Wer Betreiber Kritischer Infrastrukturen ist (KRITIS-Betreiber), bestimmt sich nach dem BSIG und der BSI-Kritisverordnung (BSI-KritisV) in der aktuellen Fassung.[5]

Der in Anlage 1 enthaltene Anforderungskatalog basiert auf der BSI-Veröffentlichung „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“[6] und ist eine vom IDW als sachgerecht angesehene Anwendung der Kriterien des § 8a BSIG zur Einrichtung geeigneter Grundsätze, Verfahren und Maßnahmen (im Folgenden Maßnahmen), die bei einer Prüfung nach diesem *IDW Prüfungshinweis* beurteilt werden.

3 Dieser *IDW Prüfungshinweis* gilt sowohl für die Auftragsart „Prüfung einer Erklärung des Betreibers Kritischer Infrastrukturen über die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ als auch für die Auftragsart „direkte Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“.

4 Zusammenfassend kennzeichnen insb. die folgenden Merkmale einen Prüfungsauftrag gemäß *IDW PS 860*[7] für die Beurteilung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen unter Anwendung dieses Prüfungshinweises:

- Involvierte Parteien sind neben dem Wirtschaftsprüfer und dem Betreiber der Kritischen Infrastruktur (verantwortlich für das Prüfungsobjekt) weitere vorgesehene Nutzer des Prüfungsberichts, die sich vom Adressaten (i.d.R. die beauftragende Partei) unterscheiden können. Zu den vorgesehenen Nutzern zählt insb. das BSI.
- Das zu prüfende IT-System zum Betrieb der Anlage mit Einfluss auf die kritische Dienstleistung ist klar bestimmbar und abgrenzbar (KRITIS-relevante IT-Systeme).
- Der Wirtschaftsprüfer berichtet über die Prüfung entsprechend der Informationsbedürfnisse der vorgesehenen Nutzer der Berichterstattung in einem Prüfungsbericht. Durch die Vorlage des Prüfungsberichts über die Wirksamkeitsprüfung (vgl. Tz. 5ff.) kann der Betreiber der Kritischen Infrastruktur in geeigneter Weise die Erfüllung der Anforderungen des § 8a Absatz 1 BSIG gegenüber dem BSI nachweisen (§ 8a Abs. 3 BSIG).

---

[3] Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz – BSIG) vom 14.08.2009 (BGBl. I S. 2821).

[4] Vgl. www.kritis.bund.de, Rubrik: Glossar (Stand: 24.03.2020).

[5] BSI-Kritisverordnung vom 22.04.2016 (BGBl. I S. 958), die durch Artikel 1 der Verordnung vom 21.06.2017 (BGBl. I S. 1903) geändert worden ist.

[6] Vgl. www.bsi.bund.de, Rubrik: Themen (Stand: 30.03.2020).

[7] Vgl. *IDW PS 860*, Tz. 5.

2. Ziel und Umfang der Prüfung

5 Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) hat mit dem *IDW PS 860* die Berufsauffassung dargelegt, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit die Prüfung von IT-Systemen außerhalb der Abschlussprüfung planen, durchführen sowie darüber Bericht erstatten.

Eine nach *IDW PH 9.860.2* durchgeführte Prüfung der nach § 8a Abs. 1 BSIG umzusetzenden Maßnahmen kann als Angemessenheitsprüfung oder zusätzlich als Wirksamkeitsprüfung i.S. von *IDW PS 860* erfolgen. Die Durchführung von Wirksamkeitsprüfungen sind gemäß der Orientierungshilfe des BSI zu Nachweisen gemäß § 8a Abs. 3 BSIG notwendig, um die Erfüllung der Anforderungen aus § 8a Abs. 1 BSIG belegen zu können.

6 Bei der Auftragsart „Prüfung einer Erklärung des Betreibers Kritischer Infrastrukturen über die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ (im Folgenden KRITIS-Erklärung) ist es Ziel der Angemessenheitsprüfung, dem Wirtschaftsprüfer auf Grundlage der durchgeführten Prüfungshandlungen ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob[8]

- die KRITIS-Erklärung der gesetzlichen Vertreter frei von wesentlichen Fehlern ist,
- die in der KRITIS-Erklärung der gesetzlichen Vertreter beschriebenen und vom Betreiber der Kritischen Infrastruktur gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet waren und
  - zu dem zu prüfenden Zeitpunkt implementiert waren.

7 Ziel der Wirksamkeitsprüfung bei dieser Auftragsart ist – über die Angemessenheitsprüfung hinaus – zu beurteilen, ob die in der Erklärung der gesetzlichen Vertreter dargestellten Maßnahmen gemäß § 8a Abs. 1 BSIG in dem zu prüfenden Zeitraum wirksam gewesen sind.[9]

8 Bei der Auftragsart „direkte Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ ist Ziel der Angemessenheitsprüfung, dem Wirtschaftsprüfer auf Grundlage der durchgeführten Prüfungshandlungen ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob[10]

- die vom Betreiber der kritischen Dienstleistung gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet waren, und
  - zu dem zu prüfenden Zeitpunkt implementiert waren.

9 Ziel der Wirksamkeitsprüfung bei dieser Auftragsart ist – über die Angemessenheitsprüfung hinaus – zu beurteilen, ob die gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in dem zu prüfenden Zeitraum wirksam waren.[11]

---

[8] Vgl. *IDW PS 860*, Tz. 15.

[9] Vgl. *IDW PS 860*, Tz. 16.

[10] Vgl. *IDW PS 860*, Tz. 21.

[11] Vgl. *IDW PS 860*, Tz. 22.

10 Die Prüfung wird für Zwecke des Betreibers der kritischen Dienstleistung durchgeführt und der Prüfungsbericht ist zur Information des Betreibers der kritischen Dienstleistung über das Ergebnis der Prüfung bestimmt. Darüber hinaus dient der Prüfungsbericht dem Betreiber der kritischen Dienstleistung dazu, den Nachweis gemäß § 8a Abs. 3 BSIG führen zu können und damit die Erfüllung der Anforderungen des § 8a Abs. 1 BSIG in geeigneter Weise nachzuweisen.

3. Gegenstand der Prüfung

11 Gegenstand der „Prüfung einer Erklärung des Betreibers Kritischer Infrastrukturen über die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ nach diesem *IDW Prüfungshinweis* ist die Erklärung der gesetzlichen Vertreter des Unternehmens über Maßnahmen in Bezug auf die Einhaltung der in Anlage 1 dargestellten Anforderungen.

12 Gegenstand einer „direkten Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ nach diesem *IDW Prüfungshinweis* sind die in der Auftragsvereinbarung abgegrenzten organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse der kritischen Dienstleistungen in Bezug auf die Einhaltung der in Anlage 1 dargestellten Anforderungen.

13 Klarstellend wird darauf hingewiesen, dass die Prüfung der Angemessenheit eines KRITIS-relevanten IT-Systems i.S. dieses *IDW Prüfungshinweises* die Erlangung eines Verständnisses über die KRITIS-relevanten Elemente des IT-Kontrollsystems einschließlich des IT-Risikobeurteilungsprozesses einschließt. Der IT-Risikobeurteilungsprozess des Betreibers Kritischer Infrastrukturen bildet somit die Grundlage für die Feststellung der IT-Risiken, die vom Management im Rahmen des IT-Kontrollsystems und damit i.R. des Informationssicherheitsmanagementsystems für Kritische Infrastrukturen (ISMS) gesteuert werden müssen, auf deren Basis die Folgeabschätzung für maßgebliche Störungen erstellt wird.

4. Kriterien

14 Der in der Anlage 1 enthaltene Anforderungskatalog ist an den Anforderungen ausgerichtet, die sich aus der „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG“[12] ergeben, und basiert auf der „Konkretisierung der Anforderungen an die gemäß §8a Absatz 1 BSIG umzusetzenden Maßnahmen“ des BSI.[13]

15 Die Konkretisierung der Anforderungen an die gemäß §8a Absatz 1 BSIG umzusetzenden Maßnahmen des BSI stellt geeignete Kriterien i.S. des *IDW PS 860*, Tz. 32, für die Beurteilung der von Berteibern kritischer Dienstleistungen getroffenen organisatorischen und technischen Vorkehrungen dar. Liegen weitere einschlägige Branchenstandards des BSI vor, sind diese im Rahmen der Prüfung zu berücksichtigen, in dem der Anforderungskatalog nach diesem *IDW*

[12] Vgl. Version 1.0 vom 01.12.2017 www.bsi.bund.de, Rubrik: Publikationen. (Stand: 24.03.2020).

[13] Vgl. www.bsi.bund.de, Rubrik Publikationen (Stand: 23.03.2020).

Prüfungshinweis ggf. um die branchenspezifischen Besonderheiten zu ergänzen ist. Eine aktuelle Übersicht der veröffentlichten branchenspezifischen Sicherheitsstandards (B3S) ist auf der Webseite des BSI[14] abrufbar. Ferner können sich Ergänzungen des Anforderungskatalogs aufgrund weiterer gesetzlicher oder sonstiger regulatorischer Anforderungen (bspw. Bankaufsichtliche Anforderungen an die IT (BAIT)[15]) ergeben.

5. Besonderheiten bei der Auftragsannahme

5.1. Prüfung einer Erklärung des Betreibers Kritischer Infrastrukturen über die gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen

16 Die angemessene Dokumentation der Maßnahmen zum Aufbau sowie zur Steuerung und Überwachung der gemäß § 8a Abs. 1 BSIG umzusetzenden organisatorischen und technischen Vorkehrungen ist Voraussetzung für deren konsistente Anwendung und personenunabhängige Funktion im Zeitablauf. Die Verantwortung für diese Dokumentation liegt bei den gesetzlichen Vertretern des Betreibers der Kritischen Infrastrukturen. Art und Umfang der Dokumentation hängen wesentlich von der Ausgestaltung der gemäß § 8a Abs. 1 BSIG umzusetzenden organisatorischen und technischen Vorkehrungen ab, die eingerichtet wurden, den Risiken für die Vertraulichkeit, die Integrität oder die Verfügbarkeit der kritischen Dienstleistung zu begegnen.

17 Die Erklärung der gesetzlichen Vertreter über die gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen hat eine Beschreibung der Maßnahmen zu Aufbau und Steuerung sowie zur Überwachung gemäß § 8a Absatz 1 BSIG umzusetzenden organisatorischen und technischen Vorkehrungen zu enthalten, die zur Einhaltung der in Anlage 1 dargestellten Anforderungen nach dem BSIG erforderlich sind. Die Verantwortung für diese Beschreibung liegt bei den gesetzlichen Vertretern des Betreibers der Kritischen Infrastrukturen.

5.2. Direkte Prüfung des Betreibers Kritischer Infrastrukturen über die gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen

18 Die angemessene Dokumentation der Maßnahmen zum Aufbau sowie zur Steuerung und Überwachung der gemäß § 8a Abs. 1 BSIG umzusetzenden organisatorischen und technischen Vorkehrungen ist Voraussetzung für deren konsistente Anwendung und personenunabhängige Funktion im Zeitablauf. Die Verantwortung für diese Dokumentation liegt bei den gesetzlichen Vertretern des Betreibers der Kritischen Infrastrukturen. Art und Umfang der Dokumentation hängen wesentlich von der Ausgestaltung der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen ab, die eingerichtet wurden, den Risiken für die Vertraulichkeit, die Integrität oder die Verfügbarkeit der kritischen Dienstleistung zu begegnen.

19 Die Dokumentation dient dem Wirtschaftsprüfer als Grundlage für die Planung und Durchführung seiner Prüfungshandlungen. Sie muss so beschaffen sein, dass sie die Maßnahmen zum Aufbau sowie zur Steuerung und Überwachung der gemäß § 8a Abs. 1 BSIG umzusetzenden organisatorischen und technischen Vorkehrungen klar, verständlich, vollständig und aktuell

[14] Vgl. www.bsi.bund.de, Rubrik KRITIS (Stand: 24.03.2020).

[15] Vgl. www.bafin.de, Rubrik Rundschreiben (Stand: 24.03.2020).

darstellt. Aus der Dokumentation muss auch die tatsächliche Durchführung der Maßnahmen einschließlich der durchführenden Personen und des Zeitpunkts der Durchführung erkennbar sein.

6. Besonderheiten bei der Durchführung der Prüfung

20 Der *IDW PS 860* legt die Grundsätze für die Planung und Durchführung von Prüfungshandlungen für eine Prüfung der Angemessenheit und – sofern einschlägig – Wirksamkeit fest. Eine Beurteilung der Wirksamkeit hat mindestens einen Prüfungszeitraum von sechs Monaten zu umfassen.

21 Geeignete Maßnahmen zur Einhaltung der Kriterien des § 8a Abs. 1 BSIG sowie Hinweise zur Durchführung der Prüfung können der Anlage 1 entnommen werden. Diese gelten sowohl für die Auftragsart „Prüfung einer Erklärung des Betreibers Kritischer Infrastrukturen über die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ als auch für die Auftragsart „Direkte Prüfung des Betreibers Kritischer Infrastrukturen“.

22 Gemäß Tz. 47 des *IDW PS 860* hat der Wirtschaftsprüfer auf der Grundlage des gewonnenen Verständnisses über das Unternehmen das rechtliche und wirtschaftliche Umfeld und der vom Betreiber der Kritischen Infrastruktur gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen die Risiken für wesentliche Fehler in der KRITIS-Erklärung bzw. die Risiken wesentlicher Mängel in den gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen zu identifizieren und zu beurteilen. Sofern der Wirtschaftsprüfer im Rahmen der Prüfungsdurchführung Nachweise erlangt, die im Widerspruch zu den Prüfungsnachweisen stehen, die Basis für seine ursprüngliche Risikobeurteilung waren, muss er die Risikobeurteilung anpassen und die weiteren geplanten Prüfungshandlungen entsprechend modifizieren. Zudem hat der Wirtschaftsprüfer gemäß Tz. 48 des *IDW PS 860* Prüfungshandlungen zu planen und durchzuführen, um das Prüfungsrisiko auf ein vertretbar niedriges Maß zu reduzieren.

23 Die in der Anlage 1 aufgeführten Prüfungshandlungen sind als Beispiele und nicht als abschließende Aufzählung zu verstehen, da die Festlegung der prüferischen Vorgehensweisen bzw. durchzuführenden Prüfungshandlungen in der Eigenverantwortlichkeit des Wirtschaftsprüfers unter Berücksichtigung der Ergebnisse seiner Risikobeurteilung sowie der notwendigen Prüfungshandlungen als Reaktion auf die beurteilten Risiken liegt.

24 Weitere beispielhafte Prüfungshandlungen ergänzend zu den in der Anlage 1 aufgeführten beispielhaften Prüfungshandlungen sind jeweils auch

- zur Prüfung der Angemessenheit der Maßnahmen die Durchsicht von Unterlagen und Dokumentationen, wie bspw. Richtlinien, Arbeitsanweisungen, Verfahrensanweisungen, Prozessdokumentationen, Verzeichnissen oder Schulungskonzepten, in denen zentrale Vorgaben zur Durchführung, zum Ablauf und zu den Verantwortlichkeiten schriftlich geregelt sind,
- zur Prüfung der Angemessenheit der Maßnahmen die Beurteilung der Unterlagen und Dokumentationen im Hinblick auf ihre regelmäßige Aktualisierung und Aktualität,
- zur Prüfung der Angemessenheit und Wirksamkeit der Maßnahmen die Beurteilung der Unterlagen und Dokumentationen im Hinblick auf ihre Vollständigkeit.

25 Soweit der Wirtschaftsprüfer bereits i.R.d. Angemessenheitsprüfung Risiken wesentlicher Mängel der KRITIS-Erklärung identifiziert, die der Betreiber der Kritischen Infrastruktur nicht identifiziert hat, hat er zu beurteilen, ob ein solches Risiko vorliegt, das seiner Erwartung nach durch das ISMS identifiziert und in der Folgeabschätzung hätte berücksichtigt werden müssen.

26 Hat der Wirtschaftsprüfer bereits anlässlich seiner Prüfungshandlungen zur Beurteilung der Risiken wesentlicher Mängel im ISMS solche wesentlichen Mängel festgestellt, kann er zu dem Ergebnis gelangen, dass sich in diesem Zusammenhang weitere Prüfungshandlungen zur Angemessenheit und Wirksamkeit erübrigen.

7. Besonderheiten bei der Berichterstattung des Wirtschaftsprüfers

27 Der Wirtschaftsprüfer erstellt eine schriftliche Berichterstattung als Prüfungsbericht.

28 Die Berichterstattung über die Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen beinhaltet:

- Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der gemäß § 8a Absatz 1 BSIG von Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen
- Anhang 1 (soweit anwendbar): Erklärung der gesetzlichen Vertreter des Betreibers der Kritischen Infrastrukturen (vgl. Anlage 2 und Anlage 3)
- Anhang 2: Darstellung der durchgeführten Prüfungshandlungen und geprüften Maßnahmen.

Zusätzlich kann als weiterer Anhang die Vollständigkeitserklärung beigefügt werden.

29 Für die Darstellung der geprüften Maßnahmen und der diesbezüglichen Prüfungshandlungen und Ergebnisse im Anhang des Prüfungsberichts (Anhang 2) hat sich der nachfolgende Aufbau in der Praxis bewährt:

<table>
<tr><td colspan="2">Beschreibung der Anforderungen</td></tr>
<tr><td>Darstellung der organisatorischen und technischen Maßnahmen</td><td>Darstellung des Prüfungsumfangs, der Prüfungshandlungen sowie deren Ergebnisse</td></tr>
<tr><td colspan="2">Beurteilung der organisatorischen und technischen Maßnahmen in Hinblick auf ihre Eignung, den Risiken von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme Komponenten oder Prozesse – die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind – zu begegnen.</td></tr>
</table>

30 Laut der Orientierungshilfe zu Nachweisen gemäß § 8a Abs. 3 BSIG sind die vom Prüfer festgestellten Sachverhalte zu jeder geprüften organisatorischen und technischen Maßnahme im Prüfbericht im Rahmen der Darstellung der durchgeführten Prüfungshandlungen und geprüften Maßnahmen (Anhang 2) aufzunehmen. Wird eine Abweichung zu den Anforderungen gemäß § 8a Abs. 1 BSIG festgestellt, handelt es sich aus Sicht des BSI auch immer dann um eine berichtspflichtige Tatsache, wenn eine „geringfügige Abweichung“ vorliegt, d.h. eine Gefährdung bzw. ein Risiko ohne akuten Handlungsbedarf besteht. Berichtspflichtige Tatsachen stellen ein Indiz für eine mangelnde Eignung, Implementierung oder Wirksamkeit der gemäß

§ 8a Abs. 1 BSIG umzusetzenden Maßnahmen dar. Die Feststellung von „schwerwiegenden Abweichungen“ i.S. der Orientierungshilfe zu Nachweisen gemäß § 8a Abs. 3 BSIG stellt ein starkes Indiz für eine mangelnde Eignung, Implementierung oder Wirksamkeit der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen dar und kann damit zu einer Einschränkung des Prüfungsurteils führen.

Anlagen

Anlage 1: Anforderungskatalog zur Konkretisierung der Kriterien des § 8a Abs. 1 BSIG sowie beispielhafte Prüfungshandlungen

Die einzelnen Anforderungen an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) sind in der BSI-Publikation „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“[16] dargestellt.

2.1 Informationssicherheitsmanagementsystem (ISMS)			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
1.	**Managementsystem für Informationssicherheit**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung zum ISMS auf Vollständigkeit, und Konsistenz in Hinblick auf die vorgenannten Anforderungen ● Einsichtnahme in die Erklärung zur Anwendbarkeit (Statement of Applicability) im Hinblick auf Vollständigkeit der kritischen Dienstleistung ● Abgleich der Verfahrensanweisung hinsichtlich Aktualität und Vollständigkeit der Inhalte gemäß des ISO-Standards der 2700x-Reihe sowie der angeforderten Kriterien **Prüfung der Wirksamkeit:** ● Auswertungen von Berichten bezogen auf die Zielerreichung/-abweichung und die regelmäßige Überprüfung und Anpassung der im ISMS definierten Ziele ● Auswertung von Nachweisen über die systematische Nachverfolgung und Beseitigung von erkannten Mängeln und Schwächen entsprechend der Vorgaben der eingesetzten Verfahren und Richtlinien im ISMS.	OIS-01
2.	**Strategische Vorgaben zur Informationssicherheit und Verantwortung der Unternehmensleitung**	Prüfung der Angemessenheit: ● Auswertung, ob die Sicherheitsziele und strategischen Vorhaben in der Informationssicherheitsleitlinie klar definiert sind und Unternehmensziele, Geschäftsprozesse, Gesetze und Verordnungen sowie Bedrohungsumgebung angemessen widerspiegeln	OIS-02

[16] www.bsi.bund.de, Rubrik: Themen (Stand: 31.03.2020).

2.1 Informationssicherheitsmanagementsystem (ISMS)			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Durchsicht der Kommunikationsplanung für alle betroffenen Parteien auf Angemessenheit. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Berichte/Auswertungen bezogen auf die Zielerreichung/-abweichung und die regelmäßige Überprüfung und Anpassung der Sicherheitsziele ● Durchsicht der Freigaben der Unternehmensleitung zur Inkraftsetzung der Informationssicherheitsleitlinie und der sich daraus ableitenden Anweisungen auf Vollständigkeit ● Einsichtnahme in die Dokumentation über die erfolgte Kommunikation mit betroffenen internen/externen Parteien.	
3.	**Zuständigkeiten und Verantwortungen im Rahmen der Informationssicherheit**	**Prüfung der Angemessenheit:** ● Einsichtnahme ins Organigramm ● Einsichtnahme in die Stellenbeschreibungen der Verantwortlichkeiten hinsichtlich der Aufgaben und Verantwortlichkeitsbereiche ● Auswertung der Informationssicherheitsleitlinie hinsichtlich der definierten Rollen zur Informationssicherheit. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Verantwortlichkeiten und Pflichten an die betroffenen internen und externen Parteien kommuniziert wurden.	OIS-03
4.	**Funktionstrennung**	**Prüfung der Angemessenheit:** ● Einsichtnahme ins Organigramm ● Aufnahme und Bewertung der Verfahren, über die Funktionstrennung dokumentiert, vorgegeben und angewiesen wird (z.B. Stellenbeschreibungen, Prozessbeschreibungen, SOD-Matrizen, Berechtigungskonzepte, etc.). **Prüfung der Wirksamkeit:** ● Auswertung der Stellenbeschreibungen hinsichtlich der Aufgaben und Verantwortlichkeitsbereiche	OIS-04

2.1 Informationssicherheitsmanagementsystem (ISMS)			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Auswertung der SoD-Matrizen und Berechtigungskonzepte in Bezug auf die funktionelle und IT-basierte Funktionstrennung ● Einsichtnahme in die Prozessbeschreibungen für Berechtigungsverwaltung hinsichtlich Funktionstrennungsaspekten.	
2.2 Asset Management			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
5.	**Asset Inventar**	**Prüfung der Angemessenheit:** ● Auswertung der Asset Management-Prozessdokumentationen und der Prozeduren zur Erfüllung der Anforderungen hinsichtlich Aktualität, Vollständigkeit, Richtigkeit, Nachvollziehbarkeit und Konsistenz eines Asset Inventars ● Auswertung, ob alle erforderlichen Informationen in der Asset-Management-Datenbankstruktur abgebildet sind. **Prüfung der Wirksamkeit:** ● Nachvollzug der Vollständigkeit und Richtigkeit des Asset Inventars anhand automatisierter Kontrollen bzw. soweit kein automatisiertes Verfahren eingesetzt wird, Nachvollzug der Nachweise über regelmäßige durchgeführte Überprüfung der Asset Inventurdaten.	AM-01
6.	**Zuweisung von Asset Verantwortlichen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Asset Management-Verfahrensanweisung und ● Befragung des Kontrollverantwortlichen im Hinblick auf seine Aufgaben und Verantwortlichkeiten in Bezug auf die inventarisierten Assets. **Prüfung der Wirksamkeit:**	AM-02

2.2 Asset Management			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Nachvollzug, ob eine verantwortliche Person/Rolle in der Asset Management-Datenbank hinterlegt ist.	
7.	**Nutzungsanweisungen für Assets**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Anweisungen zum Umgang mit Assets und Beobachtung der Zugänglichkeit der Richtlinien und Verfahrensanweisungen für Mitarbeiter ● Auswertung der Richtlinien und Anweisungen hinsichtlich Aktualität und Vollständigkeit der Inhalte. **Prüfung der Wirksamkeit:** ● Nachvollzug der in der Verfahrensanweisung definierten Kontrollen für den ordnungsgemäßen Umgang mit Assets.	AM-03
8.	**Ab- und Rückgabe von Assets**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung, die den Mitarbeiteraustritt regeln. **Prüfung der Wirksamkeit:** ● Auswertung, ob für die Mitarbeiter (für die kritischen Dienstleitungen relevante interne & externe Mitarbeiter), die das Unternehmen im Betrachtungszeitraum verlassen haben, eine Überprüfung der Rückgabe von allen Assets stattgefunden hat sowie dokumentiert wurde ● Einsichtnahme in die unterschriebenen und abgearbeiteten Laufzettel bei Beendigung des Beschäftigungsverhältnisses eines Mitarbeiters.	AM-04

2.2 Asset Management			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
9.	**Klassifikation von Informationen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Asset-Management-Prozessdokumentation und zugehörige Arbeitsanweisungen im Hinblick auf Vorgaben zum Klassifizierungsschema von Informationen und Assets. **Prüfung der Wirksamkeit:** ● Nachvollzug der Einhaltung der Klassifizierungsvorgaben im Asset Inventar.	AM-05
10.	**Kennzeichnung von Informationen und Handhabung von Assets**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Asset-Management-Prozessdokumentation und zugehörige Einsichtnahme in die Arbeitsanweisungen für die Umsetzung der Klassifizierung von Informationen und Assets. **Prüfung der Wirksamkeit:** ● Nachvollzug der Kontrollmaßnahmen zur Einhaltung der Klassifizierungsvorgaben im Asset Inventar.	AM-06
11.	**Verwaltung von Datenträgern**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinien und Verfahrensanweisungen hinsichtlich des sicheren Umgangs mit Datenträgern. ● Befragung der Mitarbeiter zur Zugänglichkeit von Richtlinien und Verfahrensanweisungen.	AM-07
12.	**Überführung und Entfernung von Assets**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Asset Management-Prozessdokumentation und zugehörige Arbeitsanweisungen im Hinblick auf Vorgaben zur Überführung und Entfernung von Assets. **Prüfung der Wirksamkeit:** ● Auswertung, ob Transporte und Vernichtungen gemäß Verfahrensanweisung durchgeführt, genehmigt sowie dokumentiert worden sind.	AM-08

2.3 Risikoanalysemethode			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
13.	**Richtlinie für die Organisation des Risikomanagements**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen zum Risikomanagement ● Befragung der Mitarbeiter zur Zugänglichkeit der Richtlinien und Verfahrensanweisungen. **Prüfung der Wirksamkeit:** ● Die regelmäßige Aktualisierung der Richtlinie in Intervallen ist z.B. anhand der Versionierung bzw. anhand von Mailinglisten oder Lesebestätigungen nachzuvollziehen.	OIS-06
14.	**Identifikation, Analyse, Beurteilung und Folgeabschätzung von IT-Risiken**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Risikomanagement-Verfahrensanweisung und Interview mit dem Verantwortlichen insb. zur Folgeabschätzung ● Einsichtnahme in das Risikomanagement-Inventar hinsichtlich der Dokumentation von Informationssicherheits- und IT-Risiken ● Einsichtnahmen in die Festlegungen zum Prozess für eine vollständige Aufnahme von KRITIS-relevanten Risiken und IT-Systemen **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die relevanten Informationssicherheits- und IT-Risiken vorgabegemäß angemessen analysiert, bewertet, dokumentiert und mit entsprechenden Maßnahmen versehen wurden ● Auswahl und Durchsicht der an die Unternehmensleitung gemeldeten Risikoberichte/-reportings, ob diese angemessen und zeitgerecht versandt wurden ● Nachvollzug der Prozesse für eine Erfassung der KRITIS-relevanten Risiken und IT-Systeme.	OIS-07
15.	**Richtlinien zur Folgeabschätzung**	**Prüfung der Angemessenheit:** ● Durchsicht der konzeptionellen Vorgaben hinsichtlich Vollständigkeit und Angemessenheit gemäß den vorgenannten Anforderungen. **Prüfung der Wirksamkeit:**	BCM-02

2.3 Risikoanalysemethode			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Die regelmäßigen Aktualisierungen der Richtlinien und Anweisungen in Intervallen ist nachzuvollziehen (z.B. anhand der Versionierung) ● Die Kenntnisnahme der Richtlinien und Anweisungen kann bspw. anhand von Mailinglisten oder Lesebestätigungen nachvollzogen werden ● Auswertung, ob die Folgeabschätzungen gemäß den Vorgaben durchgeführt wurden.	
16.	**Maßnahmenableitung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinien zur Maßnahmenableitung und Abgleich der getroffenen Regelungen auf Basis der identifizierten IT-Risiken ● Einsichtnahme in die Richtlinien zu Überwachung und Berichtswesen der Maßnahmenumsetzung. **Prüfung der Wirksamkeit:** ● Nachvollzug von Maßnahmen, inwieweit diese zur wirksamen Reduzierung der IT-Risiken beitragen ● Nachvollzug der Überwachung von Maßnahmen und des Berichtswesens für ausgewählte Maßnahmen zur Risikoreduktion.	B3S
2.4 Continuity Management			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
17.	**Verantwortung der gesetzlichen Vertreter des Betreibers der Kritischen Infrastruktur**	**Prüfung der Angemessenheit:** ● Einsicht in Organisationsplan bzw. Prozess-Dokumentationen in Hinblick auf die Einrichtung und Ernennung eines Prozessverantwortlichen ● Befragung der Unternehmensleitung zur Effektivität des Kontinuitäts- und Notfallmanagements ● Einsicht in die Stellenbeschreibung der Prozessverantwortlichen, Notfallmanager. **Prüfung der Wirksamkeit:**	BCM-01

2.4 Continuity Management			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
		● Nachvollzug der Ernennung und Bekanntgabe des Kontinuitäts- und Notfallmanagers.	
18.	**Planung der Betriebskontinuität**	**Prüfung der Angemessenheit**: ● Durchsicht des Rahmenwerks, ob die aus der Folgeabschätzung abgeleiteten Vorkehrungen und Maßnahmen implementiert wurden und konsistent zu den zugrunde gelegten Standards sind. **Prüfung der Wirksamkeit:** ● Nachvollzug der Einhaltung von Verantwortlichkeiten anhand der Inkraftsetzung von (Teil)Plänen ● Analyse ausgewählter Vorgänge, ob diese den relevanten Personenkreis zeitnah erreicht haben ● Nachvollzug von Vorgängen/Incidents ● Verifizierung der Schnittstelle zum Security Incident-Management.	BCM-03
19.	**Verifizierung, Aktualisierung und Test der Betriebskontinuität**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Prozessbeschreibung für die jährliche Aktualisierung sowie der Verfahren zur Identifikation relevanter Umfeldänderungen und Anpassung der Notfallpläne ● Einsichtnahme in die Organisation der Testvorbereitungen und Einsichtnahme in die Dokumentation der Testverfahren in Hinblick auf die Berücksichtigung aller relevanten Schadensszenarien. **Prüfung der Wirksamkeit:** ● Nachvollzug der Aktualisierung von Notfallplänen anhand der Umsetzung ausgewählter Änderungen, welche zu Anpassungen geführt haben ● Nachvollzug der durchgeführten Notfalltests anhand der Testdokumentation.	BCM-04

..

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
20.	**Notwendige/ausreichende Personal- und IT-Ressourcen (Betrieb und IT-Sicherheit)**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Dokumentationen, Richtlinien, Verfahrensanweisungen und Planungen zum Capacity Management (inkl. Überwachungsmaßnahmen) von Personal und IT-Ressourcen ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Auswertung der Überwachungsmaßnahmen auf angemessene Berücksichtigung von Kapazitätsengpässen in der Vergangenheit und Plausibilität der den Prognosen zugrundeliegenden Annahmen ● Auswertung, inwieweit der gemeldete Bedarf zur Vermeidung von Engpässen durch neue Personalressourcen gedeckt wurde (Kennzahlen).	RB-01 RB-02
21.	**Schutz vor Schadprogrammen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahren und eingesetzte Tools hinsichtlich Schutzmaßnahmen vor Schadprogrammen ● Befragung des Kontrollverantwortlichen zur Überprüfung, ob ein Schutz vor Schadprogrammen (z.B. Anti-Viren Schutz) für relevante IT-Systeme vorgesehen ist. **Prüfung der Wirksamkeit:** ● Nachvollzug der Übereinstimmung auf Einhaltung von tatsächlich durchgeführten Routinen/Aktualisierungen von Schutzprogrammen gemäß den definierten Vorgaben (z.B. Einsicht auf Einstellungen von Monitoring Cockpits bzgl. Schadprogrammen) ● Überprüfung auf tägliche Aktualisierung der Virenschutzdefinitionen ● Einsicht in Nachweise zu Monitoringaktivitäten (z.B. Durchsicht und Abzeichnen von Protokollen) und Dokumentation erfolgter Beseitigungsmaßnahmen bei Auftreten von Schadprogrammen.	RB-05

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
22.	**Datensicherung und Wiederherstellung**	**Prüfung der Angemessenheit:** ● Durchsicht der Richtlinie zur Datensicherung und Wiederherstellung, ob vorgenannte Anforderungen umgesetzt wurden ● Interview mit dem Kontrollverantwortlichen zur Implementierung der technischen und organisatorischen Maßnahmen. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob automatisierte IT-Kontrollen zur Sicherung von Daten (Backups) und Wiederherstellung von Daten (Restore) durchgeführt wurden ● Nachvollzug, ob der Zugriff auf die gesicherten Daten auf ein autorisiertes Personal beschränkt ist anhand von Log-files. ● Nachvollzug, ob die auf Sicherungsdatenträgern tatsächlich an einem Remote-Standort transportiert wurden.	RB-06 RB-09
23.	**Datensicherung und Wiederherstellung – Überwachung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinie zur Datensicherung und Wiederherstellung ● Befragung des Kontrollverantwortlichen zur Implementierung sowie Einblick in die Datensicherungssoftware. **Prüfung der Wirksamkeit:** ● Nachvollzug der Maßnahmen zur Überwachung, wie die Einhaltung der Anforderungen in Bezug auf Umfang, Häufigkeit und Dauer der Aufbewahrung sichergestellt wird ● Auswertung der Reaktionen auf Störungen anhand der Log-Dateien und der Dokumentation.	RB-07
24.	**Datensicherung und Wiederherstellung – Regelmäßige Tests**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinie zur Datensicherung und Wiederherstellung ● Durchsicht des Testplans ● Befragung des Kontrollverantwortlichen zur Implementierung der Wiederherstellungsverfahren	RB-08

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
		Prüfung der Wirksamkeit: ● Durchsicht der Nachweise für regelmäßige Tests der Lesbarkeit/Verlässlichkeit der Sicherungsdatenträger ● Durchsicht der Nachweise zu durchgeführten Wiederherstellungstests gemäß den Vorgaben und Richtlinien (bspw. Verfahren und Maßnahmen für Backup- und Recovery Prozeduren) sowie Auswertung von Planabweichungen ● Durchsicht von Nachweisen, ob angemessene Sicherungsträger verwendet werden ● Auswertung, ob die in den Tests aufgetretenen Fehler zeitnah behoben und die Ergebnisse nachvollziehbar dokumentiert wurden.	
25.	**Umgang mit Schwachstellen, Störungen und Fehlern – System-Härtung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung für die Härtung der Systeme oder Sichtung von Härtungsanleitungen für relevante Systeme ● Befragung des Kontrollverantwortlichen, ob relevante Industriestandards den Verfahrensanweisungen zugrunde gelegt wurden. **Prüfung der Wirksamkeit:** ● Einsicht in IT-Systeme und ● Nachvollzug, ob Härtungsanleitungen umgesetzt und dokumentiert sind.	RB-22
26.	**Geheimhaltung von Authentifizierungs-informationen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung zur Zuteilung geheimer Authentifizierungsinformationen ● Befragung des Kontrollverantwortlichen zur Zuteilung von Authentifizierungsinformationen ● Einsichtnahme in die Systemeinstellungen zur Gültigkeit und Änderung von Initialpasswörtern. **Prüfung der Wirksamkeit:** ● Nachvollzug der Kommunikation von Authentifizierungsinformationen	IDM-07

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
		● Nachvollzug der Gültigkeitsdauer von Initialpass-wörtern.	
27.	**Sichere Anmelde-verfahren**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung für das Authentifizierungskonzept. **Prüfung der Wirksamkeit:** ● Einsichtnahme in IT-Systeme, und Nachvollzug, ob die vorgesehenen Authentifizierungsmecha-nismen implementiert sind (z.B. LDAP) und Zu-griff ausschließlich über diese erfolgt.	IDM-08
28.	**Systemseitige Zu-griffskontrolle**	**Prüfung der Angemessenheit:** ● Durchsicht der Verfahrensanweisung für die Um-setzung technischer Maßnahmen zur Zugriffskon-trolle. **Prüfung der Wirksamkeit:** ● Nachvollzug der technischen Umsetzung des Rollen- und Berechtigungskonzepts.	IDM-10
29.	**Passwortanforde-rungen und Validie-rungsparameter**	**Prüfung der Angemessenheit**: ● Durchsicht der Verfahrensanweisung für Pass-worteinstellungen im Hinblick auf die Abdeckung der vorgenannten Anforderungen. **Prüfung der Wirksamkeit:** ● Auswertung und Vergleich der tatsächlich defi-nierten Systemeinstellungen mit den Vorga-ben/Kriterien der entsprechenden Richtlinien.	IDM-11
30.	**Einschränkung und Kontrolle administ-rativer Software**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahrensanwei-sungen, Maßnahmen hinsichtlich des Zugriffs-schutzes auf Managementkonsolen/ administra-tive Software ● Einsichtnahme in die Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen ● Einsichtnahme auf Liste mit Mitarbeitern mit Zu-griffsmöglichkeit auf Managementkonsolen/ admi-nistrative Software.	IDM-12

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
		Prüfung der Wirksamkeit: ● Auswertung und Vergleich des tatsächlich eingestellten Zugriffsschutzes mit den Vorgaben/Kriterien der entsprechenden Richtlinien ● Abgleich der Zugriffs-Logs mit der Liste der autorisierten Personen.	
31.	**Zugriffskontrolle zu Quellcode**	**Prüfung der Angemessenheit:** ● Durchsicht der Verfahrensanweisung für die Aufbewahrung von Quellcode sowie der ergänzenden für die Entwicklung der kritischen Dienstleistung relevanten Informationen. **Prüfung der Wirksamkeit:** ● Nachvollzug des Zugriffsverfahrens auf die identifizierten Systeme, die Quellcode und relevante Informationen beinhalten, und ● Einsichtnahme in die Zugriffsmethoden, ob die Kriterien entsprechend umgesetzt sind.	IDM-13
32.	**Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung**	**Prüfung der Angemessenheit:** ● Durchsicht der Verfahrensanweisung für Verschlüsselungsverfahren ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Nachvollzug der verbindlichen Anweisung und Veröffentlichung der Richtlinie.	KRY-01
33.	**Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung für Verschlüsselungsverfahren für die Übertragung von Daten. **Prüfung der Wirksamkeit:** ● Abgleich der definierten Vorgaben zu technischen Schutzmaßnahmen mit den implementierten Verschlüsselungseinstellungen und Parametern.	KRY-02

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
34.	**Verschlüsselung von sensiblen Daten bei der Speicherung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung für Verschlüsselungsverfahren für die Speicherung von Daten ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben **Prüfung der Wirksamkeit:** ● Identifizieren von sensiblen Daten und Nachvollzug, ob eine Verschlüsselung bei der Speicherung entsprechend umgesetzt ist ● Nachvollzug der Einstellungen bezogen auf die Schlüsselerzeugung, -verteilung und -speicherung (aufgrund der zentralen Bedeutung der Kontrolle könnte der Prüfer einen Codereview als sachgerecht erachten).	KRY-03
35.	**Sichere Schlüsselverwaltung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahrensanweisungen und technische Maßnahmen hinsichtlich sicherer Schlüsselverwaltung ● Durchsicht der Dokumentation hinsichtlich Aktualität, Nachvollziehbarkeit und Vollständigkeit der Inhalte gemäß den angeforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Auswertung der Schlüsselverwaltung, im Hinblick auf die geforderten Aspekte.	KRY-04
36.	**Technische Schutzmaßnahmen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die durchgeführte Risiko-Analyse ● Einsichtnahme in definierte Vorgaben zu technischen Schutzmaßnahmen, um netzwerkbasierte Angriffe zeitnah zu erkennen und darauf zu reagieren und, ob die Schutzmaßnahmen, die aus der Risikoanalyse abgeleitet wurden, vollständig und aktuell sind. **Prüfung der Wirksamkeit:**	KOS-01

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
		● Nachvollzug, ob Systeme wie IDS, IPS, DDoS-Abwehr im Netzwerk für den Schutz vor netzwerkbasierten Angriffen ordnungsgemäß nach den Verfahrensanweisungen in Betrieb sind.	
37.	**Überwachen von Verbindungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahrensanweisungen und technische und organisatorische Maßnahmen zu Netzwerksicherheit ● Einsichtnahme in die Netzwerk-Dokumentation und Review-Prozess von Netzübergängen, Verbindungen (falls vorhanden) und Überwachung von Schutzmaßnahmen ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Auswertung von Firewall- oder Filter-Regeln an Netzübergängen, ob der Verkehr verfahrensgemäß gefiltert, kontrolliert oder blockiert wird.	KOS-02
38.	**Netzwerkübergreifende Zugriffe**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation des Netzwerks (Topologie), der Sicherheitsgateways (falls vorhanden) ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Prüfungen, ob und auf welcher Grundlage für Netzperimeter Firewall-Freischaltungen oder Regeln eingerichtet wurden.	KOS-03
39.	**Netzwerke zur Administration**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation der Managementkonsolen (falls vorhanden), des Netzwerks (Topologie), Administrationskonzepte ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:**	KOS-04

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
		● Nachvollzug, ob der Zugriff bspw. über Multi-Faktor-Authentifizierung möglich ist ● Auswertung der logischen Trennung auf unveränderten Fortbestand der Adressräume während des Betrachtungszeitraums.	
40.	**Dokumentation der Netztopologie**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation der Netztopologie ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben.	KOS-06
41.	**Richtlinien zur Datenübertragung**	**Prüfung der Angemessenheit:** ● Durchsicht der Verfahrensanweisung für Verschlüsselungsverfahren für die Übertragung von Daten ● Interview mit dem Kontrollverantwortlichen zur Klassifikation von Informationen ● Durchsicht der Richtlinien und Verfahren hinsichtlich Aktualität und Vollständigkeit der Inhalte gemäß den angeforderten Kriterien/Vorgaben.	KOS-07
42.	**Vertraulichkeitserklärung**	**Prüfung der Angemessenheit:** ● Durchsicht der Muster- Geheimhaltungs- oder Vertraulichkeitserklärungen ● Durchsicht der Verfahren zu regelmäßigen Anforderungsüberprüfungen ● Durchsicht der Geheimhaltungs- oder Vertraulichkeitserklärungen auf Vollständigkeit der Inhalte gemäß den angeforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Nachvollzug der unterzeichneten Geheimhaltungs- oder Vertraulichkeitserklärungen auf Einhaltung der Vorgaben ● Nachvollzug, ob aufgrund einer regelmäßig erfolgten Überprüfung der Anforderungen im Zusammenhang mit Geheimhaltungs- oder Vertraulichkeitserklärungen eine Anpassung erforderlich	KOS-08

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		machte und dies an die internen und externen Mitarbeiter kommuniziert wurde.	
43.	**Richtlinien zur Entwicklung/Beschaffung von Informationssystemen**	**Prüfung der Angemessenheit:** ● Durchsicht der Inhalte der entsprechenden Richtlinien und Anweisungen inkl. der technischen und organisatorischen Maßnahmen für die ordnungsgemäße Entwicklung und/oder Beschaffung von Informationssystemen für die Entwicklung oder den Betrieb ● Beobachtung der Zugänglichkeit von Richtlinien und Anweisungen für Mitarbeiter/Zielgruppe.	BEI-01
44.	**Auslagerung der Entwicklung**	**Prüfung der Angemessenheit:** ● Durchsicht der Inhalte von Vertragsunterlagen/SLAs zwischen dem Betreiber der kritischen Dienstleistung und externen Dienstleistern. **Prüfung der Wirksamkeit:** ● Nachvollzug der Kontroll- und Überwachungsmaßnahmen für die Abnahme von externen Produkten und Dienstleistungen.	BEI-02
45.	**Richtlinien zur Änderung von Informationssystemen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung für das Change Management in der IT ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben.	BEI-03
46.	**Risikobewertung der Änderungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung für das Change Management in der IT ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Auswertung, ob Risiken bei Änderungen von Systemen im Ticket, Change Request o.ä. erhoben, berücksichtigt und bewertet wurden.	BEI-04

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
47.	**Kategorisierung der Änderungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung für das Change Management in der IT ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Auswertung von Nachweisen über die Kategorisierung einer Änderung basierend auf einer Risikobewertung in Bezug auf die Vorgaben einzuholender Genehmigungen gemäß der Change Management-Richtlinien, Anweisungen und Maßnahmen.	BEI-05
48.	**Priorisierung der Änderungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung für das Change Management in der IT ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Nachvollzug der Kategorisierung von Änderungen basierend auf einer Risikobewertung in Bezug auf die Vorgaben einzuholender Genehmigungen gemäß der Change Management-Richtlinien, -Anweisungen und -Maßnahmen.	BEI-06
49.	**Testen der Änderungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung für das IT Change Management ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Nachvollzug von Änderungen an IT-Systemen und deren Dokumentation in Tickets, Change Logs und Change Request, ob die Änderungen in einer Entwicklungsumgebung vor Produktivsetzung getestet wurden.	BEI-07

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
50.	**Zurückrollen der Änderungen**	**Prüfung der Angemessenheit:** ● Durchsicht der definierten Abläufe/Pläne zum Zurückrollen von Änderungen in Folge von Fehlern oder Sicherheitsbedenken. **Prüfung der Wirksamkeit:** ● Auswertung von Nachweisen zur sachgerechten Umsetzung und Durchführung der Abläufe/Pläne zum Zurückrollen von Änderungen.	BEI-08
51.	**Überprüfen von ordnungsgemäßer Testdurchführung und Genehmigung**	**Prüfung der Angemessenheit:** ● Durchsicht der Dokumentation des Change Management-Verfahrens hinsichtlich der Test- und Abnahmevorgaben sowie Genehmigungsanforderungen im Change Management-Prozess ● Durchsicht von Listen bzw. von Dokumentationen der für Test und Freigabe von Änderungen vorgesehenen und berechtigten Rollen/Gremien. **Prüfung der Wirksamkeit:** ● Durchsicht von Nachweisen über die Durchführung von Tests, Abnahme- und Genehmigungsprozeduren entsprechend der Vorgaben gemäß den eingesetzten Verfahren und Richtlinien im Change Management-Prozess.	BEI-09
52.	**Notfalländerungen**	**Prüfung der Angemessenheit:** ● Durchsicht der Dokumentation des Change Management-Verfahrens hinsichtlich der Vorgaben bei Notfalländerungen im Change Management-Prozess ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Durchsicht von Nachweisen über die Einhaltung von Dokumentations- und Freigabeanforderungen von Notfalländerungen gemäß den Vorgaben/Kriterien der eingesetzten Verfahren und Richtlinien im Change Management-Prozess.	BEI-10

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
53.	**Systemlandschaft**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Betriebsdokumentation, Netztopologien und Dokumentationen, die insb. die Existenz einer getrennten Entwicklung-, Test und Produktivumgebung anzeigt ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die IT-Systeme je nach Verwendungszweck in einer separierten Produktiv- oder Nicht-Produktivumgebung betrieben werden, sowie, ob in der Entwicklungs- oder Testumgebung Dienstleistungen für den produktiven Betrieb bereitgestellt werden ● Auswertung der Protokollierung von Maßnahmen, ob eine Anonymisierung von Produktivdaten in der Test- oder Entwicklungsumgebung stattgefunden hat oder mit zufällig generierten Testdaten gearbeitet wird.	BEI-11
54.	**Funktionstrennung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation des Change Management-Verfahrens hinsichtlich der Funktionstrennung im Change Management-Prozess ● Einsichtnahme in Listen bzw. von Dokumentationen der für Antragsautorisierung, Entwicklung, Test, Freigabe und Migration von Änderungen vorgesehenen und berechtigten Rollen. **Prüfung der Wirksamkeit:** ● Nachvollzug anhand von Nachweisen, ob die Funktionstrennung im Change Management-Prozess gemäß den eingesetzten Verfahren und ergänzenden Dokumentationen durchgeführt wird.	BEI-12
55.	**Richtlinien und Verfahren zur Risikominimierung des Zugriffs über mobile Endgeräte des KRITIS-Betreibers**	**Prüfung der Angemessenheit:** ● Durchsicht der Inhalte der Richtlinien und Verfahrensanweisungen inkl. technischer und organisatorischer Maßnahmen hinsichtlich der ordnungsmäßigen Verwendung mobiler Endgeräte	MDM-01

2.5 Technische Informationssicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Beobachtung der Zugänglichkeit der Richtlinien und Anweisungen für Mitarbeiter/Zielgruppe ● Durchsicht der Richtlinien und Verfahrensanweisungen auf Vollständigkeit der geforderten Aspekte/Kriterien. **Prüfung der Wirksamkeit:** ● Auswertung des Einsatzes mobiler Endgeräte in der Produktivumgebung bzw. im Geschäftsbetrieb auf Einhaltung der Vorgaben der Verfahrensanweisung und IT-Sicherheitsrichtlinien ● Auswertung, ob private mobile Endgeräte in Produktivumgebung oder Geschäftsbetrieb genutzt werden, und ● ob und wie dies mit den Vorgaben der IT-Sicherheitsrichtlinien übereinstimmt.	
2.6 Personelle und organisatorische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
56.	**Einstellung und Sicherheitsüberprüfung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Bewerbungsprozesse- und Richtlinien sowie in die Verfahrensanweisung für Bewerber-/Mitarbeiter-Screening Prozesse ● Interview mit den HR-Verantwortlichen für Screening ● Einsichtnahme in die Vertragsgestaltung für ausgelagerte Screeningprozesse und diesbezügliche Befragung des Kontrollverantwortlichen. **Prüfung der Wirksamkeit:** ● Nachvollzug anhand von Bewerbungsunterlagen (z.B. Personalausweis, CV, Führungszeugnis) und Überprüfung, ob das Screening gemäß Verfahrensanweisung durchgeführt, genehmigt sowie dokumentiert worden ist ● Durchsicht der vertraglichen Vereinbarungen mit spezialisierten Dienstleistern, ob Anforderungen	HR-01

2.6 Personelle und organisatorische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		zu Screeningprozessen dokumentiert sind, und Stichproben, ob diese Prozesse eingehalten wurden.	
57.	**Einstellung und Beschäftigungsvereinbarungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Musterschreiben einer Beschäftigungsvereinbarung hinsichtlich Einhaltung der Vorgaben zur Informationssicherheit ● Einsichtnahme in die Verpflichtungsvereinbarung auf Vollständigkeit (Referenz auf alle einschlägigen Gesetze, Vorschriften und Regelungen). **Prüfung der Wirksamkeit:** ● Nachvollzug, ob Verpflichtungsvereinbarungen vor Zugriff auf die kritische Dienstleistung unterschrieben wurden und ob die Sicherheitsleitlinie sowie die davon abgeleiteten Richtlinien und Anweisungen zur Informationssicherheit beigefügt wurden.	HR-02
58.	**Rollenzuweisung und Vieraugenprinzip oder Funktionstrennung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Rollen- und Rechtekonzept sowie Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen in Bezug auf Vollständigkeit, Genehmigungen und Dokumentation sowie der Verwaltung von Zugangs- und Zugriffsberechtigungen. **Prüfung der Wirksamkeit:** ● Interview mit dem Kontrollverantwortlichen zur Erläuterung des Berechtigungsaufbaus, der Funktionstrennungen und des Berechtigungsentzugs ● Inaugenscheinnahme, ob das Rollen- und Rechtekonzept sowie die Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen kommuniziert wurde und bereitgestellt ist.	IDM-01
59.	**Identitäts- und Berechtigungsmanagement – Benutzerregistrierung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Regelungen und Verfahren zur Benutzerregistrierung	IDM-02

2.6 Personelle und organisatorische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Interview mit dem Kontrollverantwortlichen zur Erläuterung der Antragswege, Authentifizierungsgrundsätze und des Loggings. **Prüfung der Wirksamkeit:** ● Nachvollzug anhand von Benutzerkennungen, ob Anforderungen des Rollen- und Rechtekonzepts sowie die Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen umgesetzt werden und ob dabei eindeutige Kennungen genutzt werden. ● Auswertung der Verwendung von Mehrbenutzer-Userkennungen und des Prozesses zur Identifizierung von Personen.	
60.	**Identitäts- und Berechtigungsmanagement – Zugriffsberechtigung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Berechtigungskonzept unter Berücksichtigung der vorgenannten Anforderungen ● Befragung des Kontrollverantwortlichen. **Prüfung der Wirksamkeit** ● Nachvollzug anhand neu angelegter oder geänderter Zugriffsberechtigungen und Rollen, ob die vorgenannten Anforderungen umgesetzt wurden ● Auswertung von Zugriffsberechtigungen, ob Anforderungen der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen umgesetzt werden und ob alle Berechtigungen lückenlos dokumentiert sind ● Auswertung der Berechtigungen auf Least-Privilege-Prinzip und Need-to-know-Prinzip und ob technische Zugriffsberechtigungen mit den formal genehmigten übereinstimmen.	IDM-03
61.	**Vergabe und Änderung (Provisionierung) von Zugriffsberechtigungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Regelungen und Verfahren zur Vergabe und Änderung von Zugriffsberechtigungen ● Einsichtnahme in die Dokumentation bei der Vergabe und Änderung von Zugriffsberechtigungen	IDM-04

2.6 Personelle und organisatorische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Auswertung von Zugriffsberechtigungen, ob Anforderungen der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen umgesetzt werden und ob alle Berechtigungen lückenlos dokumentiert sind.	
62.	**Identitäts- und Berechtigungsmanagement – Überprüfungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in relevante Dokumentationen des Rollen- und Rechtekonzepts sowie der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen im Hinblick auf eine regelmäßige Überprüfung der Zugriffsberechtigungen (Benutzerinventur) und der Liste der für die Benutzer- und Berechtigungsinventur zuständigen Personen (inkl. weitreichende/kritische Berechtigungen). **Prüfung der Wirksamkeit:** ● Nachvollzug, ob eine angemessene Benutzerinventur durchgeführt wurde sowie die daraus abgeleiteten Berechtigungsanpassungen anhand relevanter Kriterien/Vorgaben erfolgt ● Abgleich der identifizierten Berechtigungsanpassungen mit im System tatsächlich abgebildeten Benutzerberechtigungen.	IDM-05
63.	**Identitäts- und Berechtigungsmanagement – Administratoren**	**Prüfung der Angemessenheit:** ● Einsichtnahme in relevante Dokumentationen des Rollen- und Rechtekonzepts sowie der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen im Hinblick auf Administrator-berechtigungen. Prüfung, ob eine personalisierte und für die Aufgabenwahrnehmung notwendige Zuweisung vorgesehen ist ● Durchsicht der Richtlinien, Verfahrensanweisungen, Maßnahmen und entsprechenden Dokumentationen hinsichtlich Aktualität und Vollständigkeit der Inhalte gemäß den angeforderten Kriterien/Vorgaben	IDM-06

2.6 Personelle und organisatorische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Einsicht in etablierte kompensierende Kontrollen. Diese Kontrollen sollten so gestaltet sein, dass weitreichende Berechtigungen sie nicht außer Kraft setzen oder umgehen können (Löschen von Protokollen, außer Kraft setzen von Protokollierungsflags). **Prüfung der Wirksamkeit:** ● Abgleich der Mitarbeiter in der Liste aller User mit weitreichenden/kritischen Berechtigungen (bspw. Super-, System-, Admin-, Notfall-User) sowie Liste der Mitarbeiter, die direkten Zugriff auf Anwendungen, Betriebssystem- und Datenbankebene haben mit den in den Anwendungen, Betriebssystem und Datenbanken enthaltenen Administratorberechtigungen ● Nachvollzug von kompensierenden Kontrollen, wie bspw. eine Protokollierung des Zugriffs von weitreichenden Berechtigungen.	
64.	**Identitäts- und Berechtigungsmanagement – Notfallbenutzer**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Regelungen und Verfahren zu Notfallbenutzern ● Einsichtnahme in die Systemeinstellung hinsichtlich der Protokollierung von Notfallbenutzern ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Auswertung von Nachweisen zum Einsatz von Notfallbenutzern hinsichtlich der Einhaltung der angeforderten Vorgaben sowie erteilten Genehmigungen ● Abgleich zwischen den erfolgten Freischaltungen der Notfallbenutzer und den entsprechend durchgeführten Genehmigungen.	IDM-09
65.	**Festlegung notwendiger Kompetenzen (Betrieb und IT-Sicherheit)**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinienpyramide, um alle von der Sicherheitsleitlinie abgeleiteten Richtlinien und Anweisungen zur Informationssicherheit oder verwandter Themen zu identifizieren	SA-01

2.6 Personelle und organisatorische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Einsichtnahme in Stellenbeschreibungen, Tätigkeitsbeschreibungen und Anforderungen an die Qualifikation des Personals für Betrieb und IT-Sicherheit ● Einsichtnahme in Regelungen zu Vertretungen. **Prüfung der Wirksamkeit:** ● Auswertung des Genehmigungs- und Umsetzungsprozesses von Vertretungsregelungen ● Abgleich von ausgewählten Stellenbeschreibungen und Qualifikationsanforderungen mit Bewerbungsunterlagen der Mitarbeiter.	
66.	**Überprüfung und Freigabe von Richtlinien und Anweisungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung zur Überprüfung und Freigabe von Richtlinien und Anweisungen in Bezug auf angemessenen Umfang und Frequenz der Überprüfung ● Beurteilung der fachlichen Qualifikation der für die Überprüfung der Richtlinie vorgesehenen Fachkräfte durch Einsichtnahme in Schulungspläne und erworbene Qualifikationen. **Prüfung der Wirksamkeit:** ● Auswertung von Nachweisen über die jährlich erfolgte Überprüfung der Richtlinien und Anweisungen zur Informationssicherheit und auf die Einhaltung der Anforderungen zur Qualifikation der Prüfer sowie Vorgaben zu den Inhalten der Überprüfung. ● Auswertung von Nachweisen über die angemessene Freigabe von Richtlinien und Anweisungen zur Informationssicherheit nach jährlich erfolgter Überprüfung.	SA-02
67.	**Abweichungen von bestehenden Richtlinien und Anweisungen**	**Prüfung der Angemessenheit:** ● Auswertung des Prozesses zur Erfassung und Genehmigung von Ausnahmen für Richtlinien und Anweisungen auf Zeitnähe, Angemessenheit, Dokumentation und Vollständigkeit ● Beurteilung der fachlichen Qualifikation der für die Überprüfung der Richtlinie vorgesehenen	SA-03

2.6 Personelle und organisatorische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		Fachkräfte durch Einsichtnahme in Schulungspläne und erworbene Qualifikationen. **Prüfung der Wirksamkeit:** ● Auswertung von Listen bzw. von Dokumentationen der für die Freigabe von überarbeiteten Richtlinien und Anweisungen vorgesehenen Rollen/Gremien ● Durchsicht von Nachweisen über die angemessene Freigabe von Ausnahmen nach jährlich erfolgter Überprüfung.	
68.	**Schulungen und Awareness**	**Prüfung auf Angemessenheit:** ● Einsichtnahme in die Inhalte, Verfahren (inkl. Verfahren zum Aktualisierungsprozess bei Änderungen und Anpassungen des Programms) Schulungsunterlagen und Tools zum Programm der Sicherheitsausbildung und Sensibilisierung zum Thema Informationssicherheit. **Prüfung auf Wirksamkeit:** ● Durchsicht von Nachweisen zur Ausrollung des Programms der Sicherheitsausbildung und Sensibilisierung zum Thema Informationssicherheit ● Auswertung durchgeführter Trainings bei Auftreten sicherheitsrelevanter Ereignisse ● Nachvollzug von Mitarbeiterbestätigungen zu Programmmaßnahmen (z.B. Teilnahme an Schulungen).	HR-03
69.	**Disziplinarverfahren**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Prozessdokumentation zur Durchführung von Disziplinarmaßnahmen. **Prüfung der Wirksamkeit:** ● Nachvollzug, anhand von festgestellten Disziplinarverstößen, ob die Disziplinarmaßnahme dokumentiert und an die Mitarbeiter kommuniziert wurde.	HR-04

2.6 Personelle und organisatorische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
70.	**Beendigung des Beschäftigungsverhältnisses**	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Musterschreiben einer Beschäftigungsvereinbarung oder sonstige Vereinbarungen hinsichtlich Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen in Bezug auf Informationssicherheit ● Durchsicht, ob ein Passus enthalten ist, dass die Vorgaben auch bei Wechsel der Stelle oder einem Unternehmensaustritt weiter einzuhalten sind. **Prüfung der Wirksamkeit:** ● Auswertung von Arbeitnehmerverträgen auf Vertraulichkeitsvereinbarungen und Verpflichtung zur Einhaltung der Informationssicherheitsrichtlinie sowie der entsprechenden Gesetze und sonstigen Vorschriften.	HR-05
2.7 Bauliche/physische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
71.	**Rechenzentrumsversorgung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die konzeptionellen Vorgaben, ob alle Vorgaben, die für die Versorgungssicherheitsziele notwendig sind, berücksichtigt wurden ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben ● Einsicht in die Vorgaben des Wartungsplans auf Basis der Herstellerempfehlungen ● Einsicht in den Testplan für die Sicherungsmaßnahmen zur Versorgungssicherheit. **Prüfung der Wirksamkeit:** ● Nachvollzug der Kontrollmaßnahmen in Bezug auf die notwendigen Versorgungsleistungen der für die kritische Dienstleistung notwendigen IT-Systeme	BCM-05

2.7 Bauliche/physische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Nachvollzug der Tests der notwendigen Versorgungsleistungen für den Betrieb der kritischen Dienstleistung ● Nachvollzug der Ausfallsicherungen/Redundanzversorgung ● Nachvollzug der Einhaltung der Wartungsvorgaben und der Wartungsqualität.	
72.	**Perimeterschutz**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Risikoanalyse und Dokumentationen hinsichtlich physischer Sicherheit und Schutzmaßnahmen von Räumlichkeiten, Gebäuden und Systemen (z.B. Physical Security Governance Framework falls vorhanden). **Prüfung der Wirksamkeit:** ● Begehung von Gebäuden und Räumlichkeiten (inkl. Zuhilfenahme einer Checkliste) in Bezug auf Übereinstimmung mit den definierten Verfahren und Maßnahmen in den entsprechenden Dokumentationen sowie mit dem aktuellen Stand der Technik.	PS-01
73.	**Physischer Zutrittsschutz**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Dokumentationen zu physischer Sicherheit von Daten und Informationssystemen bzgl. Vollständigkeit, Aktualität, Schutzmaßnahmen gegen unbefugten Zugang zu Räumlichkeiten und Gebäuden inklusive Monitoring-Kontrollen (z.B. Kameraüberwachung oder Auswertung von Zugangsprotokollen von Türen sowie Verfahren zur Beantragung und Genehmigung von physischem Zutritt). **Prüfung der Wirksamkeit:** ● Vergleich auf Übereinstimmung der tatsächlichen Zutrittskontrollen mit den definierten Verfahren und Maßnahmen in den entsprechenden Dokumentationen ● Durchsicht von Listen der Mitarbeiter, die relevante Serverräume betreten dürfen sowie Durch-	PS-02

2.7 Bauliche/physische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		sicht von Nachweisen, dass diese Listen regelmäßig auf deren Vollständigkeit, Inhalte und Aktualität überprüft werden ● Auswertung von Nachweisen über die Überprüfung von Zugangsprotokollen von Türen.	
74.	**Schutz vor Bedrohungen von außen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Ausgangsanalyse für die Einrichtung von Brandabschnitten und der Festlegung der notwendigen Materialien und Bauausführungen ● Durchsicht der Ausgangsanalyse zu Anzahl und Positionierung von Sensoren und Meldeanlage sowie deren Vernetzung ● Einsichtnahme in Desaster Recovery Plan/Notfallkonzept in Bezug auf Berücksichtigung der Mindestmaßnahmen ● Einsichtnahme in die Schulungskonzepte, Planung der Brandschutzübungen. ● Inaugenscheinnahme der baulichen Umsetzung von z.B. den Brandabschnitten, Funktionsfähigkeit der Sensoren, des Weitermeldungsprozesses (alternativ: durch Nachweis eines durchgeführten Tests) **Prüfung der Wirksamkeit:** ● Einsichtnahme in die IT-Anwendung der Zutrittsschutzsteuerung über den Prüfungszeitraum, wer Zutritt in das Rechenzentrum hatte ● Einsichtnahme in Aufzeichnungen der Temperatur- und Luftfeuchtigkeitssensoren.	PS-03

2.7 Bauliche/physische Sicherheit			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
75.	**Schutz vor Unterbrechungen durch Stromausfälle und andere derartige Risiken**	**Prüfung der Angemessenheit:** ● Durchsicht der Ausgangsanalyse zur Mindestversorgungsleistung außerhalb der Normallage, um die kritische Dienstleistung aufrecht zu erhalten ● Analyse der daraus abgeleiteten Maßnahmen zur Aufrechterhaltung der Versorgungsleistung außerhalb der Normallage. **Prüfung der Wirksamkeit:** ● Nachvollzug von durchgeführten Simulationen/Test von Ausfallsituationen ● Begehung von Gebäuden und Räumlichkeiten in Bezug auf Übereinstimmung mit den definierten Verfahren und Maßnahmen in den entsprechenden Dokumentationen.	PS-04
76.	**Wartung der Infrastruktur**	**Prüfung der Angemessenheit:** ● Einsichtnahme in den Wartungsplan und Wartungsrichtline (insb. Fernwartung) unter Berücksichtigung der vorgenannten Anforderungen. **Prüfung der Wirksamkeit:** ● Nachvollzug der tatsächlichen Umsetzung von Vorgaben des Wartungsplans ● Auswertung der Bestätigungen der Kenntnisnahme der Richtlinien bzw. deren Änderungen durch die Dienstleister und dem externen Personal.	PS-05
2.8 Vorfallserkennung und -bearbeitung			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
77.	**Verantwortlichkeiten und Vorgehensmodell**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinie und Verfahrensanweisungen, ob vorgenannte Vorgaben umgesetzt wurden	SIM-01

2.8 Vorfallserkennung und -bearbeitung			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
		● Nachvollzug der Besetzung der Teammitglieder zur Behandlung von Informationssicherheitsvorfällen ● Interview mit dem Kontrollverantwortlichen, ob eine Erkennung von Informationssicherheitsvorfällen durchgeführt wurde und diese gemäß den definierten Kommunikationswegen kommuniziert wurden. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Rollen laut Informationssicherheitsrichtlinie besetzt sind ● Nachvollzug, ob der Prozess zur Meldung von Informationssicherheitsvorfällen bekannt ist.	
78.	**Bearbeitung von Sicherheitsvorfällen**	**Prüfung der Angemessenheit:** ● Einsichtnahme ins Vorgehensmodell sowie in relevante Konzepte, Richtlinien, Verfahrensanweisungen und Maßnahmen zum Umgang mit Security Incidents. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Dokumentation von ausgewählten Informationssicherheitsvorfällen zur Überprüfung, ob diese klassifiziert und priorisiert wurden, an das Management kommuniziert wurden und Maßnahmen getroffen wurden, um diese Vorfälle in Zukunft zu vermeiden.	SIM-03
79.	**Dokumentation und Berichterstattung über Sicherheitsvorfälle**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Informationssicherheitsrichtlinie ● Interview mit dem Kontrollverantwortlichen in Hinblick auf die Implementierung der Vorkehrungen und Maßnahmen. **Prüfung der Wirksamkeit:** ● Nachvollzug meldepflichtiger Sicherheitsvorfälle, ob der Sicherheitsvorfall gemäß den Vorgaben aus § 8b (4) BSI Gesetz unverzüglich an das BSI gemeldet wurde.	SIM-04

2.8 Vorfallserkennung und -bearbeitung			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
80.	**Security Incident Event Management**	**Prüfung der Angemessenheit:** ● Einsichtnahme ins Vorgehensmodell sowie in relevante Konzepte, Richtlinien, Verfahrensanweisungen und Maßnahmen zum Umgang mit Security Incidents ● Nachvollzug, ob eine zentrale Aggregation und eine Mustererkennung vorgesehen sind. **Prüfung der Wirksamkeit:** ● Auswertung der Einhaltung der definierten Regeln des Security Incident Management-Prozesses zur Erkennung von Beziehungen von Vorfällen und der Beurteilung gemäß deren Kritikalität.	SIM-05
81.	**Verpflichtung der Nutzer zur Meldung von Sicherheitsvorfällen an eine zentrale Stelle**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Sensibilisierungsmaßnahmen hinsichtlich der Verpflichtung von Mitarbeitern und Geschäftspartnern zur zeitnahen Meldung von Sicherheitsereignissen ● ggf. Einsichtnahme in vertraglich festgelegte Klauseln ● Einsichtnahme in die Planung von Kommunikationsmaßnahmen. **Prüfung der Wirksamkeit:** ● Nachvollzug des Inhalts der erfolgten Kommunikation gemäß den Vorgaben (z.B. Nennung der zentralen Stelle zur Meldung von Sicherheitsvorfällen).	SIM-06
82.	**Auswertung und Lernprozess**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung zur Messung, Meldung, Überwachung und Auswertung von Sicherheitsvorfällen, ob ein Prozess zur Evaluierung von erweiterten Schutzmaßnahmen vorgesehen ist ● Einsichtnahme in Auswertungen sowie „Lessons Learned“ und daraus abgeleitete Maßnahmenpläne für zukünftig wiederkehrende Vorfälle.	SIM-07

2.9 Überprüfung im laufenden Betrieb			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
83.	**Anlassbezogene Prüfungen – Konzept**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Informationssicherheitsrichtlinie und Anweisungen mit technischen und organisatorischen Maßnahmen zur Identifikation und Analyse von Schwachstellen und Nachhalten von Maßnahmen.	RB-17
84.	**Umgang mit Schwachstellen, Störungen und Fehlern – Prüfung offener Schwachstellen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in relevante Richtlinien, Verfahrensanweisungen sowie Maßnahmen zum Umgang mit Schwachstellen, Störungen und Fehlern ● Einsichtnahme in die verwendeten Quellen (z.B. Herstellerinformationen, BSI Informationen) ● Einsichtnahme in Regelungen zur Häufigkeit und Verantwortlichkeit der Durchführung. **Prüfung der Wirksamkeit:** ● Nachvollzug der Systemnachweise zu automatisch durchgeführten Überprüfungen der bekannten Schwachstellen ● Überprüfung der Aktualität der Informationsquellen für bekannte Schwachstellen ● Überprüfung der Häufigkeit der Durchführung von Schwachstellenanalysen anhand der systemseitigen und analogen Dokumentation ● Nachvollzug von dokumentierten Prozessen bei erkannten Abweichungserkennungen von der erwarteten Konfiguration oder bei sicherheitsrelevanten Anomalien.	RB-21
85.	**Informieren der Unternehmensleitung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Vorgaben des Prozesses zu den Sicherheitsprüfungen und den entsprechenden Berichts- und Kommunikationsanforderungen. **Prüfung der Wirksamkeit:** ● Einsicht in Nachweise über die durchgeführten Sicherheitsprüfungen	SPN-01

2.9 Überprüfung im laufenden Betrieb			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Auswertung von Nachweisen zur zeitnahen Behebung von daraus hervorgegangenen Feststellungen.	
86.	**Interne Überprüfungen der Compliance von IT-Prozessen mit internen Informationssicherheitsrichtlinien und Standards**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Vorgaben, Richtlinien, Standards sowie der für die kritische Dienstleistung relevanten rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen zur Überprüfung der Compliance der internen IT-Prozesse. ● Einsichtnahme des Kontroll- und Überwachungskonzepts. **Prüfung der Wirksamkeit:** ● Auswertung der Ergebnisdokumentation der jährlich durchgeführten Compliance Prüfung der internen IT-Prozesse inkl. Dokumentation der identifizierten Abweichungen und Maßnahmenplan zur zeitnahen Behebung ● Einsichtnahme in die Dokumentation zum Nachweis der implementierten Maßnahmen zur Beurteilung der Feststellungen.	SPN-02
87.	**Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen – interne IT-Prüfungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die dokumentierten Regelungen und Prozesse sowie die festgelegten Zeitintervalle für interne IT-Prüfungen ● Einsichtnahme in Prozessvorlagen (z.B. für die Dokumentation der Auditdurchführung oder Auditberichte) ● ggf. Einsichtnahme in Vereinbarungen mit Unterauftragnehmern. **Prüfung der Wirksamkeit:** ● Auswertung der bisherigen Auditreports und weiteren Audit-Dokumente ● Einsichtnahme in die erhobenen Feststellungen ● Nachvollzug des Prozesses zur Behebung von Feststellungen ● Auswertung, ob Feststellungen aus bisherigen Audits mit Korrekturmaßnahmen behoben wurden.	SPN-03

2.9 Überprüfung im laufenden Betrieb			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
88.	**Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen – Planung externer Audits**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Regelungen zur Planung externer Audits zur Sicherstellung der Integrität, Vertraulichkeit und Authentizität der Daten und der Verfügbarkeit der kritischen Dienstleistung, IT und Komponenten ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Durchsicht der Berechtigungsprozesse für externe Auditoren (Lese- und Schreibrechte) auf kritische Dienstleistung und Daten ● Nachvollzug, ob Aktivitäten identifiziert wurden, die die Verfügbarkeit der IT oder Komponenten beeinträchtigen und so zu Beeinträchtigungen der Verfügbarkeit der kritischen Dienstleistung führen könnten ● Auswertung, ob es Regelungen im Umgang mit den o.g. Aktivitäten gibt (insb. hinsichtlich der Durchführung außerhalb regulärer Geschäftszeiten).	COM-02
89.	**Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen – Durchführung externer Audits**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Protokolle von Aktivitäten bisher durchgeführter externer Audits ● Einsichtnahme in Verträge mit externen Auditoren. **Prüfung der Wirksamkeit:** ● Nachvollzug organisatorischer und technischer Vorkehrungen für externe Audits ● Auswertung der bisherigen Berechtigungen externer Auditoren (Lese- und Schreibrechte) auf kritische Dienstleistungen und Daten ● Auswertung der Durchführungsintervalle von externen Audits ● Einsichtnahme in bisherige Auditreports und weitere Audit-Dokumente ● Einsichtnahme in die erhobenen Feststellungen ● Nachvollzug des Prozesses zur Behebung von Feststellungen	COM-03

2.9 Überprüfung im laufenden Betrieb			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
		● Auswertung, ob Feststellungen aus bisherigen Audits mit Korrekturmaßnahmen behoben wurden.	
90.	**Systematische Log-Auswertung – Konzept**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinien und Anweisungen zur Log-Auswertung von für den Betrieb der kritischen Dienstleistung notwendigen Assets ● Interview mit Kontroll-verantwortlichen und den Datenschutzbeauftragten. **Prüfung der Wirksamkeit:** ● Nachvollzug der Angemessenheit und Vollständigkeit der Richtlinien (u.a. Aufbewahrung von Log-Daten) ● Auswertung von Log-Daten (z.B. An- und Abmeldevorgänge, Erstellung/Änderung/Löschung von Benutzern) ● Auswertung der Durchführungsintervalle von Protokollierungen ● Nachvollzug der Einhaltung datenschutzrechtlicher Anforderungen.	RB-10 RB-14
91.	**Systematische Log-Auswertung – kritische Assets**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Risikoanalyse zur Identifizierung aller protokollierungs- und überwachungskritischen Assets ● Einsichtnahme in die Liste aller protokollierungs- und überwachungskritischen Assets ● Einsichtnahme in die definierten erweiterten Protokollierungs- und Überwachungsmaßnahmen für kritische Assets. **Prüfung der Wirksamkeit:** ● Nachvollzug der dokumentierten Verantwortlichkeiten zur Aktualisierung der Liste kritischer Assets ● Nachvollzug der Umsetzung der definierten Protokollierungs- und Überwachungsmaßnahmen für kritische Assets	RB-12

2.9 Überprüfung im laufenden Betrieb			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
		● Nachvollzug anhand von systemgenerierten Nachweisen/Screenshots, die belegen, dass kritische Assets erweiterten Protokollierungs- und Überwachungsmaßnahmen unterlegen haben.	
92.	**Systematische Log-Auswertung – Aufbewahrung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren zum Thema Durchführung und Management der Protokollierung von Assets, welche im Zusammenhang mit der Entwicklung oder dem Betrieb der kritischen Dienstleistung verwendet werden ● Einsichtnahme in entsprechende Dokumentationen/Listen, auf welche Personen der Zugriff auf die zentralen Protokollierungs-server beschränkt ist, und ob dies angemessen ist ● Einsicht in die Maßnahmen zur Trennung der Übertragung von Nutz- und Protokolldaten entsprechend des Schutzbedarfs. **Prüfung der Wirksamkeit:** ● Nachvollzug der „Durchgängigkeit der Authentisierung“ über den Prüfungszeitraum durch Einsichtnahme in die entsprechenden Systemparameter und Änderungslogs ● Nachvollzug der durchgängigen logischen/physischen Trennung von Protokoll- und Nutzdaten in Abhängigkeit des Schutzbedarfs.	RB-13
93.	**Systematische Log-Auswertung – Konfiguration**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Vorgaben zum Zugriff und der Verwaltung von Protokollierungs- und Überwachungsfunktionalitäten ● Einsichtnahme in Berechtigungen für Zugriff und Verwaltung von Protokollierungs- und Überwachungsfunktionalitäten. **Prüfung der Wirksamkeit:** ● Nachvollzug des Änderungsprozesses (u.a. Genehmigungen) für Protokolldaten- und Überwachungsdaten ● Nachvollzug der Umsetzung einer Multi-Faktor-Authentifizierung beim Zugriff und der Verwaltung	RB-15

2.9 Überprüfung im laufenden Betrieb			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grund-lage (C5 #)
		der Protokollierungs- und Überwachungsfunktionalitäten ● Systemseitige Auswertung von Zugriffs-/Änderungsberechtigungen von Mitarbeitern.	
94.	**Systematische Log-Auswertung – Verfügbarkeit**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Regelungen zur Verfügbarkeit der Protokollierungs- und Überwachungssoftware sowie der Nutzung redundanter Software. **Prüfung der Wirksamkeit:** ● Auswertung, ob Protokollierungs- und Überwachungssoftware redundant vorhanden ist und wie schnell die Verfügbarkeit wieder gewährleistet wird ● Einsichtnahme in Dokumentation bei bisherigen Ausfällen oder von Übungen/Tests zum Ausfall der Protokollierungs- und Überwachungssoftware ● Nachvollzug der Verantwortlichkeiten und Meldewege bei Ausfall von Protokollierungs- und Überwachungssoftware.	RB-16
95.	**Penetrationstest**	**Prüfung der Angemessenheit:** ● Einsichtnahme in dokumentierte Testmethodik von Penetrationstests ● Einsichtnahme in Regelungen und Durchführungsintervalle für Penetrationstests. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Bescheinigungen und Prüfberichte von durchgeführten Penetrationstests ● Auswertung, ob die bisherigen Penetrationstests regelmäßig durchgeführt wurden und die für den sicheren Betrieb der kritischen Dienstleistung als kritisch definierten Infrastruktur-Komponenten abdecken ● Nachvollzug der Vorgehensweise zur Behebung von Feststellungen mit mindestens mittlerer bis sehr hoher Kritikalität in Bezug auf die Vertraulichkeit, Integrität oder Verfügbarkeit der kritischen Dienstleistung	RB-18

2.9 Überprüfung im laufenden Betrieb			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
		● Nachvollzug bisheriger Korrektivmaßnahmen für Feststellungen aus vorangegangenen Penetrationstests.	
96.	**Umgang mit Schwachstellen, Störungen und Fehlern – Integration mit Änderungs- und Incident-Management**	**Prüfung auf Angemessenheit:** ● Beobachtung der Zugänglichkeit von Richtlinien und Verfahrensanweisungen für Mitarbeiter ● Einsicht in die relevanten Richtlinien, Verfahrensanweisungen und Dokumentationen zum Change Management ● Abgleich der Konsistenz der definierten Maßnahmen im Change Management, Problem und Incident Management mit der Vorgehensweise im Falle von Störungen und Fehlern.	RB-19
2.10 Externe Informationsversorgung und Unterstützung			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
97.	**Kontakt zu relevanten Behörden und Interessenverbänden**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinie für den Kontakt mit relevanten Behörden und Interessensverbänden ● Interview mit dem Verantwortlichen für die entsprechenden Kommunikationsverfahren. **Prüfung der Wirksamkeit:** ● Einsichtnahme von Protokollen zum Austausch mit Behörden und Interessenverbänden und Umsetzung ggf. empfohlener Maßnahmen.	OIS-05

2.11 Lieferanten, Dienstleister und Dritte			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	**Beispielhafte Prüfungshandlungen**	Grund-lage (C5 #)
98.	**Richtlinie zum Umgang mit und Sicherheitsanforderungen an Dienstleister des KRITIS-Betreibers**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinie ● Befragung des Kontrollverantwortlichen in Bezug auf die geforderten Kriterien/Vorgaben ● Durchsicht der Prozessdokumentation zur Aktualisierung der Sicherheitsanforderungen an Dienstleister. **Prüfung der Wirksamkeit:** ● Auswertung von Verträgen bzw. Vereinbarungen mit Dienstleistern, ob diese den Anforderungen des KRITIS-Betreibers entsprechen ● Auswertung erfolgter Aktualisierungen der Sicherheitsanforderungen an Dienstleister.	DLL-01
99.	**Kontrolle der Leistungserbringung und der Sicherheitsanforderungen an Dienstleister und Lieferanten des KRITIS-Betreibers**	**Prüfung der Angemessenheit:** ● Einsichtnahme in SLA Reportings sowie Dienstleistungsreportings ● Einsichtnahme in Reportings (z.B. zu sicherheitsrelevanten Vorfällen, Betriebsstörungen, Ausfällen etc.) ● Durchsicht der Planung zur Überprüfung, ob die in der Anforderung beschriebenen Maßnahmen vorhanden waren. **Prüfung der Wirksamkeit:** ● Auswertung der Planeinhaltung ● Nachvollzug der Kontrollen zur Überwachung der Dienstleister mit Relevanz für die kritische Infrastruktur ● Auswertung von Prüfberichten von Dienstleistern ● Nachvollzug, ob identifizierte Abweichungen einer Risikoanalyse unterzogen wurden und durch mitigierende Maßnahmen adressiert wurden.	DLL-02

2.12 Meldewesen			
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Beispielhafte Prüfungshandlungen	Grundlage (C5 #)
100.	**Einrichtung einer Kontaktstelle**	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Organigramm und die Stellenbeschreibung für die Kontaktstelle gemäß § 8 Abs. 3 BSIG. ● Prüfung der Wirksamkeit: ● Nachvollzug der umgesetzten Maßnahmen zur Einrichtung der Meldestelle gemäß IT-Sicherheitsgesetz ● Auswertung der an das BSI abgegebenen Meldungen zur Benennung der Kontaktstelle gemäß § 8b Abs. 3 BSIG.	keine

Die nachfolgenden Anlagen enthalten Beispiele für die Formulierung von Prüfungsberichten. Die zusätzlichen Bestandteile eines Prüfungsberichts gegenüber einem Prüfungsvermerk sind jeweils wie folgt kenntlich gemacht: *[kursiv]*

Anlage 2: Auftragsart „Prüfung einer Erklärung gemäß § 8a Abs. 1 BSIG von Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen – Formulierungsbeispiel für den Prüfungsbericht über die Wirksamkeitsprüfung

Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der gemäß § 8a Abs. 1 BSIG von Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen (geeignet als Nachweis gemäß § 8a Abs. 3 BSIG)

An den [Betreiber der Kritischen Infrastrukturen]

Wir haben die in der Anlage beigefügte Erklärung der gesetzlichen Vertreter [KRITIS-Erklärung] zur Beschreibung der gemäß § 8a Abs. 1 BSIG von der [Betreiber der Kritischen Infrastrukturen] (im Folgenden der „Betreiber“) umzusetzenden Maßnahmen sowie die Geeignetheit und Wirksamkeit dieser Maßnahmen für den Zeitraum vom [Datum] bis [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen sind geeignet, wenn sie – in Übereinstimmung mit den Kriterien des § 8a Abs. 1 BSIG – Risiken maßgeblicher Störungen mit hinreichender Sicherheit begegnen.

Diesen Prüfungsbericht kann der Betreiber als Nachweis (§ 8a Abs. 3 BSIG) für die Erfüllung der Anforderungen nach § 8a Abs. 1 BSIG verwenden.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter des Betreibers sind für die Aufstellung der KRITIS-Erklärung verantwortlich. Dies schließt die Verantwortung für die internen Kontrollen ein, die sie als notwendig erachten, um eine KRITIS-Erklärung aufzustellen, die frei von wesentlichen – beabsichtigten und unbeabsichtigten – Fehlern ist.

Des Weiteren sind die gesetzlichen Vertreter dafür verantwortlich, dass die Maßnahmen gemäß § 8a Abs. 1 BSIG in allen wesentlichen Belangen

- so konzeptioniert werden, dass sie geeignet sind,
- implementiert werden und wirksam sind, d.h. auch
- überwacht und dokumentiert werden.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen die Kriterien des § 8a Abs. 1 BSIG nur mit hinreichender statt absoluter Sicherheit erfüllen.

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die KRITIS-Erklärung frei von wesentlichen Fehlern ist. Dieses

Urteil erstreckt sich auch darauf, ob die in der KRITIS-Erklärung der gesetzlichen Vertreter beschriebenen und vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen

- geeignet waren und
- im geprüften Zeitraum implementiert und wirksam waren.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Die Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen (IDW PH 9.860.2)* durchgeführt.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet.

Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit die vorgenannten Urteile abgeben können.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.2* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um entsprechende Prüfungsurteile abgeben zu können.

Dies schließt die Beurteilung von Risiken wesentlicher – beabsichtigter oder unbeabsichtigter – Fehler in der KRITIS-Erklärung der gesetzlichen Vertreter ein.

Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der KRITIS-Erklärung der gesetzlichen Vertreter angewandten Grundsätze, Verfahren und Maßnahmen sowie der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens.

Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der KRITIS-Erklärung der gesetzlichen Vertreter relevante interne Kontrollsystem abzugeben.

Für die Beurteilung der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Geeignetheit, Implementierung und Wirksamkeit der umgesetzten Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Diese Prüfung umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbau- und einer Funktionsprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

[Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalte keine gesonderten Prüfungsurteile ab.

- *Sonstige Feststellungen, u.a.*
  - *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der KRITIS-Erklärung oder der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen,*
  - *nicht wesentliche falsche Angaben in der KRITIS-Erklärung,*
  - *nicht wesentliche Mängel in der Geeignetheit oder Wirksamkeit der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen.*]

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- ist die KRITIS-Erklärung der gesetzlichen Vertreter frei von wesentlichen Fehlern,
- waren die in der KRITIS-Erklärung der gesetzlichen Vertreter beschriebenen und vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - im geprüften Zeitraum implementiert sowie
  - im geprüften Zeitraum wirksam.

[Prüfungsurteil mit Einschränkung]

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- ist die KRITIS-Erklärung der gesetzlichen Vertreter frei von wesentlichen Fehlern,
- waren die in der KRITIS-Erklärung der gesetzlichen Vertreter beschriebenen und vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und

- im geprüften Zeitraum implementiert sowie
- im geprüften Zeitraum wirksam.

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften KRITIS-relevanten IT-Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien des § 8a BSIG in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die KRITIS-Erklärung der gesetzlichen Vertreter zu den gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit dieser Maßnahmen erstrecken sich auf den Zeitraum vom [Datum] bis [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter]

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ für die gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen, die für Zwecke der [Nennung des Zwecks der Erfüllung der Anforderungen des § 8a Abs. 1 BSIG gegenüber dem BSI (§ 8a Abs. 3 BSIG)] konzipiert wurden. Folglich ist die KRITIS-Erklärung der gesetzlichen Vertreter zu den gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsbericht an den Betreiber gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

KRITIS-Erklärung der gesetzlichen Vertreter zu den gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen

Darstellung der durchgeführten Prüfungshandlungen und geprüften Maßnahmen

Allgemeine Auftragsbedingungen

Anlage 3: Auftragsart „Prüfung einer Erklärung gemäß § 8a Abs. 1 BSIG von Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen – Formulierungsbeispiel für den Prüfungsbericht über die Angemessenheitsprüfung

Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der gemäß § 8a Abs. 1 BSIG von Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen (nicht geeignet als Nachweis gemäß § 8a Abs. 3 BSIG)

An den [Betreiber der Kritischen Infrastrukturen]

Wir haben die in der Anlage beigefügte Erklärung der gesetzlichen Vertreter [KRITIS-Erklärung] zur Beschreibung der gemäß § 8a Abs. 1 BSIG von der [Betreiber der Kritischen Infrastrukturen] (im Folgenden der „Betreiber“) umzusetzenden Maßnahmen sowie die Geeignetheit dieser Maßnahmen zum [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen sind geeignet, wenn sie – in Übereinstimmung mit den Kriterien des § 8a Abs. 1 BSIG – Risiken maßgeblicher Störungen mit hinreichender Sicherheit begegnen.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter des Betreibers sind für die Aufstellung der KRITIS-Erklärung verantwortlich. Dies schließt die Verantwortung für die internen Kontrollen ein, die sie als notwendig erachten, um eine KRITIS-Erklärung aufzustellen, die frei von wesentlichen – beabsichtigten und unbeabsichtigten – Fehlern ist.

Des Weiteren sind die gesetzlichen Vertreter dafür verantwortlich, dass die Maßnahmen gemäß § 8a Abs. 1 BSIG in allen wesentlichen Belangen

- so konzeptioniert werden, dass sie geeignet sind,
- implementiert werden und wirksam sind, d.h. auch
- überwacht und dokumentiert werden.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen die Kriterien des § 8a Abs. 1 BSIG nur mit hinreichender statt absoluter Sicherheit erfüllen.

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die KRITIS-Erklärung frei von wesentlichen Fehlern ist. Dieses Urteil erstreckt sich auch darauf, ob die in der KRITIS-Erklärung der gesetzlichen Vertreter beschriebenen und vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen

- geeignet waren und
- zum [Datum] implementiert waren.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Die Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen (IDW PH 9.860.2)* durchgeführt. Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet.

Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit die vorgenannten Urteile abgeben können.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.2* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um entsprechende Prüfungsurteile abgeben zu können.

Dies schließt die Beurteilung von Risiken wesentlicher – beabsichtigter oder unbeabsichtigter – Fehler in der KRITIS-Erklärung der gesetzlichen Vertreter ein.

Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der KRITIS-Erklärung der gesetzlichen Vertreter angewandten Grundsätze, Verfahren und Maßnahmen sowie der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens.

Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der KRITIS-Erklärung der gesetzlichen Vertreter relevante interne Kontrollsystem abzugeben.

Für die Beurteilung der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Geeignetheit und Implementierung der umgesetzten Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Diese Prüfung umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbauprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

[***Prüfungshandlungen und Prüfungsfeststellungen***

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalte keine gesonderten Prüfungsurteile ab.

- *Sonstige Feststellungen, u.a.*
  - *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der KRITIS-Erklärung oder der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen,*
  - *nicht wesentliche falsche Angaben in der KRITIS-Erklärung,*
  - *nicht wesentliche Mängel in der Geeignetheit der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen.*]

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- ist die KRITIS-Erklärung der gesetzlichen Vertreter frei von wesentlichen Fehlern,
- waren die in der KRITIS-Erklärung der gesetzlichen Vertreter beschriebenen und vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - zum geprüften Zeitpunkt [Datum] implementiert.

[Prüfungsurteil mit Einschränkung]

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- ist die KRITIS-Erklärung der gesetzlichen Vertreter frei von wesentlichen Fehlern,
- waren die in der KRITIS-Erklärung der gesetzlichen Vertreter beschriebenen und vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - zum [Datum] implementiert.

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften KRITIS-relevanten IT-Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien des § 8a BSIG in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die KRITIS-Erklärung der gesetzlichen Vertreter zu den gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Geeignetheit der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen beziehen sich auf den Zeitpunkt zum [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter]

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ für die gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Folglich ist die KRITIS-Erklärung der gesetzlichen Vertreter zu den gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsbericht an den Betreiber gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

KRITIS-Erklärung der gesetzlichen Vertreter zu den gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen

Darstellung der durchgeführten Prüfungshandlungen und geprüften Maßnahmen

Allgemeine Auftragsbedingungen

Anlage 4: Auftragsart „Direkte Prüfung der gemäß § 8a Abs. 1 BSIG von Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen – Formulierungsbeispiel für den Prüfungsbericht über die Wirksamkeitsprüfung

Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der gemäß § 8a Abs. 1 BSIG von Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen (geeignet als Nachweis gemäß § 8a Abs. 3 BSIG)

An den [Betreiber der Kritischen Infrastrukturen]

Wir haben die Geeignetheit und Wirksamkeit gemäß § 8a Abs. 1 BSIG der von [Betreiber der Kritischen Infrastrukturen] (im Folgenden der „Betreiber“) umzusetzenden Maßnahmen für den Zeitraum vom [Datum] bis [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen sind geeignet, wenn sie – in Übereinstimmung mit den Kriterien des § 8a Abs. 1 BSIG – Risiken maßgeblicher Störungen mit hinreichender Sicherheit begegnen. Zur Darstellung der gemäß § 8a Abs. 1 BSIG der vom Betreiber umzusetzenden Maßnahmen und durchgeführten Prüfungshandlungen verweisen wir auf nachstehende Anlage.

Diesen Prüfungsbericht kann der Betreiber als Nachweis (§ 8a Abs. 3 BSIG) für die Erfüllung der Anforderungen nach § 8a Abs. 1 BSIG verwenden.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter des Betreibers sind dafür verantwortlich, dass die Maßnahmen gemäß § 8a Abs. 1 BSIG in allen wesentlichen Belangen

- so konzeptioniert werden, dass sie geeignet sind,
- implementiert werden und wirksam sind, d.h. auch
- überwacht und dokumentiert werden.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen die Kriterien des § 8a Abs. 1 BSIG nur mit hinreichender statt absoluter Sicherheit erfüllen.

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen

- geeignet waren und
- im geprüften Zeitraum implementiert und wirksam waren.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Die Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen (IDW PH 9.860.2)* durchgeführt.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet.

Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit die vorgenannten Urteile abgeben können.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.2* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um entsprechende Prüfungsurteile abgeben zu können.

Für die Beurteilung der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Geeignetheit, Implementierung und Wirksamkeit der umgesetzten Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Diese Prüfung umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbau- und einer Funktionsprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

[**Prüfungshandlungen und Prüfungsfeststellungen**

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalte keine gesonderten Prüfungsurteile ab.

- *Sonstige Feststellungen, u.a.*
  - *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen,*
  - *nicht wesentliche Mängel in der Geeignetheit oder Wirksamkeit der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen.*]

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- waren die vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - im geprüften Zeitraum implementiert sowie
  - im geprüften Zeitraum wirksam.

[Prüfungsurteil mit Einschränkung]

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- waren die vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - im geprüften Zeitraum implementiert sowie
  - im geprüften Zeitraum wirksam.

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften KRITIS-relevanten IT-Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien des § 8a BSIG in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen erstrecken sich auf den Zeitraum vom [Datum] bis [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen dieser Maßnahmen falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter]

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ für die gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen, die für Zwecke der [Nennung des Zwecks der Erfüllung der Anforderungen des § 8a Abs. 1 BSIG gegenüber dem BSI (§ 8a Abs. 3 BSIG)] konzipiert wurden. Folglich ist unser Prüfungsbericht an den Betreiber für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsbericht an den Betreiber gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Darstellung der durchgeführten Prüfungshandlungen und geprüften Maßnahmen

Allgemeine Auftragsbedingungen

Anlage 5: Auftragsart „Direkte Prüfung der gemäß § 8a Abs. 1 BSIG von Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen – Formulierungsbeispiel für den Prüfungsbericht über die Angemessenheitsprüfung

Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der gemäß § 8a Abs. 1 BSIG von Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen (nicht geeignet als Nachweis gemäß § 8a Abs. 3 BSIG)

An den [Betreiber der Kritischen Infrastrukturen]

Wir haben die Geeignetheit der gemäß § 8a Abs. 1 BSIG der von [Betreiber der Kritischen Infrastrukturen] (im Folgenden der „Betreiber“) umzusetzenden Maßnahmen zum [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen sind geeignet, wenn sie – in Übereinstimmung mit den Kriterien des § 8a Abs. 1 BSIG – Risiken maßgeblicher Störungen mit hinreichender Sicherheit begegnen. Zur Darstellung der gemäß § 8a Abs. 1 BSIG der vom Betreiber umzusetzenden Maßnahmen und durchgeführten Prüfungshandlungen verweisen wir auf nachstehende Anlage.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter des Betreibers sind dafür verantwortlich, dass die Maßnahmen gemäß § 8a Abs. 1 BSIG in allen wesentlichen Belangen

- so konzeptioniert werden, dass sie geeignet sind,
- implementiert werden und wirksam sind, d.h. auch
- überwacht und dokumentiert werden.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen die Kriterien des § 8a Abs. 1 BSIG nur mit hinreichender statt absoluter Sicherheit erfüllen.

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen

- geeignet waren und
- zum [Datum] implementiert waren.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Die Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen (IDW PH 9.860.2)* durchgeführt.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet.

Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit die vorgenannten Urteile abgeben können.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.2* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um entsprechende Prüfungsurteile abgeben zu können.

Für die Beurteilung der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Geeignetheit und Implementierung der umgesetzten Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Diese Prüfung umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbauprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

[***Prüfungshandlungen und Prüfungsfeststellungen***

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalte keine gesonderten Prüfungsurteile ab.

- *Sonstige Feststellungen, u.a.*
  - *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen,*
  - *nicht wesentliche Mängel in der Geeignetheit der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen.*]

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- waren die vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - zum geprüften Zeitpunkt [Datum] implementiert.

[Prüfungsurteil mit Einschränkung]

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- waren die vom Betreiber gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - zum geprüften Zeitpunkt [Datum] implementiert.

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften KRITIS-relevanten IT-Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien des § 8a BSIG in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Geeignetheit der gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen bezieht sich auf den Zeitpunkt [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen dieser Maßnahmen falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter]

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ für die gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Folglich ist unser Prüfungsbericht an den Betreiber für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsbericht an den Betreiber gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Darstellung der durchgeführten Prüfungshandlungen und geprüften Maßnahmen

Allgemeine Auftragsbedingungen

Neufassung des IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F. (10.2021))

(Stand: 15.10.2021)

Neufassung des IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F. (10.2021))

Stand: 15.10.2021[1]

1. Vorbemerkungen

1 Dieser *IDW Prüfungshinweis* basiert auf dem *IDW PS 860*[2], der die Grundsätze und Vorgehensweise festlegt, nach denen IT-Prüfungen außerhalb der Abschlussprüfung durchzuführen sind.

Er konkretisiert die Anforderungen, Anwendungshinweise und sonstigen Erläuterungen des *IDW PS 860* in Bezug auf die Prüfung von Cloud-Diensten, die auf der Basis von IT-Systemen durchgeführt werden (im Folgenden Cloud-Dienste) und legt die Berufsauffassung dar, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit bei der Prüfung von Cloud-Diensten bei deren Anbietern (Cloud-Anbieter) vorgehen.

---

[1] Verabschiedet vom Fachausschuss für Informationstechnologie (FAIT) am 29.04.2020 und billigende Kenntnisnahme durch den Hauptfachausschuss (HFA) am 15.05.2020. Anpassung an den BSI C5:2020 verabschiedet vom FAIT am 23.09.2021 und billigende Kenntnisnahme durch den HFA am 15.10.2021.

[2] *IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* (Stand: 02.03.2018).

2 Cloud-Anbieter bündeln in der Praxis Cloud-Dienste in Form von Servicemodellen, insb.:

Infrastructure as a Service (IaaS)

Bei diesem Servicemodell stellt der Cloud-Anbieter dem Cloud-Kunden eine auf dessen Bedarf angepasste IT-Infrastruktur, bspw. Festplattenkapazität, Netzwerkserverkapazität oder Speicherkapazität zur Verfügung.

Platform as a Service (PaaS)

Bei diesem Servicemodell stellt der Cloud-Anbieter eine Umgebung zum Betrieb von selbstentwickelten Softwarelösungen bereit. Der Cloud-Kunde kann auf dieser Plattform eigene Anwendungen entwickeln, testen und betreiben.

Software as a Service (SaaS)

Dieses Servicemodell bezeichnet eine Dienstleistung, bei der eine IT-Anwendung aus der Cloud bezogen wird, bspw. eine Anlagenbuchführung oder eine Software zur Verwaltung der Kundenbeziehungen.

3 Die in Anlage 1 enthaltenen Ziele in Abschn. 1 bis 17 basieren auf dem vom BSI[3] herausgegebenen Kriterienkatalog Cloud Computing (C5:2020) (im Folgenden BSI C5:2020[4] für ein sicheres und ordnungsmäßiges Cloud-Computing. Die Ziele in Anlage 1, Abschn. 1 bis 19 werden vom IDW als geeignete Kriterien i.S. des *IDW PS 860*, Tz. 10 d), Tz. 28 ff., zur Einrichtung angemessener Grundsätze, Verfahren und Maßnahmen (im Folgenden Maßnahmen) für die Bereitstellung von Cloud-Diensten durch den Cloud-Anbieter angesehen, die bei einer Prüfung nach diesem *IDW Prüfungshinweis* beurteilt werden.

4 Dieser *IDW Prüfungshinweis* gilt sowohl für die Auftragsart „Prüfung der Erklärung des Cloud-Anbieters“ als auch für die Auftragsart „direkte Prüfung des Cloud-Dienstes“.

5 Zusammenfassend kennzeichnen insb. die folgenden Merkmale einen Prüfungsauftrag gemäß *IDW PS 860*[5] für die Beurteilung der von Cloud-Anbietern umzusetzenden Maßnahmen unter Anwendung dieses *IDW Prüfungshinweises*:

- Involvierte Parteien sind neben dem Wirtschaftsprüfer und dem Cloud-Anbieter (verantwortlich für das Prüfungsobjekt) weitere vorgesehene Nutzer des Prüfungsberichts, die sich vom Adressaten (i.d.R. die beauftragende Partei) unterscheiden können.
- Der zu prüfende Cloud-Dienst ist klar bestimmbar und abgrenzbar.
- Der Wirtschaftsprüfer gibt ein Urteil mit hinreichender Sicherheit ab und berichtet über die Prüfung entsprechend der Informationsbedürfnisse der vorgesehenen Nutzer der Berichterstattung in einem Prüfungsbericht oder zusätzlich in einem Prüfungsvermerk.
- Durch den Wirtschaftsprüfer werden die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit sowie die Anforderungen des *IDW QS 1*[6] eingehalten.

---

3 Bundesamt für Sicherheit in der Informationstechnik.

4 Kriterienkatalog Cloud Computing (C5:2020), Stand: Oktober 2020, vgl. www.bsi.bund.de.

5 Vgl. *IDW PS 860*, Tz. 5.

6 Vgl. *IDW Qualitätssicherungsstandard: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* (Stand: 09.06.2017).

2. Ziel und Umfang der Prüfung

6 Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) hat mit dem *IDW PS 860* die Berufsauffassung dargelegt, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit die Prüfung von IT-Systemen außerhalb der Abschlussprüfung planen, durchführen sowie darüber Bericht erstatten.

7 Eine nach *IDW PH 9.860.3 n.F.* (10.2021) durchgeführte Prüfung der Cloud-Dienste kann als Angemessenheitsprüfung oder zusätzlich als Wirksamkeitsprüfung erfolgen.

8 Bei der Auftragsart „Prüfung der Erklärung des Cloud-Anbieters" ist es Ziel der Angemessenheitsprüfung, dem Wirtschaftsprüfer auf Grundlage der durchgeführten Prüfungshandlungen ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob[7]

- die Erklärung des Cloud-Anbieters in allen wesentlichen Belangen frei von wesentlichen Fehlern[8] ist,
- die in der Erklärung des Cloud-Anbieters beschriebenen und vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet sind und
  - zu dem zu prüfenden Zeitpunkt implementiert sind.

9 Die Maßnahmen sind geeignet, wenn sie den Risiken der Nichterreichung der Ziele mit hinreichender Sicherheit begegnen. Es ist davon auszugehen, dass die Maßnahmen den Risiken der Nichterreichung der Ziele mit hinreichender Sicherheit begegnen, wenn sie die jeweiligen Basiskriterien oder Zusatzkriterien des BSI C5:2020 in Anlage 1, Abschn. 1 bis 17 bzw. die darüber hinausgehenden Anforderungen in Anlage 1, Abschn. 18 bzw. 19 erfüllen.

10 Ziel der Wirksamkeitsprüfung bei dieser Auftragsart ist – über die Angemessenheitsprüfung hinaus – zu beurteilen, ob die in der Erklärung des Cloud-Anbieters beschriebenen und vom Cloud-Anbieter umzusetzenden Maßnahmen in dem zu prüfenden Zeitraum wie vorgesehen durchgeführt wurden.[9]

11 Sofern eine Prüfung nach *IDW PS 860* i.V.m. *IDW PH 9.860.3* n.F. auch zum Nachweis der Konformität der Basiskriterien nach dem BSI C5 dienen soll, muss die Prüfung zwingend als Wirksamkeitsprüfung durchgeführt werden.

12 Bei der Auftragsart „direkte Prüfung des Cloud-Dienstes" ist Ziel der Angemessenheitsprüfung, dem Wirtschaftsprüfer auf Grundlage der durchgeführten Prüfungshandlungen ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob[10]

- die vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet sind und
  - zu dem zu prüfenden Zeitpunkt implementiert sind.

13 Die Maßnahmen sind geeignet, wenn sie den Risiken der Nichterreichung der Ziele mit hinreichender Sicherheit begegnen. Es ist davon auszugehen, dass die Maßnahmen den Risiken

---

[7] Vgl. *IDW PS 860*, Tz. 15.

[8] Zur Interpretation des Begriffs „wesentliche Fehler" durch das BSI vgl. BSI C5:2020, Abschn. 1.2 „Begriffsbestimmungen".

[9] Vgl. *IDW PS 860*, Tz. 16.

[10] Vgl. *IDW PS 860*, Tz. 21.

der Nichterreichung der Ziele mit hinreichender Sicherheit begegnen, wenn sie die jeweiligen Basiskriterien oder Zusatzkriterien des BSI C5:2020 in Anlage 1, Abschn. 1 bis 17 bzw. die darüber hinausgehenden Anforderungen in Anlage 1, Abschn. 18 bzw. 19 erfüllen.

14 Ziel der Wirksamkeitsprüfung bei dieser Auftragsart ist – über die Angemessenheitsprüfung hinaus – zu beurteilen, ob die umzusetzenden Maßnahmen in dem zu prüfenden Zeitraum wie vorgesehen durchgeführt wurden.[11]

15 Die Prüfung wird für Zwecke des Cloud-Anbieters durchgeführt und der Prüfungsbericht bzw. Prüfungsvermerk ist zur Information des Cloud-Anbieters über das Ergebnis der Prüfung bestimmt. Darüber hinaus dient der Prüfungsbericht bzw. Prüfungsvermerk dem Cloud-Anbieter dazu, gegenüber Kunden die Erfüllung der in Anlage 1 genannten Kriterien in geeigneter Weise nachzuweisen.

3. Gegenstand der Prüfung

16 Gegenstand der „Prüfung der Erklärung des Cloud-Anbieters“ nach diesem *IDW Prüfungshinweis* sind die Systembeschreibung[12] und die darauf aufbauende Erklärung der gesetzlichen Vertreter des Cloud-Anbieters über Maßnahmen in Bezug auf die Erreichung der in Anlage 1 für die jeweiligen Servicemodelle dargestellten Ziele. Exemplarische Bestandteile der Systembeschreibung und der Erklärung des Cloud-Anbieters sind im BSI C5:2020, Abschn. 3.4.4 genannt.

17 Gegenstand einer „direkten Prüfung des Cloud-Dienstes“ nach diesem *IDW Prüfungshinweis* sind die in der Auftragsvereinbarung abgegrenzten Maßnahmen in Bezug auf die Erreichung der in Anlage 1 für die jeweiligen Servicemodelle dargestellten Ziele.

18 Sofern der Cloud-Anbieter Teile der für Cloud-Kunden erbrachten Dienstleistungen an Dritte ausgelagert hat, ist dieser Sachverhalt in der Systembeschreibung darzustellen und bei der Prüfung zu berücksichtigen. Wie in *IDW PS 951 n.F. (03.2021)*[13] wird zwischen der „Inklusive Methode“ und der „Carve-out Methode“ unterschieden. Bei der „Inklusive Methode“ wird das auf die Cloud-Dienstleistung bezogene Interne Kontrollsystem des Subdienstleisters in die Erklärung des Cloud-Anbieters aufgenommen und damit Bestandteil der Prüfung der Angemessenheit und – sofern einschlägig – Wirksamkeit. Bei der „Carve-out Methode“ werden die dienstleistungsbezogenen Kontrollen des Subdienstleisters nicht in die Erklärung des Cloud-Anbieters aufgenommen. Die Prüfung richtet sich allein auf die Kontrollen, die der Cloud-Anbieter zur Steuerung und Überwachung des Subdienstleisters eingerichtet hat.

19 Die im BSI C5:2020 Abschn. 4 dargelegten Rahmenbedingungen des Cloud-Dienstes sind bei einer „Prüfung der Erklärung des Cloud-Anbieters“ Bestandteil der Systembeschreibung des Cloud-Anbieters und bei einer „direkten Prüfung des Cloud-Dienstes“ im Prüfungsbericht zu dokumentieren.

---

[11] Vgl. *IDW PS 860*, Tz. 22.

[12] Vgl. BSI C5:2020, Abschn. 3.4.4.1 „Systembeschreibung“.

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

20 Die Prüfung eines für die Erbringung von Cloud-Diensten relevanten IT-Systems i.S. dieses *IDW Prüfungshinweises* schließt die für Cloud-Dienste relevanten Elemente des IT-Kontrollsystems einschließlich des IT-Risikobeurteilungsprozesses ein. Der IT-Risikobeurteilungsprozess des Cloud-Anbieters bildet somit die Grundlage für die Feststellung der IT-Risiken, die vom Management im Rahmen des IT-Kontrollsystems und damit im Rahmen des Informationssicherheitsmanagementsystems (ISMS) für Cloud-Dienste gesteuert werden müssen.

4. Kriterien

21 Die in der Anlage 1 enthaltenen Ziele stellen geeignete Kriterien i.S. des *IDW PS 860*, Tz. 10 d), Tz. 28 ff., für die Beurteilung der von Cloud-Anbietern getroffenen Maßnahmen dar.

22 Die Ziele und Basiskriterien oder Zusatzkriterien bzw. Anforderungen der Anlage 1 enthalten ein an den Servicemodellen ausgerichtetes mehrstufiges Vorgehen. Für das Servicemodell IaaS (Abschn. 1-17) referenzieren diese auf den BSI C5:2020. Der BSI C5:2020 unterscheidet zwischen Basiskriterium, Zusatzkriterium und Ergänzenden Informationen. Bei einer Prüfung nach diesem *IDW Prüfungshinweis* ist das Basiskriterium aus dem BSI C5:2020 immer zu berücksichtigen. Sofern der Cloud-Anbieter Kunden mit erhöhtem Schutzbedarf hat, ist auch das Zusatzkriterium des BSI C5:2020 zu berücksichtigen. Soweit dies bei rechnungslegungsrelevanten Cloud-Diensten der Fall ist, wurde hierauf ebenfalls in der Anlage 1 referenziert. Die Ziele und Basiskriterien oder Zusatzkriterien in Anlage 1 eignen sich somit auch für die Prüfung von rechnungslegungsrelevanten Cloud-Diensten. Ergänzende Informationen kommentieren die Kriterien und werden daher in der Anlage 1 nicht berücksichtigt.

23 Cloud-Anbieter, die das Servicemodell PaaS zur Verfügung stellen, haben zusätzlich zu den Zielen und Basiskriterien oder Zusatzkriterien des BSI C5:2020 für das Servicemodell IaaS die in Abschn. 18 der Anlage 1 genannten Ziele und Anforderungen zu beachten. Diese beziehen sich auf die weitergehenden Anforderungen des *IDW RS FAIT 5*[14] i.V.m. *IDW RS FAIT 1*[15].

24 Anbieter von SaaS-Servicemodellen haben neben den für IaaS-Servicemodelle geltenden Zielen und Basiskriterien oder Zusatzkriterien des BSI C5:2020 zusätzlich die Ziele und Anforderungen in Abschn. 19 der Anlage 1 zu berücksichtigen, die sich insb. auf die Ordnungsmäßigkeit und Sicherheit der Anwendungen richten. Diese Anforderungen umfassen die in *IDW RS FAIT 1* und *IDW RS FAIT 5* genannten Ordnungsmäßigkeits- und Sicherheitskriterien.

25 Die in der Anlage 1 aufgeführten Ziele und Basiskriterien oder Zusatzkriterien des BSI C5:2020 in Abschn. 1 bis 17 bzw. Anforderungen in Abschn. 18 bzw. 19 sind nicht als abschließende Aufzählung zu verstehen, da die Festlegung in der Verantwortung der gesetzlichen Vertreter des Cloud-Anbieters liegt. Sie sind grundsätzlich in Abhängigkeit vom zu prüfenden Servicemodell zu berücksichtigen.

---

[14] *IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen einschließlich Cloud Computing (IDW RS FAIT 5)* (Stand: 04.11.2015).

[15] *IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)* (Stand: 24.09.2002).

26 Ferner können sich Ergänzungen der Ziele und Basiskriterien oder Zusatzkriterien bzw. Anforderungen aufgrund weiterer gesetzlicher oder sonstiger regulatorischer Vorgaben (bspw. Bankaufsichtliche Anforderungen an die IT (BAIT)[16]) ergeben.

5. Besonderheiten bei der Durchführung der Prüfung

27 Der *IDW PS 860* legt die Grundsätze für die Planung und Durchführung von Prüfungshandlungen für eine Prüfung der Angemessenheit und – sofern einschlägig – Wirksamkeit fest.

28 Gemäß *IDW PS 860*, Tz. 47, hat der Wirtschaftsprüfer auf der Grundlage des gewonnenen Verständnisses über das Unternehmen, das rechtliche und wirtschaftliche Umfeld und der vom Cloud-Anbieter umzusetzenden Maßnahmen die Risiken für wesentliche Fehler in der Erklärung des Cloud-Anbieters bzw. die Risiken wesentlicher Mängel in den umzusetzenden Maßnahmen zu identifizieren und zu beurteilen. Sofern der Wirtschaftsprüfer im Rahmen der Prüfungsdurchführung Nachweise erlangt, die im Widerspruch zu den Prüfungsnachweisen stehen, die Basis für seine ursprüngliche Risikobeurteilung waren, muss er die Risikobeurteilung anpassen und die weiteren geplanten Prüfungshandlungen entsprechend modifizieren. Zudem hat der Wirtschaftsprüfer gemäß *IDW PS 860*, Tz. 48, Prüfungshandlungen zu planen und durchzuführen, um das Prüfungsrisiko auf ein vertretbar niedriges Maß zu reduzieren.

29 Die in der Anlage 1 aufgeführten Prüfungshandlungen sind als Beispiele und nicht als abschließende Aufzählung zu verstehen, da die Festlegung der durchzuführenden Prüfungshandlungen im pflichtgemäßen Ermessen des Wirtschaftsprüfers unter Berücksichtigung der Ergebnisse seiner Risikobeurteilung sowie der notwendigen Prüfungshandlungen als Reaktion auf die beurteilten Risiken liegt.

30 Weitere beispielhafte Prüfungshandlungen ergänzend zu den in der Anlage 1 aufgeführten beispielhaften Prüfungshandlungen sind jeweils auch

- die Einsichtnahme in Unterlagen und Dokumentationen, wie bspw. Richtlinien, Arbeitsanweisungen, Verfahrensanweisungen, Prozessdokumentationen, Verzeichnisse oder Schulungskonzepte, in denen zentrale Vorgaben zur Durchführung, zum Ablauf und zu den Verantwortlichkeiten schriftlich geregelt sind (zur Prüfung der Angemessenheit der Maßnahmen),
- die Beurteilung der Unterlagen und Dokumentationen im Hinblick auf ihre regelmäßige Aktualisierung und Aktualität (zur Prüfung der Angemessenheit der Maßnahmen),
- die Beurteilung der Unterlagen und Dokumentationen im Hinblick auf ihre Vollständigkeit (zur Prüfung der Angemessenheit und Wirksamkeit der Maßnahmen).

31 Soweit der Wirtschaftsprüfer bereits im Rahmen der Angemessenheitsprüfung Risiken wesentlicher Mängel der Erklärung des Cloud-Anbieters identifiziert, die der Cloud-Anbieter selbst nicht identifiziert hat, hat er zu beurteilen, ob ein solches Risiko vorliegt, das seiner Erwartung nach durch das dienstleistungsbezogene Interne Kontrollsystem des Cloud-Anbieters zu identifizieren war und hätte berücksichtigt werden müssen.

[16] Vgl. www.bafin.de, Rubrik Recht & Regelungen – Verwaltungspraxis – Rundschreiben (letzter Abruf am: 14.10.2021).

32 Hat der Wirtschaftsprüfer bereits anlässlich seiner Prüfungshandlungen zur Beurteilung der Risiken wesentlicher Mängel im dienstleistungsbezogenen Interne Kontrollsystem des Cloud-Anbieters solche wesentlichen Mängel festgestellt, kann er zu dem Ergebnis gelangen, dass sich in diesem Zusammenhang weitere Prüfungshandlungen zur Angemessenheit und Wirksamkeit erübrigen.

6. Besonderheiten bei der Berichterstattung des Wirtschaftsprüfers

33 Der Wirtschaftsprüfer verfasst eine schriftliche Berichterstattung als Prüfungsbericht. Der Prüfungsbericht beinhaltet eine zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und ggf. Funktionsprüfungen und der weiteren Prüfungshandlungen sowie Prüfungsfeststellungen.

34 Falls neben dem Prüfungsbericht ein gesonderter Prüfungsvermerk erstellt werden soll, hat der Wirtschaftsprüfer in dem Prüfungsvermerk auf den Prüfungsbericht hinzuweisen.

35 Für die Darstellung der geprüften Maßnahmen und der diesbezüglichen Prüfungshandlungen und Ergebnisse in der Anlage der Berichterstattung über die Prüfung hat sich der nachfolgende Aufbau in der Praxis bewährt:

<table>
<tr><td colspan="2">Beschreibung der Ziele und der jeweiligen Basiskriterien oder Zusatzkriterien des BSI C5:2020 bzw. Anforderungen</td></tr>
<tr><td>Darstellung der Maßnahmen basierend auf der Anlage 1 dieses IDW Prüfungshinweises</td><td>Darstellung des Prüfungsumfangs, der Prüfungshandlungen sowie deren Ergebnisse</td></tr>
<tr><td colspan="2">Beurteilung der Maßnahmen im Hinblick auf ihre Eignung, die Kriterien und damit die Ziele zu erfüllen</td></tr>
</table>

Anlagen

Anlage 1: Ziele und Basiskriterien oder Zusatzkriterien des BSI C5:2020 bzw. Anforderungen für die Prüfung von Cloud-Diensten sowie beispielhafte Prüfungshandlungen

Die in der nachfolgenden Tabelle aufgeführten Überschriften der Abschn. 1 bis 19 enthalten die Ziele für ein sicheres und ordnungsmäßiges Cloud-Computing. Darunter sind links die jeweiligen Basiskriterien oder Zusatzkriterien bzw. Anforderungen enthalten, um diese Ziele zu erreichen, rechts daneben beispielhafte Prüfungshandlungen. Für die Abschn. 1 bis 17 entstammen die Ziele für ein sicheres Cloud-Computing und die Basiskriterien oder Zusatzkriterien dem BSI C5:2020 und sind entsprechend referenziert.

Für die Servicemodelle gelten die folgenden Ziele und Basiskriterien oder Zusatzkriterien bzw. Anforderungen:

- IaaS: Abschn. 1 bis 17
- PaaS: Abschn. 1 bis 17 und Abschn. 18
- SaaS: Abschn. 1 bis 17 und Abschn. 19.

1. Organisation der Informationssicherheit (OIS) **Zielsetzung: Planung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Rahmenwerks zur Informationssicherheit innerhalb der Organisation**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
1.	**Informationssicherheitsmanagementsystem (ISMS)** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung zum ISMS im Hinblick auf Vollständigkeit und Konsistenz der Berücksichtigung der Anforderungen ● Einsichtnahme in die Erklärung zur Anwendbarkeit (Statement of Applicability) im Hinblick auf Vollständigkeit ● Abgleich der Verfahrensanweisung hinsichtlich Aktualität und Vollständigkeit der Inhalte gemäß des ISO-Standards der 2700x-Reihe sowie der weiteren vom Management dem ISMS zugrunde gelegten Kriterien ● Befragung des ISMS-Verantwortlichen hinsichtlich der Ergebnisse der letzten Managementbewertung sowie zur Steuerung und Überwachung der Informationssicherheit. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Berichte sowie die Managementbewertung bezogen auf die Zielerreichung/-abweichung und die regelmäßige Überprüfung und Anpassung der im ISMS definierten Ziele	OIS-01

1. Organisation der Informationssicherheit (OIS) **Zielsetzung: Planung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Rahmenwerks zur Informationssicherheit innerhalb der Organisation**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Einsichtnahme in Nachweise über die systematische Nachverfolgung und Beseitigung von erkannten Mängeln und Schwächen entsprechend der Vorgaben der eingesetzten Verfahren und Richtlinien im ISMS.	
2.	**Leitlinie zur Informationssicherheit** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Unterlagen, ob eine Leitlinie zur Informationssicherheit verabschiedet ist und relevante Inhalte (Stellenwert der Informationssicherheit, Sicherheitsziele, Organisationsstruktur) angemessen widerspiegelt ● Einsichtnahme in die Kommunikationsplanung für alle betroffenen Parteien auf Angemessenheit. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Berichte/Auswertungen bezogen auf die Zielerreichung/-abweichung und die regelmäßige Überprüfung und Anpassung der Sicherheitsziele ● Einsichtnahme in die Freigaben der Unternehmensleitung zur Inkraftsetzung der Leitlinie zur Informationssicherheit und der sich daraus ableitenden Anweisungen auf Vollständigkeit ● Einsichtnahme in die Dokumentation über die erfolgte Kommunikation mit betroffenen internen/externen Parteien.	OIS-02
3.	**Schnittstellen und Abhängigkeiten** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation der (geteilten) Verantwortlichkeiten, Schnittstellen und Abhängigkeiten (zwischen dem Cloud-Anbieter und beteiligten anderen Parteien wie Kunden oder Drittdienstleistern) hinsichtlich der Aufgaben und Verantwortlichkeitsbereiche zum Umgang mit Schwachstellen, Sicherheitsvorfällen und Störungen. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob Veränderungen an Verantwortlichkeiten und Schnittstellen an alle betroffenen internen und externen Parteien zeitnah kommuniziert wurden.	OIS-03

1. Organisation der Informationssicherheit (OIS) **Zielsetzung: Planung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Rahmenwerks zur Informationssicherheit innerhalb der Organisation**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
4.	**Aufgabentrennung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in relevante und definierte Kontrolldokumentationen, Konzepte, Verfahrensanweisungen zur Trennung von Rollen und Verantwortlichkeiten im Rahmen der Informationssicherheit (u.a. Berechtigungen, Entwicklung/Test/Freigabe von Änderungen, Betrieb sowie zu kompensierenden Überwachungstätigkeiten und Kontrollen, sofern eine Funktionstrennung aus organisatorischen oder technischen Gründen nicht eingerichtet ist ● Abgleich der Unterlagen und Verfahren hinsichtlich Aktualität, Vollständigkeit der Inhalte und angemessener Abbildung geforderter Funktionstrennungen. **Prüfung der Wirksamkeit:** ● Nachvollzug der Bereiche Rollenadministration, Berechtigungsvergabe, Änderungen am Cloud-Dienst und Wartung der relevanten physischen und logischen Infrastruktur des Cloud-Dienstes im Hinblick auf die Einhaltung der Vorgaben zur Vermeidung von Funktionstrennungskonflikten ● Nachvollzug der Wirksamkeit kompensierender Kontrollen bei fehlender Funktionstrennung.	OIS-04
5.	**Kontakt zu relevanten Behörden und Interessenverbänden** Das Basiskriterium und in Fällen, in denen der Cloud-Dienst durch Organisationen des öffentlichen Sektors genutzt wird, ist auch das Zusatzkriterium des BSI C5:2020 zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Anweisungen für den Kontakt mit relevanten Behörden und Interessensverbänden ● Für das Zusatzkriterium Einsichtnahme in Nachweise über die Aktualität der Kontakte mit dem Nationalen IT-Lagezentrum und dem CERT-Bund des BSI. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise zum Austausch mit Behörden und Interessenverbänden im Hinblick auf die Umsetzung ggf. empfohlener Maßnahmen	OIS-05

1. Organisation der Informationssicherheit (OIS) **Zielsetzung: Planung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Rahmenwerks zur Informationssicherheit innerhalb der Organisation**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Einsichtnahme in Aufzeichnungen betreffend die Verarbeitung der über die Kontakte erhaltenen Informationen gemäß der Verfahren zum Umgang mit Risiken (vgl. OIS-06) und Schwachstellen (vgl. OPS-19).	
6.	**Richtlinie für den Umgang mit Risiken** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen zum Risikomanagement betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Richtlinien in Bezug auf: – Kommunikation an die Mitarbeiter – Bereitstellung/Verfügbarkeit für die Mitarbeiter – Verfahren zur entsprechenden Handhabung von Aktualisierungen (vgl. SP-02).	OIS-06
7.	**Anwendung des Verfahrens für den Umgang mit Risiken** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Risikomanagement-Inventar hinsichtlich der Dokumentation von Risiken betreffend den Cloud-Dienst. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Ergebnisdokumentation des anlassbezogenen, aber mindestens jährlich vollzogenen Risiko-Assessment-Verfahrens einschließlich Dokumentation der identifizierten Veränderungen/Abweichungen und des Maßnahmenplans zur zeitnahen Behandlung der Risiken ● Einsichtnahme in die entsprechende Dokumentation zum Nachweis der implementierten Maßnahmen bei identifizierten Veränderungen/Abweichungen und Risiken.	OIS-07

2. Sicherheitsrichtlinien und Arbeitsanweisungen (SP) **Zielsetzung: Bereitstellen von Richtlinien und Anweisungen bzgl. des Sicherheitsanspruchs und zur Unterstützung der geschäftlichen Anforderungen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
8.	**Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinienpyramide, um alle von der Leitlinie zur Informationssicherheit abgeleiteten Richtlinien und Anweisungen zur Informationssicherheit oder zu verwandten Themen zu identifizieren ● Inaugenscheinnahme der Verfahren zur Aktualisierung, Vervollständigung, Genehmigung und Kommunikation der Inhalte der Richtlinien und Anweisungen gemäß den im Kriterium genannten Aspekten. **Prüfung der Wirksamkeit erfolgt bei der jeweiligen Richtlinie.**	SP-01
9.	**Überprüfung und Freigabe von Richtlinien und Anweisungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung zur Überprüfung und Freigabe von Richtlinien und Anweisungen ● Einsichtnahme in Nachweise über den angemessenen Umfang und die Frequenz der Überprüfung ● Einsichtnahme in Schulungspläne und erworbene Qualifikationen im Hinblick auf die fachliche Qualifikation der für die Überprüfung der Richtlinie vorgesehenen Fachkräfte. **Prüfung der Wirksamkeit**: ● Einsichtnahme in Nachweise über die jährlich erfolgte Überprüfung der Richtlinien und Anweisungen zur Informationssicherheit und über die Einhaltung der Anforderungen zur Qualifikation der Prüfer sowie der Vorgaben zu den Inhalten der Überprüfung ● Einsichtnahme in Nachweise über die angemessene Freigabe von Richtlinien und Anweisungen zur Informationssicherheit nach jährlich erfolgter Überprüfung.	SP-02
10.	**Abweichungen von bestehenden Richtlinien und Anweisungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Beobachtung des Prozesses zur Erfassung und Genehmigung von Ausnahmen für Richtlinien und Anweisungen zur Informationssicherheit hinsichtlich Zeitnähe, Angemessenheit, Dokumentation und Vollständigkeit.	SP-03

2. Sicherheitsrichtlinien und Arbeitsanweisungen (SP) **Zielsetzung: Bereitstellen von Richtlinien und Anweisungen bzgl. des Sicherheitsanspruchs und zur Unterstützung der geschäftlichen Anforderungen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise über die zeitlich befristete Genehmigung und mindestens jährliche Überprüfung der Ausnahmen durch die Risikoeigentümer.	

3. Personal (HR) **Zielsetzung: Sicherstellen, dass Mitarbeiter ihre Aufgaben verstehen, sich ihrer Verantwortung in Bezug auf Informationssicherheit bewusst sind und die Assets der Organisation bei Änderung der Aufgaben oder Beendigung geschützt werden.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
11.	**Überprüfung der Qualifikation und Vertrauenswürdigkeit** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensanweisung zur Überprüfung der Qualifikation und Vertrauenswürdigkeit von internen und externen Mitarbeitern, um festzustellen, ob die für die Personenüberprüfung rechtlich zulässigen Schritte durchgeführt werden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über durchgeführte Überprüfungen der Qualifikation und Vertrauenswürdigkeit für neu eingestellte Mitarbeiter.	HR-01
12.	**Beschäftigungs- und Vertragsbedingungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Muster einer Beschäftigungsvereinbarung hinsichtlich Einhaltung der Vorgaben zur Informationssicherheit. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Mitarbeiter auf die Richtlinien und Anweisungen zur Informationssicherheit verpflichtet wurden.	HR-02
13.	**Programm zur Sicherheitsausbildung und Sensibilisierung** Das Basiskriterium und das Zusatzkriterium des	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren betreffend die im Kriterium genannten Aspekte.	HR-03

3. Personal (HR) **Zielsetzung: Sicherstellen, dass Mitarbeiter ihre Aufgaben verstehen, sich ihrer Verantwortung in Bezug auf Informationssicherheit bewusst sind und die Assets der Organisation bei Änderung der Aufgaben oder Beendigung geschützt werden.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
	BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise zur Ausrollung des Programms der Sicherheitsausbildung und Sensibilisierung zum Thema Informationssicherheit. ● Nachvollzug von Nachweisen zur Aktualisierung des Schulungsprogramms, z.B. nach Sicherheitsvorfällen oder bei neuen Bedrohungen, und zu Teilnahmen an Schulungen ● Nachvollzug der Auswertung des Lernerfolgs und der Bewertung der Teilnehmer zur Verbesserung der Trainingsinhalte.	
14.	**Maßregelungsprozess** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinien und Anweisungen zu gemeldeten Verstößen und deren Sanktionierung ● Einsichtnahme in die Kommunikation dieser Regelungen an Mitarbeiter und Dienstleister. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Aufzeichnungen über die Sanktionierung festgestellter Verstöße.	HR-04
15.	**Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Verträge oder Verpflichtungserklärungen, ob demnach bei Auflösung oder Änderung eines Beschäftigungsverhältnisses die Richtlinien und Anweisungen mit Bezug zur Informationssicherheit für einen definierten Zeitraum weiter einzuhalten sind. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über entsprechende schriftliche Bestätigungen von Mitarbeitern und Dienstleistern.	HR-05
16.	**Vertraulichkeitsvereinbarungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Muster der Vertraulichkeitsvereinbarungen für Mitarbeiter und Dienstleister, ob die Geheimhaltungs- und Vertraulichkeitspflichten des Cloud-Anbieters berücksichtigt sind.	HR-06

3. Personal (HR) **Zielsetzung: Sicherstellen, dass Mitarbeiter ihre Aufgaben verstehen, sich ihrer Verantwortung in Bezug auf Informationssicherheit bewusst sind und die Assets der Organisation bei Änderung der Aufgaben oder Beendigung geschützt werden.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		Prüfung der Wirksamkeit: ● Nachvollzug, ob die in den Vertraulichkeitsvereinbarungen enthaltenen Anforderungen mindestens jährlich überprüft werden und ob diese für Mitarbeiter, und Dienstleister abgeschlossen wurden, bevor diese Zugriff auf Daten der Cloud-Kunden erhalten haben.	

4. Asset Management (AM) **Zielsetzung: Identifizieren der organisationseigenen Assets gewährleisten und ein angemessenen Schutzniveau über deren gesamten Lebenszyklus sicherstellen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
17.	**Inventarisierung der Assets** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Asset-Management-Prozessdokumentationen und der Prozeduren zur Erfüllung der Anforderungen hinsichtlich Aktualität, Vollständigkeit, Richtigkeit, Nachvollziehbarkeit und Konsistenz eines Asset Inventars ● Einsichtnahme in das Incident Management, ob eine Verknüpfung zum Asset-Inventar vorhanden ist, um Cloud-Kunden bei kritischen Ereignissen identifizieren und informieren zu können ● Einsichtnahme in die Verfahren zur Inventarisierung im Hinblick auf die Protokollierung von Änderungen. **Prüfung der Wirksamkeit:** ● Nachvollzug der Aufzeichnungen zu automatischen oder manuellen Kontrollen zur vollständigen, richtigen, gültigen und konsistenten Erfassung der Informationen zu den Assets ● Nachvollzug anhand von Nachweisen über Incidents, ob Cloud-Kunden anhand der Assets identifiziert und benachrichtigt wurden.	AM-01

4. Asset Management (AM) **Zielsetzung: Identifizieren der organisationseigenen Assets gewährleisten und ein angemessenen Schutzniveau über deren gesamten Lebenszyklus sicherstellen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
18.	**Richtlinie für den zulässigen Gebrauch und sicheren Umgang mit Assets** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Anweisungen zum Umgang mit Assets auf angemessene Vorgaben für die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien und Anweisungen – an die Mitarbeiter kommuniziert sind, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	AM-02
19.	**Inbetriebnahme von Hardware** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Asset Management-Prozessdokumentation betreffend den Freigabeprozess für den Einsatz von in Betrieb zu nehmender Hardware. **Prüfung der Wirksamkeit:** ● Einsicht in Aufzeichnungen über die Durchführung des Freigabeprozesses, ob die Genehmigungen erst nach Verifikation der sicheren Konfiguration der Mechanismen für Fehlerbehandlung, Protokollierung, Verschlüsselung, Authentisierung und Autorisierung erteilt wurden.	AM-03
20.	**Außerbetriebnahme von Hardware** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Asset Management-Prozessdokumentation betreffend die Genehmigung der Außerbetriebnahme von Hardware und die vollständige/unwiderrufliche Löschung von Daten bzw. Vernichtung von Datenträgern. **Prüfung der Wirksamkeit:** ● Einsicht in Aufzeichnungen zur Durchführung der Außerbetriebnahme, ob diese erst nach vollständiger und unwiderruflicher Löschung der Daten oder der ordnungsgemäßen Vernichtung der Datenträger erfolgte.	AM-04
21.	**Verpflichtung auf zulässigen Gebrauch und sicheren Umgang mit ausgehändigten Assets sowie Rückgabe**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Prozessdokumentation zur Verpflichtung der Mitarbeiter und Dienstleister auf zulässigen Gebrauch und sicheren Umgang mit ausgegebenen Assets sowie die Rückgabe	AM-05

4. Asset Management (AM) **Zielsetzung: Identifizieren der organisationseigenen Assets gewährleisten und ein angemessenen Schutzniveau über deren gesamten Lebenszyklus sicherstellen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
	Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	bei Beendigung des Beschäftigungs- bzw. Vertragsverhältnisses. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Mitarbeiter und Dienstleister auf den zulässigen Gebrauch und sicheren Umgang mit ausgegebenen Assets verpflichtet wurden (z.B. unterschriebene Verpflichtungserklärung vor Ausgabe) ● Nachvollzug, ob bei Beendigung des Vertragsverhältnisses eine dokumentierte Rückgabe der ausgehändigten Assets erfolgte (z.B. Laufzettel) ● Nachvollzug, ob bei Vorfällen (z.B. Verlust oder unautorisierter Zugriff) gemäß der Richtlinie gehandelt wurde (siehe auch SIM-04).	
22.	**Klassifizierung und Kennzeichnung von Assets** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren im Hinblick auf Vorgaben zur einheitlichen Klassifizierung und Kennzeichnung von Informationen und Assets betreffend die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. **Prüfung der Wirksamkeit:** ● Einsichtnahme in das Asset-Inventar betreffend die richtlinienkonforme Klassifizierung von Assets ● Einsichtnahme in Dokumente betreffend die richtlinienkonforme Kennzeichnung in Bezug auf die o.g. Schutzziele.	AM-06

5. Physische Sicherheit (PS) **Zielsetzung: Verhindern von unberechtigtem physischem Zutritt und Schutz vor Diebstahl, Schaden, Verlust und Ausfall des Betriebs.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
23.	**Sicherheitsanforderungen für Räumlichkeiten und Gebäude** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Sicherheitsanforderungen für Räumlichkeiten und Gebäude auf angemessene Vorgaben für die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Sicherheitsanforderungen – an die Mitarbeiter kommuniziert sind, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	PS-01
24.	**Redundanzmodell** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation betreffend die Architektur zur Bereitstellung des Cloud-Dienstes und Beurteilung der Eignung für eine Betriebsredundanz. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Aufzeichnungen über Tests zur Validierung der Funktionsfähigkeit der Redundanz, ob diese mindestens jährlich durchgeführt wurden und festgestellte Mängel behandelt wurden.	PS-02
25.	**Perimeterschutz** Die Basisanforderung des BSI C5 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Dokumentationen hinsichtlich physischer Sicherheit und Schutzmaßnahmen auf Basis der Sicherheitskonzeption (siehe PS-01). **Prüfung der Wirksamkeit:** ● Inaugenscheinnahme von Gebäuden und Räumlichkeiten und Einsichtnahme in ergänzende Dokumente betreffend die Ausprägung geeigneter Sicherheitsmaßnahmen (z.B. Sicherheitstüren, Bewegungsmelder, Videoüberwachung) sowie Beurteilung der Türen, Fenster und sonstigen Bauelemente gemäß der technischen Normen.	PS-03
26.	**Physische Zutrittskontrolle** Die Basisanforderung des BSI C5 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Anweisungen zur Beantragung und Genehmigung von physischem Zutritt betreffend die im Kriterium genannten Aspekte ● Inaugenscheinnahme von Gebäuden und Räumlichkeiten betreffend das Vorhandensein eines geeigneten Zutrittskontrollsystems.	PS-04

5. Physische Sicherheit (PS) **Zielsetzung: Verhindern von unberechtigtem physischem Zutritt und Schutz vor Diebstahl, Schaden, Verlust und Ausfall des Betriebs.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		Prüfung der Wirksamkeit: ● Einsichtnahme in Aufzeichnungen über die richtlinienkonforme Vergabe, Sperrung und Entzug von Zutrittsberechtigungen ● Nachvollzug, ob Zutritte entsprechend den Vorgaben protokolliert werden.	
27.	**Schutz vor Feuer und Rauch** Die Basisanforderung und das Zusatzkriterium des BSI C5 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren zum Schutz vor Feuer und Rauch im Hinblick auf die im Kriterium genannten Aspekte ● Einsichtnahme in die Richtlinien und Verfahren zur Überwachung der Umgebungsparameter zum Schutz vor Feuer und Rauch. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über die regelmäßige Wartung der technischen Einrichtung sowie über die Durchführung von Brandschutzübungen und Brandschutzbegehungen ● Nachvollzug, ob bei Überschreiten von Schwellwerten Meldungen ausgelöst und an die vorgesehenen Empfänger weitergeleitet wurden ● Einsichtnahme in Protokolle Dritter über technische Abnahmen und Gutachten.	PS-05
28.	**Schutz vor Ausfall der Versorgungseinrichtungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren zum Schutz vor Ausfall der Versorgungseinrichtungen im Hinblick auf die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug von Ausfallsimulationen, Tests und Wartungen des Cloud-Anbieters anhand von Aufzeichnungen (z.B. Protokolle) ● Inaugenscheinnahme von Gebäuden und Räumlichkeiten im Hinblick auf redundante Einrichtungen zur Strom- und Kälteversorgung.	PS-06
29.	**Überwachung der Betriebs- und Umgebungsparameter**	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Konzept zur Überwachung der Betriebsparameter und der darin festgelegten Vorgaben	PS-07

5. Physische Sicherheit (PS) **Zielsetzung: Verhindern von unberechtigtem physischem Zutritt und Schutz vor Diebstahl, Schaden, Verlust und Ausfall des Betriebs.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
	Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	● Einsichtnahme in die Konfiguration der Systeme zur Überwachung hinsichtlich Umsetzung des Konzepts. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Aufzeichnungen über die regelmäßige Überwachung der Betriebsparameter und die Information der zuständigen Stellen bei Verlassen des zulässigen Regelbereichs ● Nachvollzug, ob bei Verlassen des Regelbereichs geeignete Maßnahmen eingeleitet wurden.	

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
30.	**Kapazitätsmanagement – Planung** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Dokumentationen, Richtlinien, Verfahrensanweisungen und Planungen zum Capacity Management von Personal- und IT-Ressourcen (einschließlich Überwachungsmaßnahmen) ● Einsichtnahme in Richtlinien, Verfahrensanweisungen und Dokumentationen hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug des Capacity Managements im Hinblick auf angemessene Berücksichtigung von Kapazitätsengpässen in der Vergangenheit und Plausibilität der den Prognosen zugrundeliegenden Annahmen ● Nachvollzug, inwieweit der gemeldete Bedarf zur Vermeidung von Engpässen durch neue Personal- bzw. IT-Ressourcen gedeckt wurde	OPS-01

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Nachvollzug, ob die Kapazitätsplanung in Einklang mit den Dienstgütevereinbarungen steht.	
31.	**Kapazitätsmanagement – Überwachung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentationen, Richtlinien, Verfahrensanweisungen zum Capacity Management (einschließlich Überwachungsmaßnahmen) von Personal- und IT-Ressourcen, ob diese den vertraglichen Vereinbarungen und Dienstgütevereinbarungen entsprechen ● Einsichtnahme in die Konfiguration von IT-Systemen zur Überwachung der Ressourcen und Beurteilung, ob diese ermöglichen, die vertraglichen Vereinbarungen und Dienstgütevereinbarungen zu erfüllen (z.B. durch Definition und Darstellung von Metriken für die Kapazität von Ressourcen mit Informations-, Warn- und Alarmschwellen). **Prüfung der Wirksamkeit:** ● Nachvollzug ausgewählter technischer und organisatorischer Maßnahmen, ob diese während des Prüfungszeitraums durchgeführt wurden ● Nachvollzug, ob die technischen Konfigurationen zur Überwachung im gesamten Prüfungszeitraum bestanden haben, z.B. über Einsichtnahme in Change-Tickets oder Systemprotokolle ● Nachvollzug, ob aus Ergebnissen der durchgeführten Überwachungsmaßnahmen und Abweichungen zu den definierten Vorgaben in vertraglichen Vereinbarungen sowie Dienstgütevereinbarungen Maßnahmen abgeleitet und zeitnah umgesetzt wurden.	OPS-02
32.	**Kapazitätsmanagement – Steuerung von Ressourcen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in vertragliche Vereinbarungen und in Dienstgütevereinbarungen und Beurteilung, ob der Kunde die Möglichkeit hat, die Nutzung der Systemressourcen festzulegen und zu überwachen. **Prüfung der Wirksamkeit:** ● Nachvollzug der durch die Cloud-Kunden veranlassten Kapazitätsanpassungen.	OPS-03

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
33.	**Schutz vor Schadprogrammen – Konzept** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahren und eingesetzte Tools betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert sind, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	OPS-04
34.	**Schutz vor Schadprogrammen – Umsetzung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Nachvollzug, ob alle Systemkomponenten in den Schutz vor Schadprogrammen einbezogen sind. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise darüber, ob Routinen/Aktualisierungen von Schutzprogrammen gemäß den definierten Vorgaben während des Prüfungszeitraums tatsächlich aktualisiert und durchgeführt wurden (z.B. durch Einsichtnahme in Logs von Schutzprogrammen) ● Soweit Schutzprogramme mit einer signatur- oder verhaltensbasierten Erkennung und Entfernung von Schadprogrammen eingerichtet sind, Nachvollzug auf mindestens tägliche Aktualisierung der Programme ● Einsichtnahme in Nachweise zu durchgeführten Monitoringaktivitäten (z.B. Protokolle) und in die Dokumentation über die Beseitigung von Schadprogrammen.	OPS-05
35.	**Vorgaben zur Datensicherung und Wiederherstellung – Konzept** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte ● Beobachtung des Verfahrens, wie die vertraglichen Vereinbarungen mit den Cloud-Kunden in das Konzept zur Datensicherung und Wiederherstellung überführt werden.	OPS-06

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		Prüfung der Wirksamkeit: ● Nachvollzug, ob während des Prüfungszeitraums ausschließlich autorisierte Personen Zugriff auf die Datensicherungs- und Wiederherstellungsprozeduren und die gesicherten Daten hatten.	
36.	**Datensicherung und Wiederherstellung – Überwachung** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahren und Maßnahmen zur Überwachung von Backup- und Recovery-Prozeduren im Hinblick auf die im Kriterium genannten Aspekte ● Nachvollzug der Zugänglichkeit der relevanten Protokolle zur Überwachung der Datensicherung für Cloud-Kunden im Self-Service Portal. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Protokolle, ob im Prüfungszeitraum Datensicherungen gemäß den vertraglichen Anforderungen der Cloud-Kunden oder den geschäftlichen Vorgaben durchgeführt wurden ● Einsichtnahme in Nachweise zur Nachverfolgung und zeitnahen Behebung von Störungen ● Nachvollzug, ob die Nachweise aus der Überwachung der Datensicherung und der Wiederherstellung über den Prüfungszeitraum in das Self-Service-Portal eingestellt wurden.	OPS-07
37.	**Datensicherung und Wiederherstellung – Regelmäßige Tests** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Dokumentationen aus dem Test von Wiederherstellungsverfahren, ob die Einhaltung der vertraglichen Vereinbarungen sowie die Vorgaben zur maximal tolerierbaren Ausfallzeit (Recovery Time Objective, RTO) und zum maximal zulässigen Datenverlust (Recovery Point Objective, RPO) erfüllt waren ● Nachvollzug der Zugänglichkeit der Ergebnisse aus Wiederherstellungstests für Cloud-Kunden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise zu durchgeführten Wiederherstellungstests, ob ein Abgleich mit den vertraglichen Vereinbarungen sowie den anwendbaren Vorgaben stattgefunden hat	OPS-08

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Einsichtnahme in Nachweise zur Nachverfolgung und zeitnahen Behebung von in den Tests identifizierten Abweichungen.	
38.	**Datensicherung und Wiederherstellung – Aufbewahrung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahren und Maßnahmen zur Auslagerung der Datensicherungen an einen entfernten Remote-Standort; sofern die Daten über das Netz übertragen werden, geschieht dies in verschlüsselter Form und in einen örtlich von den gesicherten Daten getrennten Cloud-Bereich ● Einsichtnahme in die Evaluierung und Risikoeinschätzung zur Entfernung des Remote-Standorts zum Hauptstandort ● Nachvollzug, ob die Maßnahmen zur physischen und umgebungsbezogenen Sicherheit am Remote-Standort dem Hauptstandort entsprechen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise/Protokolle über regelmäßige Datenübertragungen oder Transporte von Datensicherungen zum Remote-Standort und Beurteilung im Hinblick auf Verschlüsselung und Allokation der Datensicherungen ● Inaugenscheinnahme der physischen Sicherungsmaßnahmen am Remote-Standort für Datensicherungen gemäß PS-02 bis PS-07	OPS-09
39.	**Protokollierung und Überwachung – Konzept** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über die Nachverfolgung und zeitnahe Behebung von Störungen bzw. über eingeleitete Maßnahmen.	OPS-10

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
40.	**Protokollierung und Überwachung – Konzept zum Umgang mit Metadaten** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinien und Verfahren hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Metadaten ausschließlich für die vertraglich festgelegten Zwecke verwendet werden ● Nachvollzug, ob Metadaten über den Prüfungszeitraum anonymisiert wurden.	OPS-11
41.	**Protokollierung und Überwachung – Zugriff, Speicherung und Löschung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Konfiguration der für die Protokollierung und Überwachung eingesetzten IT-Systeme betreffend die Einschränkung der Zugriffe sowie der zeitlichen Befristung der Aufbewahrung von Protokolldateien und deren regelmäßiger Löschung gemäß den anwendbaren Richtlinien und Vorgaben. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise/Protokolle über die regelmäßige Löschung von Protokolldateien und Metadaten im Prüfungszeitraum.	OPS-12
42.	**Protokollierung und Überwachung – Erkennung von Ereignissen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Konzept zur automatischen Überwachung von Protokolldateien auf sicherheitsrelevante Ereignisse und Ereigniskorrelation ● Einsichtnahme in die Konfiguration der IT-Systeme zur Überwachung der Protokolldateien hinsichtlich geeigneter Definition von Regeln zur Erkennung sicherheitsrelevanter Ereignisse, Ereigniskorrelation und Information der zuständigen Stellen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Aufzeichnungen zu sicherheitsrelevanten Ereignissen im Betrachtungszeitraum, ob geeignete Maßnahmen zur Reaktion auf Ereignisse zeitgerecht eingeleitet wurden.	OPS-13

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
43.	**Protokollierung und Überwachung – Aufbewahrung der Protokollierungsdaten** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren zur Aufbewahrung von Protokolldaten betreffend die im Kriterium genannten Aspekte ● Nachvollzug, ob Prozesse zur Bereitstellung einer kundenspezifischen Protokollierung vorgesehen sind ● Einsichtnahme in Maßnahmen zur Authentisierung oder Verschlüsselung der Datenübertragung zwischen den beteiligten IT-Systemen ● Einsichtnahme in die Maßnahmen zur Trennung der Übertragung von Nutz- und Protokolldaten entsprechend dem Schutzbedarf und deren unveränderliche Aufbewahrung. **Prüfung der Wirksamkeit:** ● Nachvollzug der durchgängigen Authentisierung bzw. Verschlüsselung über den Prüfungszeitraum durch Einsichtnahme in die entsprechenden Systemparameter und Änderungsprotokolle. ● Nachvollzug der Unveränderlichkeit der Protokolldaten über den Prüfungszeitraum gemäß IDM-06.	OPS-14
44.	**Protokollierung und Überwachung – Zurechenbarkeit** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Protokollierungsvorgaben von Benutzerzugriffen auf Tenant-Ebene, ob diese eine forensische Analyse ermöglichen ● Nachvollzug, ob Schnittstellen für die forensische Analyse von Protokollierungsdaten zur Verfügung stehen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Protokollierungsdaten und Prüfung auf Einhaltung der Vorgaben zur eindeutigen Identifizierung von Benutzerzugriffen auf Tenant-Ebene ● Nachvollzug, ob über die Schnittstelle Daten für eine forensische Analyse bereitgestellt werden können.	OPS-15

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
45.	**Protokollierung und Überwachung – Konfiguration** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Vorgaben sowie Systemkonfigurationen, ob der Zugriff auf und die Verwaltung von Systemkomponenten zur Protokollierung- und Überwachung auf autorisierte Benutzer beschränkt ist ● Beobachtung eines autorisierten Benutzers beim Zugriff auf Systemkomponenten zur Protokollierung und Überwachung, ob eine Zwei-Faktor-Authentifizierung eingerichtet ist. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über die Einhaltung der Kriterien zur autorisierten Freigabe und Überprüfung bei Änderungen der Konfiguration von Protokollierungen und Überwachungen ● Nachvollzug, ob den Kunden die Protokolle in angemessener Form und zeitnah zur Verfügung gestellt wurden ● Nachvollzug, ob die Einstellung zur Zwei-Faktor-Authentifizierung über den Prüfungszeitraum aktiviert war.	OPS-16
46.	**Protokollierung und Überwachung – Verfügbarkeit der Überwachungs-Software** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in relevante Dokumentationen und Systemeinstellungen, ob Ausfälle der Protokollierungs- und Überwachungssoftware automatisch gemeldet werden ● Einsichtnahme in Nachweise, ob die zentralen Komponenten zur Überwachung redundant ausgelegt sind und eine automatische Umschaltung vorgesehen ist. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise, die belegen, dass bei Ausfällen der Protokollierungs- und Überwachungssoftware eine zeitnahe Meldung an die zuständigen Stellen erfolgte und ob diese geeignete Maßnahmen zeitnah eingeleitet haben bzw. die automatische Umschaltung auf die redundanten Komponenten stattgefunden hat.	OPS-17

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
47.	**Umgang mit Schwachstellen, Störungen und Fehlern – Konzept** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert sind, – für die Mitarbeiter verfügbar sind; – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	OPS-18
48.	**Umgang mit Schwachstellen, Störungen und Fehlern – Penetrationstests** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in relevante Richtlinien und Verfahrensanweisungen sowie in die Dokumentation der durchgeführten Penetrationstests hinsichtlich Aktualität und Vollständigkeit betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise, ob die Penetrationstests mindestens jährlich durchgeführt wurden und die für den sicheren Betrieb des Cloud-Dienstes als kritisch identifizierten Infrastruktur-Komponenten abdeckten ● Nachvollzug der Vorgehensweise zur Behebung von Feststellungen mit mindestens mittlerer bis sehr hoher Kritikalität in Bezug auf die Vertraulichkeit, Integrität oder Verfügbarkeit des Cloud-Dienstes ● Nachvollzug erfolgter Korrektivmaßnahmen für Feststellungen aus vorangegangenen Penetrationstests.	OPS-19
49.	**Umgang mit Schwachstellen, Störungen und Fehlern – Messungen, Analysen und Bewertungen der Verfahren** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren, ob regelmäßige Messungen, Analysen und Bewertungen zum Umgang mit Schwachstellen (Vulnerabilities) und Störungen (Incidents) vorgesehen sind, um deren fortdauernde Angemessenheit und Wirksamkeit zu überprüfen.	OPS-20

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		Prüfung der Wirksamkeit: ● Einsichtnahme in die Dokumentation zur quartalsweisen Beurteilung der Verfahren zum Umgang mit Schwachstellen und Störungen, ob auf Basis der Ergebnisse geeignete Maßnahmen zur Verbesserung initiiert wurden.	
50.	**Einbindung des Cloud-Kunden bei Störungen (Incidents)** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in relevante vertragliche Vereinbarungen hinsichtlich Art, Umfang und Turnus der Kommunikation zum Status von Incidents und deren Behebung. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise, welche die Kommunikation an den Kunden zum Status aufgetretener Incidents sowie deren Behebung dokumentieren.	OPS-21
51.	**Prüfung und Dokumentation offener Schwachstellen** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Systemeinstellungen, ob der Vulnerability-Scanner monatlich automatisiert auf bekannte Schwachstellen scannt, der Schweregrad beurteilt und eine zeitnahe Behebung auf Basis der im Zusatzkriterium genannten Zeitfenster eingeleitet wird ● Einsichtnahme in Nachweise über die Eignung der Informationsquellen für bekannte Schwachstellen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Systemprotokolle, ob der Vulnerability-Scan monatlich durchgeführt wurde ● Einsichtnahme in Nachweise über die Behebung von festgestellten Schwachstellen nach Bereitstellung des Sicherheitspatches gemäß den in dem Zusatzkriterium vorgesehen Zeitfenstern.	OPS-22
52.	**Umgang mit Schwachstellen, Störungen und Fehlern – System-Härtung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Nachweise darüber, ob relevante Branchenstandards den Verfahrensanweisungen zugrunde gelegt wurden bzw. ob die Härtung aufgrund einer Risikoanalyse durchgeführt wurde	OPS-23

6. Regelbetrieb (OPS) **Zielsetzung: Sicherstellen eines ordnungsgemäßen Regelbetriebs einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
	Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	● Soweit nicht veränderliche („immutable“) Images eingesetzt werden, Einsichtnahme in die Dokumentation über das Verfahren zur konsistenten Erstellung der Images gemäß definierter Sicherheitsvorgaben. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Konfigurations- und Logdateien, ob unveränderbare Images verwendet und in den Härtungsanleitungen umgesetzt und dokumentiert wurden.	
53.	**Separierung der Datenbestände in der Cloud-Infrastruktur** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in relevante Konzepte, welche die Separierung von Daten auf gemeinsam genutzten Ressourcen definieren. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise zur Umsetzung der Separierung der Datenbestände in der Cloud-Infrastruktur.	OPS-24

7. Identitäts- und Berechtigungsmanagement (IDM) **Zielsetzung: Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (i.d.R. privilegierte Benutzer) zur Verhinderung von unberechtigten Zugriffen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
54.	**Richtlinie für Zugangs- und Zugriffsberechtigungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert wurden, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	IDM-01

7. Identitäts- und Berechtigungsmanagement (IDM) **Zielsetzung: Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (i.d.R. privilegierte Benutzer) zur Verhinderung von unberechtigten Zugriffen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
55.	**Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Verfahrensanweisungen, ob die Einhaltung des Rollen- und Rechtekonzepts und die Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen angemessen unterstützt werden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise und Beurteilung, ob die Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen für interne und externe Mitarbeiter sowie Systemkomponenten entsprechend den Vorgaben erfolgten.	IDM-02
56.	**Sperrung und Entzug von Zugangsberechtigungen bei Inaktivität oder mehrfach fehlgeschlagenen Anmeldungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Systemeinstellungen, ob für einen Zeitraum von zwei Monaten inaktive sowie mehrfach falsch angemeldete User-IDs von Mitarbeitern und Dienstleistern gesperrt werden ● Einsichtnahme in Systemeinstellungen und Verfahrensanweisungen, ob gesperrte Berechtigungen nach sechs Monaten vollständig entzogen werden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die User-Liste, ob Sperrungen und der Entzug von Zugangsberechtigungen bei Inaktivität innerhalb der geforderten Zeitvorgaben erfolgten ● Nachvollzug, ob das Entsperren genehmigt wurde.	IDM-03
57.	**Entzug oder Anpassung von Zugriffsberechtigungen bei Veränderungen des Aufgabengebiets** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen im Hinblick auf das Vorhandensein und die Aktualität von Regelungen zum Entzug oder zur Anpassung von Berechtigungen bei Wechsel des Aufgabengebiets innerhalb der definierten Zeitfenster.	IDM-04

7. Identitäts- und Berechtigungsmanagement (IDM) **Zielsetzung: Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (i.d.R. privilegierte Benutzer) zur Verhinderung von unberechtigten Zugriffen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		Prüfung der Wirksamkeit: ● Einsichtnahme in Nachweise zur Entziehung von Benutzer-Zugriffsberechtigungen sowie zur Deaktivierung des Benutzeraccounts bei Beschäftigungsende nach spätestens 48 Stunden für privilegierte bzw. 14 Tagen für alle anderen Zugriffsberechtigungen.	
58.	**Regelmäßige Überprüfung der Zugriffsberechtigungen** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinien zur Verwaltung von Zugriffsberechtigungen im Hinblick auf eine mindestens jährliche (bei privilegierten Berechtigungen halbjährliche) Überprüfung der Zugriffsberechtigungen (Benutzerinventur) durch hierfür geeignete Mitarbeiter. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob eine Benutzerinventur innerhalb der vorgesehenen Zeiträume durchgeführt wurde und ob daraus abgeleitete Berechtigungsanpassungen zeitnah, spätestens aber 7 Tage nach ihrer Feststellung durch autorisierte Personen vorgenommen wurden.	IDM-05
59.	**Privilegierte Zugriffsberechtigungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen, hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Systemprotokolle zu Aktivitäten von Benutzern mit privilegierten Zugriffsberechtigungen und Nachvollzug der automatischen Überwachung der protokollierten Informationen auf definierte Ereignisse und ggf. potenziellen Missbrauch ● Nachvollzug von eingeleiteten Disziplinarmaßnahmen bei nachweislich missbräuchlicher Nutzung privilegierter Zugriffsberechtigungen ● Abgleich von im System abgebildeten User-IDs mit weitreichenden Berechtigungen mit dem Aufgabengebiet des Mitarbeiters.	IDM-06

7. Identitäts- und Berechtigungsmanagement (IDM) **Zielsetzung: Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (i.d.R. privilegierte Benutzer) zur Verhinderung von unberechtigten Zugriffen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
60.	**Zugriff auf Daten der Cloud-Kunden** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen, ob Zugriffe auf Daten der Cloud-Kunden durch Mitarbeiter und Dienstleister des Cloud-Anbieters durch autorisiertes Personal des Cloud-Kunden zuvor autorisiert wird, nachdem dieses die im Zusatzkriterium enthaltenen Informationen erhalten hat. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Nachweise über Zugriffe auf Daten des Cloud-Kunden und Nachvollzug, ob dem Cloud-Kunden die Informationen zeitgerecht übermittelt wurden und eine vorherige Zustimmung des Cloud Kunden vorlag.	IDM-07
61.	**Vertraulichkeit von Authentisierungsinformationen** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in relevante Richtlinien und Verfahrensanweisungen, ob die im Kriterium und im Zusatzkriterium genannten Aspekte berücksichtigt wurden ● Einsichtnahme in die Systemeinstellungen, z.B. zur Gültigkeit und Änderung von Initialpasswörtern oder zur Anwendung kryptographisch starker Passworthashfunktionen. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob alle Mitarbeiter und Dienstleister des Cloud-Anbieters eine Erklärung zur Geheimhaltung von Authentisierungsinformationen unterschrieben haben ● Einsichtnahme in Systemprotokolle hinsichtlich Einhaltung der Passwortkonventionen über den Prüfungszeitraum.	IDM-08
62.	**Authentisierungsmechanismen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Systemeinstellungen zur sachgerechten Abbildung der im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Multi-Faktor-Authentifizierung beim Zugang zu Produktionssystemen technisch erzwungen wird	IDM-09

7. Identitäts- und Berechtigungsmanagement (IDM) **Zielsetzung: Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (i.d.R. privilegierte Benutzer) zur Verhinderung von unberechtigten Zugriffen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Nachvollzug, ob Zugriffe ausschließlich über die vorgesehenen Authentifizierungsmechanismen erfolgen ● Einsichtnahme in Systemprotokolle hinsichtlich Einhaltung der Authentifizierungsmechanismen über den Prüfungszeitraum.	

8. Kryptographie und Schlüsselmanagement (CRY) **Zielsetzung: Sicherstellen eines angemessenen und wirksamen Gebrauchs von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
63.	**Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinien und Verfahren hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert wurden, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	CRY-01
64.	**Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen, ob für die Datenübertragung eine starke Verschlüsselung sowie Authentifizierung implementiert sind und ob die Verschlüsselungsverfahren dem Stand der Technik entsprechen (Algorithmen, Schlüssellängen, bekannte Schwachstellen). **Prüfung der Wirksamkeit:** ● Abgleich der definierten Vorgaben zu technischen Schutzmaßnahmen mit den implementierten Verschlüsselungseinstellungen und Parametern ● Einsichtnahme in Logaufzeichnungen hinsichtlich Veränderungen der Parameter im Prüfungszeitraum.	CRY-02

8. Kryptographie und Schlüsselmanagement (CRY) **Zielsetzung: Sicherstellen eines angemessenen und wirksamen Gebrauchs von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
65.	**Verschlüsselung von sensiblen Daten bei der Speicherung** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, vertragliche Vereinbarungen mit Cloud-Kunden und technische Maßnahmen zur Generierung, Zustellung und Aufbewahrung der privaten Schlüssel von Cloud-Kunden ● Einsichtnahme in Nachweise, ob der Cloud-Anbieter ein Verfahren etabliert hat, so dass ihm die privaten Schlüssel zu keiner Zeit zugänglich sind. **Prüfung der Wirksamkeit:** ● Nachvollzug des Verfahrens für die Schlüsselerzeugung, -verteilung und -speicherung im Hinblick auf die Nichtzugänglichkeit für den Cloud-Anbieter ● Aufgrund der zentralen Bedeutung der Schlüsselerzeugung, -verteilung und -speicherung kann bei softwaregestützter Schlüsselgenerierung eine Einsichtnahme in den Code sachgerecht sein, um festzustellen, ob er für die Schlüsselgenerierung geeignet ist („Codereview“).	CRY-03
66.	**Sichere Schlüsselverwaltung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahrensanweisungen und technische Maßnahmen hinsichtlich Aktualität, Nachvollziehbarkeit und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte ● Falls pre-shared keys verwendet wurden, Nachvollzug, ob die Besonderheiten in Bezug auf die sichere Nutzung dieses Verfahrens gesondert aufgeführt wurden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise zu allen Aspekten des Lebenszyklus in der Schlüsselverwaltung im Hinblick auf kontinuierliche Anwendung im Prüfungszeitraum.	CRY-04

9. Kommunikationssicherheit (COS) **Zielsetzung: Sicherstellen des Schutzes von Informationen in Netzen und den entsprechenden informationsverarbeitenden Systemen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
67.	**Technische Schutzmaßnahmen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die gemäß OIS-06 durchgeführte Risiko-Analyse zur angemessenen Bestimmung von technischen Schutzmaßnahmen zur zeitnahen Erkennung und Reaktion auf netzwerkbasierte Angriffe ● Einsichtnahme in die Systemeinstellungen des übergreifenden SIEM-Systems bezogen auf die Übernahme von Daten, die aus entsprechend implementierten technischen Schutzmaßnahmen stammen. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob bei netzbasierten Angriffen zeitnah die vom Cloud-Anbieter vorgesehenen Maßnahmen eingeleitet wurden.	COS-01
68.	**Sicherheitsanforderungen an Verbindungen im Netz des Cloud-Anbieters** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahrensanweisungen und technische Maßnahmen hinsichtlich Aktualität, Nachvollziehbarkeit und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte ● Einsichtnahme in Nachweise über die tatsächlich umgesetzten Maßnahmen im Hinblick auf definierte Anforderungen in Bezug auf Separierung von Sicherheitszonen, verwendete Netzwerkprotokolle, Separierung des Datenverkehrs, (Standort-) übergreifende Kommunikation. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Sicherheitsmaßnahmen über den Prüfungszeitraum unverändert eingerichtet waren ● Nachvollzug, ob die physische bzw. logische Trennung von Netzen der Cloud-Kunden im Prüfungszeitraum umgesetzt war.	COS-02
69.	**Überwachung von Verbindungen im Netz des Cloud-Anbieters** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahrensanweisungen hinsichtlich Aktualität, Nachvollziehbarkeit und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte	COS-03

9. Kommunikationssicherheit (COS) **Zielsetzung: Sicherstellen des Schutzes von Informationen in Netzen und den entsprechenden informationsverarbeitenden Systemen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Einsichtnahme in Nachweise über technische und organisatorische Maßnahmen zur Umsetzung der im Kriterium genannten Aspekte, z.B. Separierung von Netzen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Firewall- oder Filter-Regeln an Netzübergängen, ob der Datenverkehr verfahrensgemäß gefiltert, kontrolliert oder blockiert wird ● Einsichtnahme in Nachweise zur mindestens jährlich durchzuführenden Überprüfung von Konzeption und Konfiguration des Netzes ● Einsichtnahme in Nachweise zu durchgeführten Risikoanalysen und Feststellung, ob im Bedarfsfall eine Risikobeurteilung gemäß OIS-06 durchgeführt und Maßnahmen zur Behandlung definiert und nachverfolgt wurden (vgl. OPS-18) ● Einsichtnahme in Nachweise zur Prüfung und Feststellung der geschäftlichen Rechtfertigung für die Verwendung aller Dienste, Protokolle und Ports.	
70.	**Netzübergreifende Zugriffe** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahrensanweisungen und Systemeinstellungen, ob alle Netzwerkperimeter in Sicherheitsgateways eingebunden sind ● Einsichtnahme in Nachweise, ob Prozesse zur Etablierung und Nutzung von Zugangsberechtigungen für netzübergreifende Zugriffe auf Basis der Sicherheitsanalyse definiert und dabei die Anforderungen der Cloud-Kunden beachtet wurden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise, ob die Einstellungen für die Gateways über den Prüfungszeitraum bestanden und alle Netzperimeter abgedeckt haben ● Einsichtnahme in Nachweise über netzübergreifende Zugriffe im Prüfungszeitraum auf Einhaltung der Vorgaben.	COS-04
71.	**Netze zur Administration** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien, Verfahrensanweisungen und Systemeinstellungen, ob getrennte Netze für die Administration, Migration und zur Erzeugung	COS-05

9. Kommunikationssicherheit (COS) **Zielsetzung: Sicherstellen des Schutzes von Informationen in Netzen und den entsprechenden informationsverarbeitenden Systemen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		virtueller Maschinen eingerichtet wurden und der Zugriff nur durch eine Multi-Faktor-Authentifizierung erfolgt. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob der Zugriff über den Zugriffszeitraum nur über eine Multi-Faktor-Authentifizierung möglich war ● Einsichtnahme in Nachweise, die belegen, dass die logische Trennung während des Betrachtungszeitraums bestanden hat.	
72.	**Segregation des Datenverkehrs in gemeinsam genutzten Netzumgebungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen hinsichtlich Aktualität, Nachvollziehbarkeit und Vollständigkeit der Inhalte im Hinblick auf die Trennung des Datenverkehrs der Cloud-Kunden in gemeinsam genutzten Netzwerken. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die logische Segmentierung über den Prüfungszeitraum eingerichtet war.	COS-06
73.	**Dokumentation des Netzes** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation der Netztopologie und Beurteilung, ob die Dokumentation nachvollziehbar, vollständig und aktuell ist und die im Kriterium genannten Aspekte berücksichtigt wurden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise aus Störungen, ob die Dokumentation zur zeitgerechten Wiederherstellung ausreichend gewesen ist.	COS-07
74.	**Richtlinien zur Datenübertragung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte ● Einsichtnahme in Richtlinien und Anweisungen, ob durch die Vorgaben ein Bezug zur Klassifikation von Informationen hergestellt wurde. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert wurden, – für die Mitarbeiter verfügbar sind,	COS-08

9. Kommunikationssicherheit (COS) **Zielsetzung: Sicherstellen des Schutzes von Informationen in Netzen und den entsprechenden informationsverarbeitenden Systemen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		– Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	

10. Portabilität und Interoperabilität (PI) **Zielsetzung: Ermöglichen der Eigenschaft, den Cloud-Dienst über andere Cloud-Dienste oder IT-Systemen der Cloud-Kunden ansprechen zu können, die gespeicherten Daten bei Beendigung des Auftragsverhältnisses zu beziehen und beim Cloud-Anbieter sicher zu löschen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
75.	**Dokumentation und Sicherheit der Eingangs- und Ausgangs-Schnittstellen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation hinsichtlich Interoperabilität durch dokumentierte Vorgaben zu Eingangs- und Ausgangs-Schnittstellen sowie zur Anwendung von standardisierten Kommunikationsprotokollen, insb. um die Rückgabe der Daten ermöglichen zu können. **Prüfung der Wirksamkeit:** ● Nachvollzug der tatsächlich verwendeten/eingestellten Netzwerkprotokolle im Hinblick auf die Einhaltung der definierten Vorgaben.	PI-01
76.	**Vertragliche Vereinbarungen zur Bereitstellung von Daten** Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Standardvertragswesen mit Cloud-Kunden hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium und im Zusatzkriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in vertragliche Vereinbarungen mit Kunden, ob die Aspekte aus dem Basiskriterium und die rechtlichen und regulatorischen Anforderungen im aktuellen Stand adressiert sind ● Nachvollzug eines Beispieldatenabzugs auf Vollständigkeit und Integrität.	PI-02
77.	**Sichere Datenlöschung**	**Prüfung der Angemessenheit:** ● Einsichtnahme in die definierten Vorgaben und Methoden, ob Inhaltsdaten, Datensicherungen und Metadaten von Cloud-Kunden im Falle der Beendigung des	PI-03

10. Portabilität und Interoperabilität (PI) **Zielsetzung: Ermöglichen der Eigenschaft, den Cloud-Dienst über andere Cloud-Dienste oder IT-Systemen der Cloud-Kunden ansprechen zu können, die gespeicherten Daten bei Beendigung des Auftragsverhältnisses zu beziehen und beim Cloud-Anbieter sicher zu löschen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
	Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	Auftragsverhältnisses gemäß den vertraglichen Vereinbarungen vollständig gelöscht werden ● Einsichtnahme in die Löschverfahren, ob eine Datenwiederherstellung mit forensischen Mitteln unterbunden wird. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über die Durchführung von Datenlöschungen bezogen auf die Einhaltung der vertraglichen Vereinbarungen.	

11. Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV) **Zielsetzung: Sicherstellen der Informationssicherheit im Entwicklungszyklus von Informationssystemen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
78.	**Richtlinien zur Entwicklung/Beschaffung von Informationssystemen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in entsprechende Richtlinien und Anweisungen für die ordnungsgemäße Entwicklung oder Beschaffung von Informationssystemen, für die Entwicklung oder den Betrieb des Cloud-Dienstes und Beurteilung der Vollständigkeit betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert wurden, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	DEV-01
79.	**Auslagerung der Entwicklung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Vertragsunterlagen/SLAs zwischen Cloud-Anbieter und externen Dienstleistern und Beurteilung der Vollständigkeit betreffend die im Kriterium genannten Aspekte.	DEV-02

11. Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV) **Zielsetzung: Sicherstellen der Informationssicherheit im Entwicklungszyklus von Informationssystemen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		Prüfung der Wirksamkeit: ● Einsichtnahme in die durch den Cloud-Anbieter vorgenommenen Abnahmeprüfungen der Qualität der erbrachten Leistungen ● Einsichtnahme in Nachweise über die vom Cloud-Anbieter durchgeführten Überprüfungen des externen Dienstleisters zum Ausschluss bekannter Schwachstellen.	
80.	**Richtlinien zur Änderung von Informationssystemen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Richtlinien und Verfahren zum Change Management hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert wurden, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	DEV-03
81.	**Programm zur Sicherheitsausbildung und Sensibilisierung bezüglich kontinuierlicher Software-Bereitstellung und zugehöriger Systeme, Komponenten oder Werkzeuge** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Programm zur Sicherheitsausbildung in der Software-Entwicklung und Beurteilung von Aktualität und Vollständigkeit der Inhalte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise zur Durchführung der Sicherheitsausbildung in der Software-Entwicklung (z.B. Teilnehmerlisten, Erfolgskontrollen).	DEV-04
82.	**Risikobewertung, Kategorisierung und Priorisierung von Änderungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Change Management-Richtlinien, -Anweisungen und -Maßnahmen, ob Änderungen einer Risikoanalyse unterzogen und kategorisiert und priorisiert werden. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob Risiken bei Änderungen von Systemen im Ticket, Change Request o.ä. erhoben, berücksichtigt und bewertet wurden.	DEV-05

11. Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV) **Zielsetzung: Sicherstellen der Informationssicherheit im Entwicklungszyklus von Informationssystemen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Einsichtnahme in die Nachweise über die Risikobewertung, Kategorisierung und Priorisierung von Änderungen hinsichtlich Einhaltung der Richtlinien und Vorgaben.	
83.	**Testen der Änderungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Testvorgaben (Umfang, Qualifikation des verantwortlichen Personals) bzw. in Testparameter (im Fall von automatisierten Testverfahren) in Bezug auf Vollständigkeit und Aktualität betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Nachweise über die durchgeführten Tests hinsichtlich Einhaltung der Richtlinien zum Change Management ● Einsichtnahme in die Nachweise zur Behebung von Fehlern und Schwachstellen abhängig vom Schweregrad.	DEV-06
84.	**Protokollierung von Änderungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Rollen- und Rechtekonzept gemäß IDM-01 und Beurteilung der Autorisierungsmechanismen hinsichtlich des Zugriffs auf den Quellcode und die für die Entwicklung des Cloud-Dienstes relevanten Informationen ● Einsichtnahme in das Tool zur Quellcode-Verwaltung und Software-Bereitstellung, ob Änderungen am Quellcode Benutzern oder Systemkomponenten zugeordnet werden können und protokolliert werden. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die tatsächlich erfolgten Zugriffe autorisiert waren ● Nachvollzug, ob die Protokollierung über den Prüfungszeitraum unverändert war und aktiv gewesen ist.	DEV-07
85.	**Versionskontrolle** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren, ob eine Versionskontrolle eingerichtet ist, die auch ein Zurückrollen von Änderungen möglich macht. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Versionskontrolle über den Prüfungszeitraum unverändert war und aktiv gewesen ist	DEV-08

11. Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV) **Zielsetzung: Sicherstellen der Informationssicherheit im Entwicklungszyklus von Informationssystemen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Sofern im Prüfungszeitraum stattgefunden: Einsichtnahme in Nachweise über die Durchführung der Abläufe zum Zurückrollen von Änderungen.	
86.	**Freigaben zur Bereitstellung in der Produktionsumgebung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen, ob Änderungen am Cloud-Dienst durch autorisiertes Personal oder autorisierte Systemkomponenten freigegeben werden ● Einsichtnahme in Standardverträge, unter welchen Voraussetzungen Cloud-Kunden in die Freigabe eingebunden werden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über die Durchführung von Freigaben unter Beachtung der vertraglichen Vereinbarungen mit Cloud-Kunden auf die Einhaltung der Vorgaben.	DEV-09
87.	**Trennung der Umgebungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation der Systemlandschaft auf Existenz von getrennten Entwicklungs-, Test- und Produktivumgebungen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise darüber, dass keine Produktivdaten in Entwicklungs- und Testumgebungen kopiert und dort verwendet werden.	DEV-10

12. Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO) **Zielsetzung: Sicherstellen des Schutzes von Informationen auf die Dienstleister bzw. Lieferanten des Cloud-Anbieters (Unterauftragnehmer) zugreifen können, sowie Überwachung der vereinbarten Leistungen und Sicherheitsanforderungen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
88.	**Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren zur Steuerung und Überwachung Dritter hinsichtlich Aktualität und Vollständigkeit der Inhalte im Hinblick auf die im Kriterium genannten Aspekte.	SSO-01

12. Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO) **Zielsetzung: Sicherstellen des Schutzes von Informationen auf die Dienstleister bzw. Lieferanten des Cloud-Anbieters (Unterauftragnehmer) zugreifen können, sowie Überwachung der vereinbarten Leistungen und Sicherheitsanforderungen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
	Das Basiskriterium und das Zusatzkriterium des BSI C5:2020 sind zu berücksichtigen.	● Einsichtnahme in Verträge mit Subdienstleistern, ob eine Berichterstattung durch Dritte oder Informations- und Prüfrechte vereinbart sind. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert wurden, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	
89.	**Risikobeurteilung der Dienstleister und Lieferanten** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren zur Risikobeurteilung von Dienstleistern und Lieferanten hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über die Durchführung von Risikobeurteilungen von Dienstleistern und Lieferanten auf Berücksichtigung der im Kriterium genannten Aspekte. ● Einsichtnahme in Nachweise zur mindestens jährlich durchgeführten Überprüfung der Risikobeurteilung.	SSO-02
90.	**Verzeichnis der Dienstleister und Lieferanten** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Aufzeichnungen über Dienstleister und Lieferanten des Cloud-Anbieters hinsichtlich Aktualität und Vollständigkeit der im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob im Verzeichnis alle Dienstleister und Lieferanten des Cloud-Anbieters enthalten sind ● Einsichtnahme in Nachweise über eine mindestens jährlich durchgeführte Überprüfung der Angaben auf Vollständigkeit, Richtigkeit und Gültigkeit.	SSO-03
91.	**Überwachung der Einhaltung der Anforderungen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen, ob die vertraglichen Vereinbarungen	SSO-04

12. Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO) **Zielsetzung: Sicherstellen des Schutzes von Informationen auf die Dienstleister bzw. Lieferanten des Cloud-Anbieters (Unterauftragnehmer) zugreifen können, sowie Überwachung der vereinbarten Leistungen und Sicherheitsanforderungen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
	Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	mit Dienstleistern über Berichterstattungen die Risikobeurteilung des Cloud-Anbieters widerspiegeln ● Einsichtnahme in Richtlinien und Verfahrensanweisungen, ob die vereinbarten Berichterstattungen regelmäßig angefordert, überwacht und die daraus erhaltenen Ergebnisse entsprechend der im Kriterium genannten Aspekte nachverfolgt werden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise, ob die vertraglich vereinbarten Berichterstattungen gemäß den Richtlinien und Verfahrensanweisungen regelmäßig angefordert, ausgewertet und die Ergebnisse nachverfolgt wurden.	
92.	**Ausstiegsstrategie für den Bezug von Leistungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Ausstiegsstrategien für den Bezug von Leistungen im Fall einer sehr hohen Abhängigkeit des Cloud-Anbieters vom Dienstleister und Lieferanten betreffend die im Kriterium genannten Aspekte und die Berücksichtigung im BCM. **Prüfung der Wirksamkeit** ● Nachvollzug, ob Ausstiegsstrategien im Rahmen von BCM-Tests berücksichtigt werden.	SSO-05

13. Umgang mit Sicherheitsvorfällen (SIM) **Zielsetzung: Gewährleisten eines konsistenten und umfassenden Vorgehens zur Erfassung, Bewertung, Kommunikation und Behandlung von Sicherheitsvorfällen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
93.	**Richtlinie für den Umgang mit Sicherheitsvorfällen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren zum Umgang mit Sicherheitsvorfällen hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. ● Einsichtnahme in Dokumentationen (Aufgabenbeschreibungen, Organisationsstruktur) zum Aufbau eines CERTs. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert wurden, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	SIM-01
94.	**Bearbeitung von Sicherheitsvorfällen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Vorgehensmodell sowie in relevante Konzepte, Richtlinien und Verfahrensanweisungen zum Umgang mit Sicherheitsvorfällen im Hinblick auf den Einsatz qualifizierten Personals und die Klassifizierung, Priorisierung und Ursachenanalyse. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Dokumentation von Sicherheitsvorfällen und Beurteilung, ob diese klassifiziert und priorisiert sowie Maßnahmen getroffen wurden, um diese Vorfälle in Zukunft zu vermeiden.	SIM-02
95.	**Dokumentation und Berichterstattung über Sicherheitsvorfälle** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen, ob Prozesse vom Cloud-Anbieter definiert sind, die eine Dokumentation der Lösung von Sicherheitsvorfällen und eine Berichterstattung an die Kunden vorsehen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Berichterstattung zu Sicherheitsvorfällen im Hinblick auf die Einhaltung der Vorgaben zur Dokumentation und Übermittlung an die Cloud-Kunden gemäß den vertraglichen Vereinbarungen.	SIM-03

13. Umgang mit Sicherheitsvorfällen (SIM) **Zielsetzung: Gewährleisten eines konsistenten und umfassenden Vorgehens zur Erfassung, Bewertung, Kommunikation und Behandlung von Sicherheitsvorfällen.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
96.	**Verpflichtung der Nutzer zur Meldung von Sicherheitsvorfällen an eine zentrale Stelle** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Sensibilisierungsmaßnahmen hinsichtlich der Verpflichtung von Mitarbeitern und Geschäftspartnern zur zeitnahen Meldung von Sicherheitsereignissen mit Bezug auf den Cloud-Dienst ● Einsichtnahme in vertraglich festgelegte Klauseln ● Einsichtnahme in die Planung von Kommunikationsmaßnahmen. **Prüfung der Wirksamkeit:** ● Befragung von Mitarbeitern hinsichtlich erfolgter Sensibilisierungsaktionen ● Nachvollzug des Inhalts der erfolgten Kommunikation gemäß den Vorgaben (z.B. Nennung der zentralen Stelle zur Meldung von Sicherheitsvorfällen).	SIM-04
97.	**Auswertung und Lernprozess** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Mechanismen zur Messung, Meldung, Überwachung und Auswertung von Sicherheitsvorfällen und Beurteilung, ob ein Prozess zur Evaluierung von erweiterten Schutzmaßnahmen vorgesehen ist. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Auswertungen sowie „Lessons Learned“ und daraus abgeleitete Maßnahmenpläne für zukünftig wiederkehrende Vorfälle.	SIM-05

14. Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM) **Zielsetzung: Planen, Implementieren, Aufrechterhalten und Testen von Verfahren und Maßnahmen zur Kontinuität des Geschäftsbetriebs und für das Notfallmanagement.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
98.	**Verantwortung durch die Unternehmensleitung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Rahmenwerk mit Richtlinien, Verfahrensanweisungen, sowie sonstigen relevanten Dokumenten zum Business Continuity Management	BCM-01

14. Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM) **Zielsetzung: Planen, Implementieren, Aufrechterhalten und Testen von Verfahren und Maßnahmen zur Kontinuität des Geschäftsbetriebs und für das Notfallmanagement.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		(BCM) / Notfallkonzept im Hinblick auf die Verantwortlichkeit und die Grundhaltung der Unternehmensleitung sowie die Bereitstellung von Ressourcen ● Einsichtnahme in die Kommunikation der Unternehmensleitung zum Thema BCM. **Prüfung der Wirksamkeit:** ● Nachvollzug der Zugänglichkeit/Kommunikation der Richtlinien und Anweisungen für die Mitarbeiter/Zielgruppe.	
99.	**Richtlinien und Verfahren zur Business Impact Analyse** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren hinsichtlich Aktualität und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert wurden, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	BCM-02
100.	**Planung der Betriebskontinuität** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Pläne zur betrieblichen Kontinuität und in Notfallpläne hinsichtlich Aktualität, Konsistenz (aller Pläne der verschiedenen Standorte) und Vollständigkeit der Inhalte betreffend die im Kriterium genannten Aspekte ● Einsichtnahme in die Pläne zum BCM auf Konsistenz mit den Ergebnissen der Business Impact Analyse ● Einsichtnahme in das Rahmenwerk, ob bei den geplanten Regelungen und Maßnahmen gängige Standards (z.B. ISO, BSI) berücksichtigt wurden. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die implementierten Wiederherstellungsverfahren den geplanten Verfahren entsprechen und kontinuierlich durchgeführt und aktualisiert wurden. ● Nachvollzug der Einhaltung von Verantwortlichkeiten bei der Inkraftsetzung von (Teil-)Plänen.	BCM-03

14. Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM) **Zielsetzung: Planen, Implementieren, Aufrechterhalten und Testen von Verfahren und Maßnahmen zur Kontinuität des Geschäftsbetriebs und für das Notfallmanagement.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Einsichtnahme in Dokumente zu im Prüfungszeitraum vorgefallenen Notfällen auf Einhaltung der in den Plänen vorgeschriebenen Vorgehensweise	
101.	**Verifizierung, Aktualisierung und Test der Betriebskontinuität** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Vorgaben, ob die Notfallpläne mindestens jährlich oder bei relevanten Umfeld-änderungen überprüft und aktualisiert werden ● Einsichtnahme in die Testvorbereitungen und die Dokumentation der Testverfahren im Hinblick auf die Berücksichtigung aller relevanten Schadensszenarien ● Einsichtnahme in Nachweise, ob die Kunden und relevante Dritte angemessen in die Tests einbezogen werden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Pläne zur betrieblichen Kontinuität und die Notfallpläne, ob diese mindestens jährlich oder bei umgebungsbedingten Veränderungen aktualisiert wurden ● Einsichtnahme in Nachweise über mindestens jährlich durchgeführte Tests und Abgleich der Einhaltung der Vorgaben in Richtlinien und relevanten Dokumentationen ● Einsichtnahme in Nachweise darüber, dass Testergebnisse je nach Relevanz für zukünftige Maßnahmen der betrieblichen Kontinuität berücksichtigt werden.	BCM-04

15. Compliance (COM) **Zielsetzung: Vermeiden von Verstößen gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Anforderungen zur Informationssicherheit und Überprüfen der Einhaltung.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
102.	**Identifizierung anwendbarer gesetzlicher, regulatorischer, selbstauferlegter oder vertraglicher Anforderungen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Vorgaben und Richtlinien, ob die für die Cloud-Dienste relevanten gesetzlichen, regulatorischen, selbstauferlegten und vertraglichen Anforderungen in Bezug auf die Informationssicherheit vollständig definiert und dokumentiert sind. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert wurden, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	COM-01
103.	**Richtlinie für die Planung und Durchführung von Audits** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen zur Planung und Durchführung unabhängiger, externer Audits und Beurteilung der Übereinstimmung mit den Anforderungen gemäß SP-01. ● Einsichtnahme in Richtlinien und Verfahrensanweisungen betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Richtlinien – an die Mitarbeiter kommuniziert wurden, – für die Mitarbeiter verfügbar sind, – Verfahren zur entsprechenden Handhabung von Aktualisierungen enthalten (vgl. SP-02).	COM-02

15. Compliance (COM) **Zielsetzung: Vermeiden von Verstößen gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Anforderungen zur Informationssicherheit und Überprüfen der Einhaltung.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
104.	**Interne Audits des Informationssicherheitsmanagementsystems** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Planung von internen Audits, ob die Compliance des Informationssicherheitsmanagementsystems mit den relevanten und anwendbaren gesetzlichen, regulatorischen, selbstauferlegten und vertraglichen Anforderungen sowie die Einhaltung der Richtlinien und Arbeitsanweisungen mindestens jährlich überprüft wird. **Prüfung der Wirksamkeit:** ● Einsichtnahme und Auswertung der Ergebnisdokumentation der mindestens jährlich durchgeführten Compliance-Prüfung einschließlich der Dokumentation der identifizierten Abweichungen und der Erstellung eines Maßnahmenplans ● Einsichtnahme in die Dokumentation, dass die in internen Audits identifizierten Schwachstellen und Abweichungen gemäß der Richtlinie für den Umgang mit Risiken (vgl. OIS-06) bewertet und in einen Maßnahmenplan überführt wurden.	COM-03
105.	**Informationen über die Informationssicherheitsleistung und Managementbewertung des ISMS** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Berichtswesen, ob die oberste Leitung des Cloud- Anbieters regelmäßig über die Eignung, Angemessenheit und Wirksamkeit des ISMS informiert wird. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise, dass die Informationen über das ISMS mindestens jährlich in die Managementbewertung des ISMS einfließen.	COM-04

16. Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ) **Zielsetzung: Gewährleisten eines angemessenen Umgangs mit Ermittlungsanfragen staatlicher Stellen hinsichtlich juristischer Überprüfung, Information der Cloud-Kunden und Begrenzung des Zugriffs auf oder der Offenlegung von Daten.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
106.	**Juristische Beurteilung von Ermittlungsanfragen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen zum Umgang mit Ermittlungsanfragen staatlicher Stellen, ob diese durch qualifiziertes Personal des Cloud-Anbieters juristisch beurteilt werden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Dokumentation, ob staatliche Ermittlungsanfragen auf eine anwendbare und rechtsgültige Grundlage geprüft wurden.	INQ-01
107.	**Information der Cloud-Kunden über Ermittlungsanfragen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen zur Behandlung von Ermittlungsanfragen staatlicher Stellen, ob betroffene Cloud-Kunden informiert werden, soweit dem nicht rechtliche Gründe entgegenstehen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Dokumentation, dass betroffene Cloud-Kunden über Ermittlungsanfragen staatlicher Stellen informiert wurden, soweit diesem nicht rechtliche Gründe entgegenstanden.	INQ-02
108.	**Voraussetzungen für den Zugriff auf oder der Offenlegung von Daten bei Ermittlungsanfragen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen zur Behandlung von Ermittlungsanfragen staatlicher Stellen, ob ein Zugriff auf oder die Offenlegung von Daten der Cloud-Kunden nur auf Basis einer juristischen Prüfung stattfindet. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Dokumentation, dass bei einer Offenlegung von Daten die Prüfung der jeweiligen Ermittlungsanfrage staatlicher Stellen ergab, dass eine anwendbare und rechtsgültige Rechtsgrundlage vorlag und der Ermittlungsanfrage daher stattgegeben werden musste.	INQ-03
109.	**Begrenzung des Zugriffs auf oder der Offenlegung von Daten bei Ermittlungsanfragen**	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen zur Behandlung von Ermittlungsan-	INQ-04

16. Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ) **Zielsetzung: Gewährleisten eines angemessenen Umgangs mit Ermittlungsanfragen staatlicher Stellen hinsichtlich juristischer Überprüfung, Information der Cloud-Kunden und Begrenzung des Zugriffs auf oder der Offenlegung von Daten.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
	Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	fragen staatlicher Stellen, ob nur die Daten herausgegeben werden, die Gegenstand der Ermittlungsanfrage sind ● Einsichtnahme in Richtlinien und Verfahrensanweisungen, ob nicht klar abgrenzbare Daten anonymisiert oder pseudonymisiert werden. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Protokollierung des Zugriffs staatlicher Stellen auf Daten der Cloud-Kunden ● Einsichtnahme in Dokumentationen, welche Daten offengelegt und welche Daten anonymisiert oder pseudonymisiert wurden.	

17. Produktsicherheit (PSS) **Zielsetzung: Bereitstellen aktueller Informationen zur sicheren Konfiguration und über bekannte Schwachstellen des Cloud-Dienstes für Cloud-Kunden, geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der Cloud-Kunden.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
110.	**Leitlinien und Empfehlungen für Cloud-Kunden** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Leitlinien und Empfehlungen des Cloud-Anbieters für die Cloud-Kunden, ob diese die inhaltlichen Anforderungen des Kriteriums vollständig abdecken. **Prüfung der Wirksamkeit:** ● Nachvollzug, dass die Leitlinien und Empfehlungen den Cloud-Kunden zur Verfügung gestellt wurden (z.B. über einen Online-Ablageort). ● Nachvollzug, dass die Leitlinien und Empfehlungen regelmäßig aktualisiert wurden, so dass sie mit der produktiven Version des Cloud-Dienstes übereinstimmen.	PSS-01

17. Produktsicherheit (PSS) **Zielsetzung: Bereitstellen aktueller Informationen zur sicheren Konfiguration und über bekannte Schwachstellen des Cloud-Dienstes für Cloud-Kunden, geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der Cloud-Kunden.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
111.	**Identifikation von Schwachstellen des Cloud-Dienstes** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahrensanweisungen betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Dokumentationen, ob Schwachstellen im Rahmen des Softwareentwicklungsprozesses identifiziert, deren Risiken bewertet und Maßnahmen zur zeitnahen Behebung durchgeführt wurden.	PSS-02
112.	**Online-Register bekannter Schwachstellen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Nachweise darüber, dass der Cloud-Anbieter selbst ein Online-Register bekannter Schwachstellen für den Cloud-Dienst und die vom Cloud-Anbieter bereitgestellten Assets betreibt oder auf ein solches verweist und dieses den Anforderungen des Kriteriums entspricht. **Prüfung der Wirksamkeit:** ● Nachvollzug, dass das Online-Register allgemein zugänglich ist ● Einsichtnahme in Nachweise, dass das Register täglich aktualisiert wird und die im Kriterium genannten Aspekte adressiert werden.	PSS-03
113.	**Fehlerbehandlungs- und Protokollierungsmechanismen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Dokumentationen, ob Fehlerbehandlungs- und Protokollierungsmechanismen des Cloud-Dienstes eingerichtet sind, die die Aspekte des Kriteriums erfüllen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Systemeinstellungen, ob die Fehlerbehandlungs- und Protokollierungsmechanismen wie beschrieben eingerichtet und über den Prüfungszeitraum nicht verändert wurden. ● Einsichtnahme in die Konfiguration von Zugriffsrechten auf Protokolldateien im Hinblick auf die Übereinstimmung mit den Vorgaben aus PSS-08 und IDM-01.	PSS-04

17. Produktsicherheit (PSS) **Zielsetzung: Bereitstellen aktueller Informationen zur sicheren Konfiguration und über bekannte Schwachstellen des Cloud-Dienstes für Cloud-Kunden, geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der Cloud-Kunden.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
114.	**Authentisierungsmechanismen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentationen, ob eine starke Authentisierung (z.B. durch zwei oder mehrere Faktoren) an allen Zugangspunkten vorgesehen ist und für privilegierte Benutzer erzwungen wird. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Systemeinstellungen, ob Authentisierungsmechanismen für Anwender an allen Zugangspunkten zum Cloud-Dienst über den Prüfungszeitraum eingerichtet waren und eine starke Authentisierung für privilegierte Anwender, IT-Komponenten und Anwendungen erzwungen wurde.	PSS-05
115.	**Session Management** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation zum Session Management und Beurteilung, ob dieses dem aktuellen Stand der Technik entspricht, gegen bekannte Angriffe geschützt ist und inaktive Sessions ungültig macht ● Einsichtnahme in die Systemeinstellungen des Cloud-Dienstes, ob der Cloud-Kunde das Zeitintervall für zeitbasiertes Session Management, soweit technisch möglich, selbst konfigurieren kann. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Systemeinstellungen bezogen auf das Session Management auf Übereinstimmung mit den Vorgaben im Prüfungszeitraum.	PSS-06
116.	**Vertraulichkeit von Authentisierungsinformationen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren betreffend die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Systemprotokolle auf Einhaltung der Passwortkonventionen einschließlich der initialen Erstellung der Passwörter über den Prüfungszeitraum	PSS-07

17. Produktsicherheit (PSS) **Zielsetzung: Bereitstellen aktueller Informationen zur sicheren Konfiguration und über bekannte Schwachstellen des Cloud-Dienstes für Cloud-Kunden, geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der Cloud-Kunden.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Einsichtnahme in Nachweise, dass Cloud-Kunden über die Änderung oder das Zurücksetzen von Passwörtern im Prüfungszeitraum informiert wurden. ● Einsichtnahme in die Systemeinstellungen, dass die serverseitige Speicherung von Passwörtern durch den Cloud-Anbieter mit kryptographisch starken Hash-Funktionen, die dem Stand der Technik entsprechen, in Kombination mit mindestens 32 Bit langen Salt-Werten im Prüfungszeitraum erfolgt ist.	
117.	**Rollen- und Rechtekonzept** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation zum Rollen- und Rechtekonzept hinsichtlich Aktualität und Vollständigkeit betreffend die im Kriterium genannten Aspekte ● Einsichtnahme in Nachweise, ob sich das Least-Privilege-Prinzip, das Need-to-Know-Prinzip und die Funktionstrennung in der Ausgestaltung der zur Verfügung gestellten Rollenprofile widerspiegelt. **Prüfung der Wirksamkeit:** ● Nachvollzug, dass die Dokumentation zum Rollen- und Rechtekonzept den Cloud-Kunden zur Verfügung steht ● Einsichtnahme in Nachweise darüber, dass sofern Änderungen an den vom Cloud-Anbieter zur Verfügung gestellten Funktionen erfolgt sind, dies zeitnah im Rollen- und Rechtekonzept berücksichtigt und den Kunden zur Verfügung gestellt wurden.	PSS-08
118.	**Autorisierungsmechanismen** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation der Zugriffskontrollen hinsichtlich Aktualität und Vollständigkeit betreffend die im Kriterium genannten Aspekte	PSS-09

17. Produktsicherheit (PSS) **Zielsetzung: Bereitstellen aktueller Informationen zur sicheren Konfiguration und über bekannte Schwachstellen des Cloud-Dienstes für Cloud-Kunden, geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der Cloud-Kunden.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Einsichtnahme in die Vorgaben zur Validierung der Funktionsfähigkeit der Autorisierungsmechanismen im Hinblick auf die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in die Systemeinstellungen von Zugriffskontrollen auf Übereinstimmung mit den Vorgaben ● Einsichtnahme in Nachweise über die Validierung neuer oder geänderter Funktionen der Autorisierungsmechanismen vor Bereitstellung ● Einsichtnahme in Nachweise, dass identifizierte Mängel gemäß branchenüblichen Metriken beurteilt und zeitnah behoben wurden ● Einsichtnahme, dass nicht behobene Mängel im Online-Register bekannter Schwachstellen (vgl. PSS-02) dargestellt sind.	
119.	**Software-defined Networking** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation zu Software-defined Networking (SDN) hinsichtlich Aktualität und Vollständigkeit betreffend die im Kriterium genannten Aspekte ● Einsichtnahme in die Vorgaben zur Validierung der Funktionsfähigkeit der SDN-Funktionen im Hinblick auf die im Kriterium genannten Aspekte. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über die Validierung neuer oder geänderter SDN-Funktionalitäten vor Bereitstellung ● Einsichtnahme in Nachweise, dass identifizierte Mängel risikoorientiert beurteilt und behoben wurden.	PSS-10
120.	**Images für virtuelle Maschinen und Container** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation zur Erstellung, Aktualisierung und Bereitstellung von Images und Containern betreffend die im Kriterium genannten Aspekte	PSS-11

17. Produktsicherheit (PSS) **Zielsetzung: Bereitstellen aktueller Informationen zur sicheren Konfiguration und über bekannte Schwachstellen des Cloud-Dienstes für Cloud-Kunden, geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der Cloud-Kunden.**			
Nr.	Basiskriterium oder Zusatzkriterium	Beispielhafte Prüfungshandlungen	Referenz (C5 #)
		● Einsichtnahme in die Systemkonfiguration, dass die Auswahl von Images und Containern durch den Cloud-Kunden eingeschränkt werden kann. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über die Durchführung von Härtungsmaßnahmen, um zu beurteilen, ob die im Prüfungszeitraum bereitgestellten Images nach allgemein akzeptierten Branchenstandards gehärtet waren ● Einsichtnahme in Nachweise über die Kommunikation von im Prüfungszeitraum vorgenommenen Änderungen an Images und Containern gegenüber der Vorversion an Cloud-Kunden.	
121.	**Lokationen der Datenverarbeitung und -speicherung** Das Basiskriterium des BSI C5:2020 ist zu berücksichtigen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation der Cloud-Architektur und die Vorgaben zur Systemkonfiguration bzgl. Lokationen der Datenverarbeitung und -speicherung, sofern die Vereinbarungen bzw. die vom Cloud-Anbieter bereitgestellten Funktionen den Cloud-Kunden die Möglichkeit geben, die Lokationen der Datenverarbeitung und -speicherung festzulegen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise, dass die Systemkonfiguration bzgl. Lokationen der Datenverarbeitung und Speicherung im Prüfungszeitraum nicht geändert wurde, es sei denn, dies entspricht den vertraglichen Vereinbarungen mit den Cloud-Kunden.	PSS-12

18. PaaS **Zielsetzung: Einhaltung der Sicherheits- und Ordnungsmäßigkeitsanforderungen gemäß IDW RS FAIT 5 i.V.m. IDW RS FAIT 1 für das Servicemodell PaaS**			
Nr.	Anforderungen	Beispielhafte Prüfungshandlungen	Referenz
122.	**Erweiterung der „Richtlinie zum Umgang mit und Sicherheitsanforderungen an Dienstleister und Lieferanten des Cloud-Anbieters“** Die Richtlinien und Anweisungen nach Nummer 88. (SSO-01) sind um Ordnungsmäßigkeitsanforderungen ergänzt und an Subdienstleister des Cloudanbieters kommuniziert. Dies gilt nur, sofern über die Plattform Funktionen zur Verfügung gestellt werden, die Voraussetzung für die Ordnungsmäßigkeit der Gesamtlösung sind. Hierzu können gehören: ● Protokollierungsfunktionen ● Berechtigungsverwaltung ● Archivierungsfunktionen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren hinsichtlich Aktualität und Vollständigkeit der Inhalte gemäß den geforderten Kriterien/Vorgaben. **Prüfung der Wirksamkeit:** ● Nachvollzug der Zugänglichkeit der Richtlinien und Verfahrensanweisungen für Mitarbeiter.	*IDW RS FAIT 5*, Tz. 19
123.	**Dienstleister – Eskalationsverfahren** Der Cloud-Anbieter hat mit den Kunden ein Eskalationsverfahren vereinbart, damit die Kunden eine nicht vertragsgemäße Leistung geltend machen können (Schlecht- oder Nichtleistung).	**Prüfung der Angemessenheit:** ● Einsichtnahme in Vereinbarungen mit Kunden im Hinblick auf die Bedingungen für die Geltendmachung von Schlecht- und Nichtleistungen. **Prüfung der Wirksamkeit:** ● Nachvollzug der Durchführung des definierten Eskalationsverfahrens anhand der beim Dienstleister vorhandenen Dokumente.	*IDW RS FAIT 5*, Tz. 70, 2. Alt.
124.	**Dienstleister – Dienstleistungsänderungen** Der Cloud-Anbieter hat Verfahren zu definieren und einzurichten, um bei Dienstleistungsänderungen zu analysieren, welche Auswirkungen sich auf Überwachungstätigkeiten und sein IKS sowie auf die mit dem Kunden vereinbarten korrespondierenden Kontrollen ergeben.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren zur Auswirkungsanalyse bei Änderungen der Dienstleistung hinsichtlich Aktualität und Vollständigkeit der Inhalte. **Prüfung der Wirksamkeit:** ● Nachvollzug, ob die Auswirkungsanalysen von Dienstleistungsänderungen Einfluss auf Überwachungstätigkeiten oder das IKS hatten und entsprechend die Überwachungstätigkeiten und das IKS des	*IDW RS FAIT 5*, Tz. 73

18. PaaS **Zielsetzung: Einhaltung der Sicherheits- und Ordnungsmäßigkeitsanforderungen gemäß IDW RS FAIT 5 i.V.m. IDW RS FAIT 1 für das Servicemodell PaaS**			
Nr.	Anforderungen	Beispielhafte Prüfungshandlungen	Referenz
		Cloud-Anbieters und die Schnittstellen zum Kunden angepasst wurden.	
125.	**Segregation des Datenverkehrs in gemeinsam genutzten Netzumgebungen** Der Cloud-Anbieter stellt die sichere Trennung der Netzumgebung über physisch getrennte Netze oder stark verschlüsselte VLANs sicher.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Dokumentation der Netzumgebung für den PaaS-Betrieb bzw. die Dokumentation der VLAN-Verbindungen hinsichtlich Aktualität. **Prüfung der Wirksamkeit:** ● Nachvollzug der Systemparameter bzw. VLAN-Einstellungen und ggf. deren Veränderungen im Prüfungszeitraum, ob die sichere Trennung dauerhaft bestanden hat.	COS-06
126.	**Kryptografische Schlüssel – Aktualität** Der Cloud-Anbieter prüft bei einer Nutzung von Datenverschlüsselungstechniken für die Übertragung bzw. Speicherung regelmäßig die verwendeten kryptografischen Schlüssel auf ihre Aktualität und wechselt diese regelmäßig. Abgelaufene Schlüssel werden auf sichere Art gelöscht bzw. vernichtet.	**Prüfung der Angemessenheit** ● Einsichtnahme in Richtlinien und Verfahren zur Aktualisierung von kryptografischen Schlüsseln. **Prüfung der Wirksamkeit** ● Nachvollzug, ob die kryptografischen Schlüssel gemäß den Vorgaben aktualisiert bzw. gelöscht und vernichtet wurden.	*IDW RS FAIT 5*, Tz. 84
127.	**Bereitstellung von Entwicklungs-, Test- und Produktionsplattform** Der Cloud-Anbieter hat seinen Kunden zu ermöglichen, Entwicklungs-, Test- und Produktionssysteme einzurichten. Darüber hinaus hat er Werkzeuge bereitzustellen, um eine ordnungsgemäße Übergabe entwickelter Programme in die jeweilige Systemplattform zu ermöglichen.	**Prüfung der Angemessenheit** ● Einsichtnahmen in Richtlinien und Verfahren zur Einrichtung von Entwicklungs-, Test- und Produktionsplattformen. **Prüfung der Wirksamkeit** ● Nachvollzug der Werkzeuge, ob diese eine Verbindung der Plattformen ermöglichen.	*IDW RS FAIT 1*, Tz. 102
128.	**Änderungsprozess – unterstützende Software** Der Cloud-Anbieter hat für Änderungen an der unterstützenden Software einen Prozess definiert und	**Prüfung der Angemessenheit:** ● Einsichtnahmen in Richtlinien und Verfahren zu Änderungen an unterstützender Software.	*IDW RS FAIT 5*, Tz. 92 ff.

18. PaaS **Zielsetzung: Einhaltung der Sicherheits- und Ordnungsmäßigkeitsanforderungen gemäß IDW RS FAIT 5 i.V.m. IDW RS FAIT 1 für das Servicemodell PaaS**			
Nr.	Anforderungen	Beispielhafte Prüfungshandlungen	Referenz
	eingerichtet. Als unterstützende Software kommen z.B. in Frage: ● Containerlösungen ● Compiler ● Virtuelle Maschine.	**Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise über die Einhaltung von Prozessvorgaben bei Änderungen an unterstützender Software.	
129.	**Bereitstellung von Entwicklungswerkzeugen** Der Cloud-Anbieter stellt dem Kunden die für eine angemessene Softwareentwicklung notwendigen Softwarewerkzeuge zur Verfügung, bzw. ermöglicht die Installation von entsprechenden Kundenwerkzeugen (z.B. Versionsführung von Sourcecode, Bibliothekssysteme zur Verwaltung von Sourcecode).	**Prüfung der Angemessenheit:** ● Einsichtnahme in Nachweise über die Bereitstellung und Implementierung von Entwicklungswerkzeugen.	*IDW RS FAIT 5*, Tz. 92
130.	**Prüfungsrechte** In den Kundenverträgen sind Prüfungsrechte vereinbart, um ggf. Lücken aus den Prüfungsberichten unabhängiger Dritter (z.B. *IDW PS 951 n.F. (03.2021)*) füllen zu können.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Kundenverträge, ob Prüfrechte vorgesehen sind.	*IDW RS FAIT 5*, Tz. 111

19. SaaS **Zielsetzung: Einhaltung der Sicherheits- und Ordnungsmäßigkeitsanforderungen gemäß IDW RS FAIT 5 i.V.m. IDW RS FAIT 1 für das Servicemodell SaaS**			
Nr.	Anforderungen	Beispielhafte Prüfungshandlungen	Referenz
131.	**Funktionale Anforderungen** Die vom Cloud-Anbieter bereitgestellte rechnungslegungsrelevante Software muss die allgemeinen GoB und die funktionalen Anforderungen an rechnungslegungsrelevante Systeme erfüllen (z.B. Beleg-, Journal-	**Prüfung der Angemessenheit:** ● Nutzung eines Prüfungsberichts nach *IDW EPS 880 (03.2021)*[17] ● Einsichtnahme in die Verfahrensdokumentation (z.B. Onlinehilfe, Bedienungshandbücher, Funktionsbeschreibungen) hinsichtlich	*IDW RS FAIT 1*

[17] *Entwurf einer Neufassung des IDW Prüfungsstandards: Die Prüfung von Softwareprodukten (IDW EPS 880 n.F. (03.2021))* (Stand:26.03.2021).

19. SaaS **Zielsetzung: Einhaltung der Sicherheits- und Ordnungsmäßigkeitsanforderungen gemäß IDW RS FAIT 5 i.V.m. IDW RS FAIT 1 für das Servicemodell SaaS**			
Nr.	Anforderungen	Beispielhafte Prüfungshandlungen	Referenz
	und Kontenfunktion, Abschreibungsregeln, Bilanz- und GuV-Gliederung).	Einhaltung der GoB und der funktionalen Anforderungen ● Walkthroughs zur Prüfung der Existenz von automatischen Kontrollen.	
132.	**Kommunikation von Änderungen an der Cloudsoftware** Der Cloud-Anbieter kommuniziert Änderungen an der Cloudsoftware frühzeitig an den Kunden, damit dieser die Auswirkungen auf Ordnungsmäßigkeit und Sicherheit analysieren kann.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren zur Kommunikation mit Kunden in Bezug auf Änderungen der Cloudsoftware. **Prüfung der Wirksamkeit:** ● Abgleich des Zeitpunkts der Kommunikation an den Kunden mit der Produktivsetzung der Änderung.	*IDW RS FAIT 5*, Tz. 100
133.	**Prüfung des programminternen Kontrollsystems** In der vom Cloud-Anbieter bereitgestellten IT-Anwendung sind angemessene Eingabe-, Verarbeitungs- und Ausgabekontrollen sowie Workflowkontrollen implementiert und wirksam.	**Prüfung der Angemessenheit:** ● Nutzung eines Berichts nach *IDW EPS 880 (03.2021)* ● Einsichtnahme in die Verfahrensdokumentation im Hinblick auf das programminterne Kontrollsystem. **Prüfung der Wirksamkeit:** ● Nachvollzug ausgewählter Transaktionen und Abgleich mit dem Erwartungswert ● Einsichtnahme in Nachweise darüber, ob die in Workflows hinterlegten Funktionstrennungen und Genehmigungsverfahren im Prüfungszeitraum wirksam waren.	*IDW RS FAIT 5*, Tz. 91 ff., Tz. 99
134.	**Customizing** Der Cloud-Anbieter nimmt Änderungen an der Parametrisierung und an Berechtigungen (Rollen) nur im Auftrag und nach sachlicher Abstimmung mit dem Kunden vor. Vor der Produktivsetzung von Customizingänderungen muss der Kunde eine Freigabe erteilen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Richtlinien und Verfahren zur Vornahme von Parametrisierungen und Erfassung von Berechtigungen. **Prüfung der Wirksamkeit:** ● Abgleich, ob zu Parametrisierungen und Berechtigungen Kundenaufträge vorliegen ● Abgleich, ob zu Customizingänderungen Freigabeerklärungen	*IDW RS FAIT 5*, Tz. 98, 99

19. SaaS **Zielsetzung: Einhaltung der Sicherheits- und Ordnungsmäßigkeitsanforderungen gemäß IDW RS FAIT 5 i.V.m. IDW RS FAIT 1 für das Servicemodell SaaS**			
Nr.	Anforderungen	Beispielhafte Prüfungshandlungen	Referenz
		vor der Produktivsetzung vorliegen ● Einsichtnahme in Kundenaufträge daraufhin, ob diese abgearbeitet wurden.	
135.	**Berechtigungsvergabeprozess** Der Cloud-Anbieter erfasst, ändert und löscht Benutzer ausschließlich auf Basis von Kundenanforderungen.	**Prüfung der Angemessenheit:** ● Einsichtnahme in das Genehmigungsverfahren zur Erfassung, Änderung und Löschung von Benutzern anhand der Prozessbeschreibung. **Prüfung der Wirksamkeit:** ● Abgleich, ob zu jeder Erfassung, Änderung und Löschung von Benutzern ein Kundenauftrag vorliegt. ● Nachvollzug, ob alle Kundenaufträge abgearbeitet wurden.	*IDW RS FAIT 5*, Tz. 82, 98, 99
136.	**Verfahrensdokumentation** Der Cloud-Anbieter stellt seinen Kunden die relevanten Bestandteile der aktuellen Verfahrensdokumentation zur Verfügung. Beispielsweise: ● Dokumentation des Softwareherstellers ● Dokumentation des Cloud-Anbieters.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation (z.B. Anwenderdokumentation, technische Systemdokumentation, Dokumentation von Programmänderungen) im Hinblick auf eine angemessene Beschreibung der sachlogischen Programmfunktionen.	*IDW RS FAIT 5*, Tz. 103
137.	**Aufbewahrung** Der Cloud-Anbieter hat mit seinen Kunden vertragliche Vereinbarungen über die Aufbewahrung von Daten gemäß handels- und steuerrechtlichen Aufbewahrungsfristen getroffen. Diese Vereinbarungen betreffen entweder die langfristige Speicherung von Daten in der entsprechenden Anwendung oder die Auslagerung von Daten in spezifische Archivierungssysteme. Des Weiteren beinhalten die vertraglichen Regelungen Angaben zum Speicherort.	**Prüfung der Angemessenheit** ● Einsichtnahme in die vertraglichen Vereinbarungen, ob diese die Anforderungen an die Aufbewahrung von rechnungslegungsrelevanten Daten erfüllen. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise darüber, ob in der vertraglich vereinbarten Zeit ein Zugriff auf die archivierten Daten besteht.	*IDW RS FAIT 5*, Tz. 39, 36 *IDW RS FAIT 3*

19. SaaS **Zielsetzung: Einhaltung der Sicherheits- und Ordnungsmäßigkeitsanforderungen gemäß IDW RS FAIT 5 i.V.m. IDW RS FAIT 1 für das Servicemodell SaaS**			
Nr.	Anforderungen	Beispielhafte Prüfungshandlungen	Referenz
138.	**Kontrolle von Kundenschnittstellen** Der Cloud-Anbieter stellt seinen Kunden Kontrollmöglichkeiten zur Verfügung, um die vollständige und richtige Übertragung von Daten mittels Schnittstellen nachvollziehen zu können.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Nachweise darüber, ob Kontrollmöglichkeiten für Schnittstellen (in der Praxis haben sich hierzu Kontrollsummen oder Hash Totals bewährt) vorgesehen sind. **Prüfung der Wirksamkeit:** ● Einsichtnahme in Nachweise darüber, ob die Kontrollmöglichkeiten den Kunden während des Prüfungszeitraums zur Verfügung standen.	*IDW RS FAIT 5*, Tz. 95
139.	**Prüfrechte** In den Kundenverträgen sind Prüfrechte vereinbart, um ggf. Lücken aus den Prüfungsberichten unabhängiger Dritter (z.B. *IDW PS 880*) füllen zu können.	**Prüfung der Angemessenheit:** ● Einsichtnahme in Kundenverträge, ob Prüfrechte vorgesehen sind ● Einsichtnahme in Nachweise darüber, ob Prüfrechte in Anspruch genommen werden können. Beispielsweise stellt der Cloud-Anbieter dem Kunden ein Testsystem zur Verfügung.	*IDW RS FAIT 5*, Tz. 111
140.	**Beendigung** In den Vereinbarungen zwischen Kunden und Cloud-Anbieter sind auch Regelungen zur Beendigung der Vertragsbeziehung enthalten. Diese betreffen die Herausgabe der gespeicherten Daten, die Mitwirkung des Cloud-Anbieters bei der Migration auf einen neuen Dienstleister sowie die Löschung der übergeleiteten Daten beim Cloud-Anbieter.	**Prüfung der Angemessenheit:** ● Einsichtnahme in die vertraglichen Regelungen zur Beendigung der Vertragsbeziehung.	*IDW RS FAIT 5*, Tz. 53, 116

Die nachfolgenden Anlagen enthalten Beispiele für die Formulierung von Prüfungsvermerken bzw. Prüfungsberichten. Die zusätzlichen Bestandteile eines Prüfungsberichts gegenüber einem Prüfungsvermerk sind jeweils wie folgt kenntlich gemacht: [*kursiv*]

Anlage 2: Auftragsart „Prüfung der Erklärung des Cloud-Anbieters“ – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Wirksamkeitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der von Cloud-Anbietern für das Servicemodell [IaaS, PaaS, SaaS] umzusetzenden Maßnahmen

An den [Cloud-Anbieter]

Wir haben die in der Anlage 1 beigefügte Erklärung der gesetzlichen Vertreter zur Beschreibung der von der [Cloud-Anbieter] für das Servicemodell [IaaS, PaaS, SaaS] umzusetzenden Maßnahmen sowie die Geeignetheit, Implementierung und Wirksamkeit dieser Maßnahmen für den Zeitraum vom [Datum] bis [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen sind geeignet, wenn sie den Risiken der Nichterreichung der unten genannten Kriterien mit hinreichender Sicherheit begegnen.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter des Cloud-Anbieters sind für die Aufstellung der Erklärung des Cloud-Anbieters verantwortlich. Dies schließt die Verantwortung für die internen Kontrollen ein, die sie als notwendig erachten, um eine Erklärung aufzustellen, die frei von wesentlichen – beabsichtigten und unbeabsichtigten – Fehlern ist.

Des Weiteren sind die gesetzlichen Vertreter dafür verantwortlich, dass die Maßnahmen gemäß den unten genannten Kriterien in allen wesentlichen Belangen

- so konzipiert werden, dass sie geeignet sind,
- implementiert werden und wirksam sind, d.h. auch
- überwacht und dokumentiert werden.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen die Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Aufstellung der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters sowie zur Geeignetheit und Wirksamkeit der umzusetzenden Maßnahmen umfassen die in der Neufassung des *IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021)* für das Servicemodell [IaaS, PaaS, SaaS] enthaltenen Ziele. [ggf. Beschreibung weiterer Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die Erklärung der gesetzlichen Vertreter des Cloud-Anbieters in allen wesentlichen Belangen frei von wesentlichen Fehlern ist. Dieses Urteil erstreckt sich auch darauf, ob die in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters beschriebenen und vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen

- geeignet waren und
- im geprüften Zeitraum implementiert und wirksam waren.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und der Neufassung *des IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021)* durchgeführt.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet.

Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit die vorgenannten Urteile abgeben können.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.3* n.F. *(10.2021)* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um entsprechende Prüfungsurteile abgeben zu können. Dies schließt die Beurteilung von Risiken wesentlicher – beabsichtigter oder unbeabsichtigter – Fehler in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters ein. Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters angewandten Grundsätze, Verfahren und Maßnahmen sowie der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens. Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters relevante interne Kontrollsystem abzugeben.

Für die Beurteilung der umzusetzenden Maßnahmen ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Geeignetheit, Implementierung und Wirksamkeit der umgesetzten Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Diese Prüfung umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbau- und einer Funktionsprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

[In einen Prüfungsbericht ist der folgende Abschnitt aufzunehmen:

Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

a) sonstige Feststellungen, u.a.

- *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der Erklärung des Cloud-Anbieters oder der umzusetzenden Maßnahmen,*
- *nicht wesentliche falsche Angaben in der Erklärung des Cloud-Anbieters,*
- *nicht wesentliche Mängel in der Geeignetheit oder Wirksamkeit der umzusetzenden Maßnahmen.**]***

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- ist die Erklärung der gesetzlichen Vertreter des Cloud-Anbieters in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- waren die in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters beschriebenen und vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - im geprüften Zeitraum implementiert sowie
  - im geprüften Zeitraum wirksam.

[Prüfungsurteil mit Einschränkung]

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- ist die Erklärung der gesetzlichen Vertreter des Cloud-Anbieters in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- waren die in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters beschriebenen und vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - im geprüften Zeitraum implementiert sowie
  - im geprüften Zeitraum wirksam.

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks / des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften für die Erbringung von Cloud-Diensten relevanten IT-Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Erklärung der gesetzlichen Vertreter des Cloud-Anbieters zu den umzusetzenden Maßnahmen wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit dieser Maßnahmen erstrecken sich auf den Zeitraum vom [Datum] bis [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters]

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Die umzusetzenden Maßnahmen wurden durch den Cloud-Anbieter abgegrenzt und beinhalten daher möglicherweise nicht jeden Aspekt, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom [Datum] zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Erklärung der gesetzlichen Vertreter des Cloud-Anbieters

Darstellung der geprüften Maßnahmen und der diesbezüglichen Prüfungshandlungen und Ergebnisse

Allgemeine Auftragsbedingungen

Anlage 3: Auftragsart „Prüfung der Erklärung des Cloud-Anbieters“ – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Angemessenheitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der von Cloud-Anbietern für das Servicemodell [IaaS, PaaS, SaaS] umzusetzenden Maßnahmen

An den [Cloud-Anbieter]

Wir haben die in der Anlage 1 beigefügte Erklärung der gesetzlichen Vertreter zur Beschreibung der von der [Cloud-Anbieter] für das Servicemodell [IaaS, PaaS, SaaS] umzusetzenden Maßnahmen sowie die Geeignetheit und Implementierung dieser Maßnahmen zum [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen sind geeignet, wenn sie den Risiken der Nichterreichung der untengenannten Kriterien mit hinreichender Sicherheit begegnen.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter des Cloud-Anbieters sind für die Aufstellung der Erklärung des Cloud-Anbieters verantwortlich. Dies schließt die Verantwortung für die internen Kontrollen ein, die sie als notwendig erachten, um eine Erklärung aufzustellen, die frei von wesentlichen – beabsichtigten und unbeabsichtigten – Fehlern ist.

Des Weiteren sind die gesetzlichen Vertreter dafür verantwortlich, dass die Maßnahmen gemäß den unten genannten Kriterien in allen wesentlichen Belangen

- so konzipiert werden, dass sie geeignet sind,
- implementiert werden und wirksam sind, d.h. auch
- überwacht und dokumentiert werden.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen die Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Aufstellung der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters sowie zur Geeignetheit der umzusetzenden Maßnahmen umfassen die in der Neufassung des *IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021)* für das Servicemodell [IaaS, PaaS, SaaS] enthaltenen Ziele. [ggf. Beschreibung weiterer Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die Erklärung der gesetzlichen Vertreter des Cloud-Anbieters in allen wesentlichen Belangen frei von wesentlichen Fehlern ist. Dieses Urteil erstreckt sich auch darauf, ob die in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters beschriebenen und vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen

- geeignet waren und
- zum [Datum] implementiert waren.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und der *Neufassung des IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021)* durchgeführt.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet.

Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit die vorgenannten Urteile abgeben können.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.3* n.F. *(10.2021)* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um entsprechende Prüfungsurteile abgeben zu können. Dies schließt die Beurteilung von Risiken wesentlicher – beabsichtigter oder unbeabsichtigter – Fehler in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters ein. Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters angewandten Grundsätze, Verfahren und Maßnahmen sowie der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens. Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters relevante interne Kontrollsystem abzugeben.

Für die Beurteilung der umzusetzenden Maßnahmen ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Geeignetheit und Implementierung der umgesetzten Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Diese Prüfung umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbauprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

[In einen Prüfungsbericht ist der folgende Abschnitt aufzunehmen:

Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

a) sonstige Feststellungen, u.a.
- *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der Erklärung des Cloud-Anbieters oder der umzusetzenden Maßnahmen,*
- *nicht wesentliche falsche Angaben in der Erklärung des Cloud-Anbieters,*
- *nicht wesentliche Mängel in der Geeignetheit der umzusetzenden Maßnahmen.**]***

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- ist die Erklärung der gesetzlichen Vertreter des Cloud-Anbieters in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- waren die in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters beschriebenen und vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - zum geprüften Zeitpunkt [Datum] implementiert.

[Prüfungsurteil mit Einschränkung]

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- ist die Erklärung der gesetzlichen Vertreter des Cloud-Anbieters in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- waren die in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters beschriebenen und vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - zum geprüften Zeitpunkt [Datum] implementiert.

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks / des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften für die Erbringung von Cloud-Diensten relevanten IT-Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Erklärung der gesetzlichen Vertreter des Cloud-Anbieters zu den umzusetzenden Maßnahmen wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Geeignetheit und Implementierung dieser Maßnahmen beziehen sich auf den Zeitpunkt zum [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters]

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Die umzusetzenden Maßnahmen wurden durch den Cloud-Anbieter abgegrenzt und beinhalten daher möglicherweise nicht jeden Aspekt, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom [Datum] zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Erklärung der gesetzlichen Vertreter des Cloud-Anbieters

Darstellung der geprüften Maßnahmen und der diesbezüglichen Prüfungshandlungen und Ergebnisse

Allgemeine Auftragsbedingungen

Anlage 4: Auftragsart „Direkte Prüfung des Cloud-Dienstes“ – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Wirksamkeitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der von Cloud-Anbietern für das Servicemodell [IaaS, PaaS, SaaS] umzusetzenden Maßnahmen

An den [Cloud-Anbieter]

Wir haben die Geeignetheit, Implementierung und Wirksamkeit der von der [Cloud-Anbieter] für das Servicemodell [IaaS, PaaS, SaaS] umzusetzenden Maßnahmen für den Zeitraum vom [Datum] bis [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen sind geeignet, wenn sie den Risiken der Nichterreichung der untengenannten Kriterien mit hinreichender Sicherheit begegnen. Zur Darstellung der vom Cloud-Anbieter umzusetzenden Maßnahmen und durchgeführten Prüfungshandlungen verweisen wir auf nachstehende Anlage 1.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter sind dafür verantwortlich, dass die Maßnahmen gemäß den unten genannten Kriterien in allen wesentlichen Belangen

- so konzeptioniert werden, dass sie geeignet sind,
- implementiert werden und wirksam sind, d.h. auch
- überwacht und dokumentiert werden.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen die Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Geeignetheit und Wirksamkeit der umzusetzenden Maßnahmen umfassen die in der *Neufassung des IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021)* für das Servicemodell [IaaS, PaaS, SaaS] enthaltenen Ziele. [ggf. Beschreibung weiterer Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen

- geeignet waren und
- im geprüften Zeitraum implementiert und wirksam waren.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und der *Neufassung des IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021)* durchgeführt.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet.

Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit die vorgenannten Urteile abgeben können.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.3* n.F. *(10.2021)* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um entsprechende Prüfungsurteile abgeben zu können.

Für die Beurteilung der umzusetzenden Maßnahmen ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Geeignetheit, Implementierung und Wirksamkeit der umgesetzten Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Diese Prüfung umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbau- und einer Funktionsprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

[In einen Prüfungsbericht ist der folgende Abschnitt aufzunehmen:

Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

a) sonstige Feststellungen, u.a.

- *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der umzusetzenden Maßnahmen,*
- *nicht wesentliche Mängel in der Geeignetheit oder Wirksamkeit der umzusetzenden Maßnahmen.**]***

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- waren die vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - im geprüften Zeitraum implementiert sowie
  - im geprüften Zeitraum wirksam.

[Prüfungsurteil mit Einschränkung]

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- waren die vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - im geprüften Zeitraum implementiert sowie
  - im geprüften Zeitraum wirksam.

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks / des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften für die Erbringung von Cloud-Diensten relevanten IT-Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit der umzusetzenden Maßnahmen erstrecken sich auf den Zeitraum vom [Datum] bis [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Die umzusetzenden Maßnahmen wurden durch den Cloud-Anbieter abgegrenzt und beinhalten daher möglicherweise nicht jeden Aspekt, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom [Datum] zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Darstellung der geprüften Maßnahmen und der diesbezüglichen Prüfungshandlungen und Ergebnisse

Allgemeine Auftragsbedingungen

Anlage 5: Auftragsart „Direkte Prüfung des Cloud-Dienstes“ – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Angemessenheitsprüfung

Prüfungsvermerk/Prüfungsbericht des unabhängigen Wirtschaftsprüfers über eine Prüfung der von Cloud-Anbietern für das Servicemodell [IaaS, PaaS, SaaS] umzusetzenden Maßnahmen

An den [Cloud-Anbieter]

Wir haben die Geeignetheit und Implementierung der von der [Cloud-Anbieter] für das Servicemodell [IaaS, PaaS, SaaS] umzusetzenden Maßnahmen zum [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen sind geeignet, wenn sie den Risiken der Nichterreichung der untengenannten Kriterien mit hinreichender Sicherheit begegnen. Zur Darstellung der vom Cloud-Betreiber umzusetzenden Maßnahmen und durchgeführten Prüfungshandlungen verweisen wir auf nachstehende Anlage 1.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter sind dafür verantwortlich, dass die Maßnahmen gemäß den unten genannten Kriterien in allen wesentlichen Belangen

- so konzeptioniert werden, dass sie geeignet sind,
- implementiert werden und wirksam sind, d.h. auch
- überwacht und dokumentiert werden.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen die Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Geeignetheit der umzusetzenden Maßnahmen umfassen die in der *Neufassung des IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021)* für das Servicemodell [IaaS, PaaS, SaaS] enthaltenen Ziele. [ggf. Beschreibung weiterer Kriterien]

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen

- geeignet waren und
- zum [Datum] implementiert waren.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und der *Neufassung des IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021)* durchgeführt.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet.

Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit die vorgenannten Urteile abgeben können.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.3* n.F. *(10.2021)* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um entsprechende Prüfungsurteile abgeben zu können.

Für die Beurteilung der umzusetzenden Maßnahmen ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Geeignetheit und Implementierung der umgesetzten Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Diese Prüfung umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbauprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

[In einen Prüfungsbericht ist der folgende Abschnitt aufzunehmen:

Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

a) sonstige Feststellungen, u.a.

- *ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung der umzusetzenden Maßnahmen,*
- *nicht wesentliche Mängel in der Geeignetheit der umzusetzenden Maßnahmen.* ***]***

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- waren die vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - zum geprüften Zeitpunkt [Datum] implementiert.

[Prüfungsurteil mit Einschränkung]

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- waren die vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - geeignet und
  - zum geprüften Zeitpunkt [Datum] implementiert.

[Gegebenenfalls ergänzender Hinweis

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks / des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften für die Erbringung von Cloud-Diensten relevanten IT-Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Geeignetheit und Implementierung der umzusetzenden Maßnahmen beziehen sich auf den Zeitpunkt [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der [Nennung des Zwecks] kon-

zipiert wurden. Die umzusetzenden Maßnahmen wurden durch den Cloud-Anbieter abgegrenzt und beinhalten daher möglicherweise nicht jeden Aspekt, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom [Datum] zugrunde liegen.

(Ort)

(Datum)

(Unterschrift)

Anlagen:

Darstellung der geprüften Maßnahmen und der diesbezüglichen Prüfungshandlungen und Ergebnisse

Allgemeine Auftragsbedingungen

IDW Prüfungshinweis: Die Prüfung der Einhaltung der Grundsätze der ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD-Compliance) (IDW PH 9.860.4 (07.2021))

(Stand: 14.07.2021)

IDW Prüfungshinweis: Die Prüfung der Einhaltung der Grundsätze der ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD-Compliance) (IDW PH 9.860.4 (07.2021))

Stand: 14.07.2021[1]

1. Vorbemerkungen

1 Dieser *IDW Prüfungshinweis* basiert auf dem *IDW PS 860*[2], der die Grundsätze und Vorgehensweise festlegt, nach denen IT-Prüfungen außerhalb der Abschlussprüfung durchzuführen sind.

[1] Verabschiedet vom Fachausschuss für Informationstechnologie (FAIT) am 14.06.2021. Billigende Kenntnisnahme durch den Hauptfachausschuss (HFA) am 14.07.2021.

[2] *IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* (Stand: 02.03.2018).

Er konkretisiert die Prüfung der Einhaltung der Grundsätze der ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) und legt die Berufsauffassung dar, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit bei der Prüfung vorgehen.

Die in der Anlage 1 enthaltenen Anforderungen für eine den GoBD entsprechende Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (im Folgenden GoBD-Compliance) werden vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) als geeignete Kriterien zur Einrichtung angemessener Grundsätze, Verfahren und Maßnahmen des IT-Systems (im Folgenden Maßnahmen) durch das Unternehmen angesehen, die bei einer Prüfung nach diesem *IDW Prüfungshinweis* modular, d.h. für abgegrenzte GoBD-relevante Geschäftsprozesse beurteilt werden. Diese in der Anlage 1 enthaltenen Anforderungen setzen – für die einschlägigen Geschäftsprozesse – die Vorgaben der vom Bundesministerium der Finanzen (BMF) herausgegebenen Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD-Vorgaben) um.

Dargestellt werden in der Anlage 1 GoBD-Anforderungen für die nachfolgenden Elemente eines IT-Systems:

- Basiselement: Verfahrensdokumentation und generelle IT-Kontrollen
- Ergänzungselement (1): Belegeingang
- Ergänzungselement (2): Elektronischer Belegausgang
- Ergänzungselement (3): Elektronische Aufbewahrung
- Ergänzungselement (4): Datenzugriff der Finanzverwaltung.

2 Dieser *IDW Prüfungshinweis* sieht die Prüfung der Maßnahmen des Basiselements sowie eines oder mehrerer der in der Anlage 1 bezeichneten Ergänzungselemente (1) bis (4) vor. Eine Prüfung der Maßnahmen der Ergänzungselemente (1) bis (4) kann daher einzeln oder in Kombination erfolgen und schließt stets die Einbeziehung der Prüfung der Maßnahmen des Basiselements („Verfahrensdokumentation und generelle IT-Kontrollen“) mit ein. Eine ausschließliche Beauftragung der Prüfung der Maßnahmen des Basiselements ohne die Prüfung der Maßnahmen eines Ergänzungselements erfüllt nicht die Vorgaben des *IDW PS 860* an eine IT-Prüfung der GoBD (außerhalb der Abschlussprüfung) nach diesem *IDW Prüfungshinweis*. Eine Beurteilung der Angemessenheit und ggf. Wirksamkeit der geschäftsprozessbezogenen Maßnahmen ist ohne die entsprechende Beurteilung der generellen IT-Kontrollen und der Verfahrensdokumentation nicht möglich. Ebenso ist die Beurteilung der Relevanz von generellen IT-Kontrollen und der Vollständigkeit und Richtigkeit der Darstellungen im Rahmen einer Verfahrensdokumentation nicht ohne Beurteilung der Angemessenheit der geschäftsprozessbezogenen Maßnahmen möglich.

3 Dieser *IDW Prüfungshinweis* gilt sowohl für die Auftragsart „Prüfung einer Erklärung der gesetzlichen Vertreter zur GoBD-Compliance“ als auch für die Auftragsart „direkte Prüfung der GoBD-Compliance“.

4 Zusammenfassend kennzeichnen insb. die folgenden Merkmale einen Prüfungsauftrag gemäß *IDW PS 860* für die Beurteilung der von Unternehmen umzusetzenden Maßnahmen unter Anwendung dieses *IDW Prüfungshinweises*:

- Involvierte Parteien sind neben dem Wirtschaftsprüfer und dem Unternehmen (verantwortlich für das Prüfungsobjekt) weitere vorgesehene Nutzer des Prüfungsberichts, die sich vom im Bericht genannten Empfänger (i.d.R. die beauftragende Partei) unterscheiden können.
- Die zu prüfenden Maßnahmen des IT-Systems zur Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff sind klar bestimmbar und abgrenzbar (GoBD-relevantes IT-System).
- Die Prüfung ist modular aufgebaut und schließt stets eine Prüfung der Maßnahmen des Basiselements mit ein.
- Der Wirtschaftsprüfer gibt ein Urteil mit hinreichender Sicherheit ab und berichtet über die Prüfung entsprechend dem Informationsbedarf der vorgesehenen Nutzer der Berichterstattung.
- Durch den Wirtschaftsprüfer werden die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit sowie die Anforderungen des *IDW QS 1*[3] eingehalten.

2. Ziel und Umfang der Prüfung

5 Das IDW hat mit dem *IDW PS 860* die Berufsauffassung dargelegt, nach der Wirtschaftsprüfer – unbeschadet ihrer Eigenverantwortlichkeit – die Prüfung von IT-Systemen außerhalb der Abschlussprüfung planen, durchführen sowie darüber Bericht erstatten.

6 Eine nach *IDW PH 9.860.4 (07.2021)* durchgeführte Prüfung des GoBD-relevanten IT-Systems (DV-System gemäß den GoBD, Rn. 20) kann als Angemessenheitsprüfung oder zusätzlich als Wirksamkeitsprüfung erfolgen.

7 Ein IT-System ist GoBD-relevant i.S. dieses *IDW Prüfungshinweises*, wenn es zur Erfassung, Verarbeitung, Speicherung sowie Übertragung von aufzeichnungs- und aufbewahrungspflichtigen Daten gemäß den GoBD dient (vgl. GoBD, Rn. 3, 4, 5).

8 Das IT-Kontrollsystem (IKS i.S. der GoBD, Rn. 100 ff.) ist Bestandteil des GoBD-relevanten IT-Systems und umfasst diejenigen Grundsätze, Verfahren und Maßnahmen des IT-Systems, die zur Bewältigung der Risiken aus dem Einsatz von IT (vgl. GoBD, Rn. 103 ff.) eingerichtet wurden und schließt den Risikobeurteilungsprozess mit ein. Der IT-Risikobeurteilungsprozess ist somit die Grundlage für die Feststellung der IT-Risiken, die vom Management im Rahmen des IT-Kontrollsystems im Hinblick auf das GoBD-relevante IT-System gesteuert werden müssen.

9 Die zu prüfenden Ergänzungselemente (vgl. Tz. 1) sind in der Auftragsvereinbarung festzulegen.

---

[3] Vgl. *IDW Qualitätssicherungsstandard: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* (Stand: 09.06.2017).

10 Bei der Auftragsart „Prüfung einer Erklärung der gesetzlichen Vertreter zur GoBD-Compliance“[4] ist Ziel der Angemessenheitsprüfung, dem Wirtschaftsprüfer ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob[5]

- die Erklärung der gesetzlichen Vertreter (im Folgenden GoBD-Erklärung) in allen wesentlichen Belangen frei von Fehlern ist und
- die in der GoBD-Erklärung der gesetzlichen Vertreter beschriebenen und vom Unternehmen umgesetzten Maßnahmen in allen wesentlichen Belangen angemessen waren.

11 Die Maßnahmen sind angemessen, wenn sie den Risiken der Nichteinhaltung der GoBD-Vorgaben mit hinreichender Sicherheit begegnen. Es ist davon auszugehen, dass die Maßnahmen den Risiken der Nichteinhaltung der GoBD-Vorgaben mit hinreichender Sicherheit begegnen, wenn sie die jeweiligen in der Anlage 1 referenzierten GoBD-Anforderungen für die zu prüfenden Elemente in allen wesentlichen Belangen erfüllen.

12 Ziel der Wirksamkeitsprüfung bei dieser Auftragsart ist – über die Angemessenheitsprüfung hinaus – zu beurteilen, ob die in der GoBD-Erklärung der gesetzlichen Vertreter beschriebenen und umzusetzenden Maßnahmen in dem zu prüfenden Zeitraum in allen wesentlichen Belangen wirksam gewesen sind. Diese Maßnahmen sind wirksam, wenn sie wie vorgesehen durchgeführt wurden.[6]

13 Bei der Auftragsart „direkte Prüfung der GoBD-Compliance“ ist Ziel der Angemessenheitsprüfung, dem Wirtschaftsprüfer auf Grundlage der durchgeführten Prüfungshandlungen ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob[7] die relevanten Maßnahmen in allen wesentlichen Belangen angemessen sind. Die Maßnahmen sind angemessen, wenn sie den Risiken der Nichteinhaltung der GoBD-Vorgaben mit hinreichender Sicherheit begegnen. Es ist davon auszugehen, dass die Maßnahmen den Risiken der Nichteinhaltung der GoBD-Vorgaben mit hinreichender Sicherheit begegnen, wenn sie die jeweiligen in der Anlage 1 referenzierten GoBD-Anforderungen für die zu prüfenden Elemente erfüllen.

14 Ziel der Wirksamkeitsprüfung bei dieser Auftragsart ist – über die Angemessenheitsprüfung hinaus – zu beurteilen, ob die Maßnahmen in dem zu prüfenden Zeitraum in allen wesentlichen Belangen wirksam gewesen sind. Diese Maßnahmen sind wirksam, wenn sie wie vorgesehen durchgeführt wurden.

3. Gegenstand der Prüfung

15 Gegenstand der „Prüfung einer Erklärung der gesetzlichen Vertreter zur GoBD-Compliance“ nach diesem *IDW Prüfungshinweis* ist die GoBD-Erklärung der gesetzlichen Vertreter des Unternehmens zur Beschreibung der für die Geschäftsprozesse des IT-Systems relevanten Maßnahmen sowie die Angemessenheit und – sofern einschlägig – die Wirksamkeit dieser Maßnahmen für den Berichtszeitraum.

---

4 Prüfung einer Erklärung zur GoBD-Konformität des IT-Systems.

5 Vgl. *IDW PS 860*, Tz. 15.

6 Vgl. *IDW PS 860*, Tz. 16.

7 Vgl. *IDW PS 860*, Tz. 21.

16 Gegenstand einer „direkten Prüfung der GoBD-Compliance“ nach diesem *IDW Prüfungshinweis* sind die Angemessenheit und – sofern einschlägig – die Wirksamkeit der für die Geschäftsprozesse relevanten Maßnahmen des IT-Systems des Unternehmens für den Berichtszeitraum.

4. Kriterien

17 Die in der Anlage 1 für die Basis- und Ergänzungselemente enthaltenen Anforderungen stellen geeignete Kriterien i.S. des *IDW PS 860*, Tz. 32, dar.

18 Die Anforderungen an die Basis- und Ergänzungselemente ergeben sich aus den relevanten GoBD-Vorgaben mit der entsprechenden Referenzierung auf das BMF-Schreiben vom 28.11.2019 (vgl. Spalte „GoBD-Referenz“). Die Spalte „Zusammenfassung der GoBD-Vorgaben“ dient der Beschreibung der relevanten GoBD-Vorgaben in Bezug auf die Anforderungen an die zu prüfenden Basis- und Ergänzungselemente.

19 Die in der Anlage 1 aufgeführten GoBD-Anforderungen sind nicht als abschließende Aufzählung zu verstehen, da eine etwaige Ergänzung in der Verantwortung der gesetzlichen Vertreter liegt.

20 Ferner können sich Ergänzungen der Anforderungen aufgrund weiterer gesetzlicher oder sonstiger regulatorischer Vorgaben ergeben.

5. Besonderheiten bei der Durchführung der Prüfung

21 Der *IDW PS 860* legt die Grundsätze für die Planung und Durchführung von Prüfungshandlungen für eine Prüfung der Angemessenheit und – sofern einschlägig – Wirksamkeit fest.

22 Gemäß *IDW PS 860*, Tz. 47, hat der Wirtschaftsprüfer – auf der Grundlage des gewonnenen Verständnisses über das Unternehmen, das rechtliche und wirtschaftliche Umfeld und der umzusetzenden Maßnahmen – die Risiken für wesentliche Fehler in der Erklärung zur GoBD-Erklärung der gesetzlichen Vertreter bzw. die Risiken wesentlicher Mängel in den umzusetzenden Maßnahmen zu identifizieren und zu beurteilen. Sofern der Wirtschaftsprüfer im Rahmen der Prüfungsdurchführung Nachweise erlangt, die im Widerspruch zu den Prüfungsnachweisen stehen, die Basis für seine ursprüngliche Risikobeurteilung waren, muss er die Risikobeurteilung anpassen und die weiteren geplanten Prüfungshandlungen entsprechend modifizieren. Zudem hat der Wirtschaftsprüfer gemäß *IDW PS 860*, Tz. 48, Prüfungshandlungen zu planen und durchzuführen, um das Prüfungsrisiko auf ein vertretbar niedriges Maß zu reduzieren.

23 Die in der Anlage 1 aufgeführten Prüfungshandlungen sind als Beispiele und nicht als abschließende Aufzählung zu verstehen, da die Festlegung der durchzuführenden Prüfungshandlungen im pflichtgemäßen Ermessen des Wirtschaftsprüfers unter Berücksichtigung der Ergebnisse seiner Risikobeurteilung sowie der notwendigen Prüfungshandlungen als Reaktion auf die beurteilten Risiken liegt.

24 Weitere beispielhafte Prüfungshandlungen ergänzend zu den in der Anlage 1 aufgeführten beispielhaften Prüfungshandlungen sind jeweils auch

- die Einsichtnahme in Unterlagen und Dokumentationen, wie bspw. Richtlinien, Arbeitsanweisungen, Verfahrensanweisungen, Prozessdokumentationen, Verzeichnisse oder Schulungskonzepte, in denen zentrale Vorgaben zur Durchführung, zum Ablauf und zu den Verantwortlichkeiten schriftlich geregelt sind (zur Prüfung der Angemessenheit der Maßnahmen),
- die Beurteilung der Unterlagen und Dokumentationen im Hinblick auf ihre regelmäßige Aktualisierung und Aktualität (zur Prüfung der Angemessenheit der Maßnahmen),
- die Beurteilung der Unterlagen und Dokumentationen im Hinblick auf ihre Vollständigkeit (zur Prüfung der Angemessenheit und Wirksamkeit der Maßnahmen).

25 Soweit der Wirtschaftsprüfer bereits im Rahmen der Angemessenheitsprüfung Risiken wesentlicher Fehler in der GoBD-Erklärung der gesetzlichen Vertreter identifiziert, die vom Management nicht identifiziert wurden, hat er zu beurteilen, ob ein solches Risiko vorliegt, das seiner Erwartung nach durch das IT-System zu identifizieren war und hätte berücksichtigt werden müssen.

26 Hat der Wirtschaftsprüfer bereits anlässlich seiner Prüfungshandlungen zur Beurteilung der Risiken wesentlicher Mängel des IT-Systems solche wesentlichen Mängel festgestellt, kann er zu dem Ergebnis gelangen, dass sich in diesem Zusammenhang weitere Prüfungshandlungen zur Angemessenheit und Wirksamkeit erübrigen.

6. Besonderheiten bei der Berichterstattung des Wirtschaftsprüfers

27 Der Wirtschaftsprüfer verfasst eine schriftliche Berichterstattung als Prüfungsbericht. Der Prüfungsbericht hat die geprüften Ergänzungselemente darzustellen. Der Prüfungsbericht beinhaltet eine zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und ggf. Funktionsprüfungen und der weiteren Prüfungshandlungen sowie Prüfungsfeststellungen.

28 Für die Darstellung der geprüften Maßnahmen und der diesbezüglichen Prüfungshandlungen und Ergebnisse in der Anlage der Berichterstattung über die Prüfung hat sich der nachfolgende Aufbau in der Praxis bewährt:

<table>
<tr><td colspan="2">Anforderung an die zu prüfenden Basis- und Ergänzungselemente</td></tr>
<tr><td>Darstellung der Maßnahmen basierend auf der Anlage 1 dieses IDW Prüfungshinweises</td><td>Darstellung des Prüfungsumfangs, der Prüfungshandlungen sowie deren Ergebnisse</td></tr>
<tr><td colspan="2">Beurteilung der Maßnahmen im Hinblick auf ihre Angemessenheit und – sofern einschlägig – Wirksamkeit</td></tr>
</table>

Anlagen

Anlage 1: Die Prüfung der GoBD-Anforderungen gemäß IDW PH 9.860.4 (07.2021)

In dieser Anlage werden die GoBD-Anforderungen und beispielhaften Prüfungshandlungen für die nachfolgenden Elemente eines IT-Systems dargestellt:

Basiselement: Verfahrensdokumentation und generelle IT-Kontrollen

Ergänzungselement (1): Belegeingang

Ergänzungselement (2): Elektronischer Belegausgang

Ergänzungselement (3): Elektronische Aufbewahrung

Ergänzungselement (4): Datenzugriff der Finanzverwaltung.

Basiselement: Verfahrensdokumentation und generelle IT-Kontrollen

Verfahrensdokumentation

Für die Verfahrensdokumentation ist der Steuerpflichtige verantwortlich. Dies gilt auch bei einer teilweisen oder vollständigen organisatorischen und technischen Auslagerung von Buchführungs- und Aufzeichnungsaufgaben auf Dritte (z.B. Rechenzentrum).

Nach Auffassung der Finanzverwaltung ist eine aussagefähige, vollständige und aktuelle Verfahrensdokumentation Voraussetzung für die Nachvollziehbarkeit und Nachprüfbarkeit eines (jeden) IT-gestützten Verfahrens. Hierzu hat die Verfahrensdokumentation alle zum Verständnis der Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff erforderlichen Verfahrensbestandteile, Daten und Kontrollen zu enthalten.

Das Basiselement Verfahrensdokumentation bezieht sich sowohl auf die grundsätzlichen GoBD-Vorgaben zur Erstellung und Aktualisierung einer Verfahrensdokumentation als auch auf die bei einer Prüfung der jeweiligen Geschäftsprozesse (Ergänzungselemente (1) bis (4)) zu berücksichtigen Aspekte.

Die dem Basiselement zugrundeliegende Gliederung der Verfahrensdokumentation in deren systematischen Bestandteile „Allgemeine Beschreibung“, „Anwenderdokumentation“, „Technische Systemdokumentation“ sowie „Betriebsdokumentation“ einschließlich „Internes Kontrollsystem“ wird von den GoBD nicht ausdrücklich gefordert. Diese Gliederung dient der Veranschaulichung, welche Nachweise durch die einzelnen Bestandteile einer Verfahrensdokumentation erbracht werden sollen.

Die erforderlichen Nachweise einer Verfahrensdokumentation können sich auch aus einer Zusammenstellung einzelner Dokumente ergeben, bspw. aus einem Masterdokument mit Verweisen auf mitgeltende Unterlagen (Sekundärdokumente). Die Gesamtheit aller erstellten und referenzierten Dokumente beinhaltet die Verfahrensdokumentation i.S. der GoBD, die insgesamt die relevanten Vorgaben der Finanzverwaltung zu erfüllen haben.

Basiselement: Verfahrensdokumentation			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
1.	**Erstellung- und Pflege der Verfahrensdokumentation** ● Aussagekräftige, vollständige und aktuelle Verfahrensdokumentation, die alle System- bzw. Verfahrensänderungen inhaltlich und zeitlich lückenlos dokumentiert ● Nachweis der aktuellen und historischen Verfahrensinhalte für die Dauer der Aufbewahrungsfrist ● Dokumentation aller System- bzw. Verfahrensänderungen (inhaltlich und zeitlich) ● Für den Zeitraum der Aufbewahrungsfrist muss gewährleistet und nachgewiesen sein, dass das in der Dokumentation beschriebene Verfahren dem in der Praxis eingesetzten Verfahren voll entspricht ● Änderungen müssen historisch nachvollziehbar sein ● Autorisiertes Änderungsverfahren ● Es muss sich ergeben, wie die Ordnungsvorschriften der GoBD beachtet werden.	**Angemessenheit:** ● Einsichtnahme in die Dokumentation des Prozesses zur Erstellung bzw. Pflege der Verfahrensdokumentation, um festzustellen, ob die getroffenen Maßnahmen geeignet sind im Falle von Änderungen von rechtlichen oder sonstigen Vorgaben sowie bei technischen Veränderungen an den GoBD-relevanten IT-Systemen eine sachgerechte Anpassung der Verfahrensdokumentation vorzunehmen ● Einsichtnahmen in die Dokumentation, ob der Erstellungs- und Pflegeprozess folgende Aspekte berücksichtigt: – Änderungs- und Freigabekonzept für die Änderung der Verfahrensdokumentation im Falle von Änderungen am zugrundeliegenden Prozess – Regelungen und Vorgaben für eine nachvollziehbare Änderungshistorie der Verfahrensdokumentation (i.S.v. Grundsätzen, Verfahren und Maßnahmen) – Gewährleistung der Identität des tatsächlich vorhandenen Prozesses mit dem dokumentierten Prozess – Aufbewahrung über die Dauer der gesetzlichen Aufbewahrungsfrist. – Gültigkeit der Verfahrensdokumentationen. **Wirksamkeit:** ● Nachvollzug, ob keine zeitlichen Lücken bei der Aktualisierung der Verfahrensdokumentation im Prüfungszeitraum vorliegen.	34, 35, 66, 80, 101, 150, 154

Basiselement: Verfahrensdokumentation			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		(Wirksamkeit im Zusammenhang mit den Ergänzungselementen (1) bis (4): ● Nachvollzug, ob die Verfahrensdokumentation mit den im Prüfungszeitraum eingesetzten Systemen und Verfahren übereinstimmt ● Nachvollzug, ob im Erstellungs- und Änderungsprozess alle GoBD-relevanten Kontrollen und IT-Systeme einschließlich der IT-Anwendungen berücksichtigt sind.)	
2.	**Übersichtlichkeit und Verständlichkeit, der Verfahrensdokumentation** ● Übersichtliche Gliederung, aus der Inhalt, Aufbau, Ablauf und Ergebnisse des DV-Verfahrens vollständig und schlüssig ersichtlich sind ● Verständlich und damit für einen sachverständigen Dritten in angemessener Zeit nachprüfbar ● Konkrete Ausgestaltung ist abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten DV-Systems.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, ob diese für einen sachverständigen Dritten nachvollziehbar ist. Für die Nachvollziehbarkeit der Verfahrensdokumentation ist es insb. erforderlich, dass – eine Beschreibung des Aufbaus, Ablaufs und der Ergebnisse des DV-Verfahrens vollständig und sachlogisch erfolgt. – ein Verständnis des Aufbaus, Ablaufs und der Ergebnisse des DV-Verfahrens ohne Kenntnis von Programmiersprachen („Klartext“) ermöglicht wird. – die für ein Verständnis des Aufbaus, Ablaufs und der Ergebnisse des DV-Verfahrens notwendigen Abkürzungs-, Symbol- und Schlüsselverzeichnisse vorhanden sind. **(Die Prüfung der Wirksamkeit der Maßnahmen erfolgt im Zusammenhang mit den Ergänzungselementen (1) bis (4)** Nachvollzug, ob ein übergreifendes Master- bzw. Hauptdokument vorhanden ist, welches die sachlogischen Zusammenhänge und Prozesse sowie das GoBD-Kontrollumfeld beschreibt,	151, 149

Basiselement: Verfahrensdokumentation			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		ergänzt durch mitgeltende Unterlagen (sog. Sekundärdokumente)).	
3.	**Bestandteile und Inhalte der Verfahrensdokumentation (Allgemeine Beschreibung)** Die Verfahrensdokumentation besteht i.d.R. aus folgenden Bestandteilen: ● Allgemeine Beschreibung ● Anwenderdokumentation ● Technische Systemdokumentation ● Betriebsdokumentation.	**Angemessenheit:** Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob geeignete Unterlagen bzw. Formulierungen vorliegen, ● die eine sachgerechte allgemeine Beschreibung des IT-Systems und der IT-Anwendungen darstellen, ● die eine aktuelle Anwenderdokumentation beinhalten sowie ● die notwendigen Inhalte einer technischen Systemdokumentation und einer Dokumentation des IT-Betriebs enthalten.	153
4.	**Bestandteile und Inhalte der Verfahrensdokumentation: Allgemeine Beschreibung** Die allgemeine Beschreibung umfasst insb.: ● Ausführungen zu Rahmenbedingungen, ● Aufgabenstellung und ● Einsatzgebiet.	**Angemessenheit:** Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Ausführungen zu folgenden Aspekten enthalten sind: ● Zielsetzung und Einsatzgebiet ● Beschreibung des Unternehmens (Aufgabenstellung und Organisation) ● Steuerrechtliche Anforderungen (Steuerlicher Maßstab) ● Darstellung der steuerrelevanten Anwendungen/DV-Systeme einschließlich Vor- und Nebensysteme. **(Die Prüfung der Wirksamkeit der Maßnahmen erfolgt im Zusammenhang mit den Ergänzungselementen (1) bis (4)** Nachvollzug, ob die Ausführungen zu folgenden Aspekten aktuell und richtig sind:	153

Basiselement: Verfahrensdokumentation			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		● Zielsetzung und Einsatzgebiet ● Beschreibung des Unternehmens (Aufgabenstellung und Organisation) ● Steuerrechtliche Anforderungen (Steuerlicher Maßstab) ● Darstellung der steuerrelevanten Anwendungen/DV-Systeme einschließlich Vor- und Nebensysteme.)	
5.	**Bestandteile und Inhalte der Verfahrensdokumentation: Anwenderdokumentation und sachlogische Prozessbeschreibung** Aus der Verfahrensdokumentation muss ersichtlich sein, wie die elektronischen Belege erfasst, empfangen, verarbeitet, ausgegeben und aufbewahrt werden.	**Angemessenheit:** Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob die folgenden Bestandteile/Inhalte (ggf. je DV-System und Anwendung) enthalten sind: ● Allgemeine Beschreibung des eingesetzten DV-Systems ● Beschreibung der fachlichen Prozesse und Prozessverantwortlichkeiten, wie insb. Datenempfang, Datenerfassung, Datenverarbeitung, Prüfung, Ausgabe sowie Aufbewahrung einschließlich der Aufbewahrungsregeln und -fristen ● Datenbereitstellung für Prüfungszwecke (Zugriffsarten Z1 bis Z3) sowie die Vorgehensweise im Rahmen der Erst- bzw. Zweitqualifikation steuerrelevanter Daten ● Schnittstellenbeschreibungen bzw. eine Darstellung der Beziehungen zwischen den einzelnen Anwendungsmodulen ● Organisationsanweisungen und Benutzerhandbücher ● Schlüsselverzeichnisse. **(Die Prüfung der Wirksamkeit der Maßnahmen erfolgt im Zusammenhang mit den Ergänzungselementen (1) bis (4)**	153, 152, 66, 79

Basiselement: Verfahrensdokumentation			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		Nachvollzug, ob die Ausführungen zu folgenden Aspekten aktuell und richtig sind: ● Allgemeine Beschreibung des eingesetzten DV-Systems ● Beschreibung der fachlichen Prozesse und Prozessverantwortlichkeiten, wie insb. Datenempfang, Datenerfassung, Datenverarbeitung, Prüfung, Ausgabe sowie Aufbewahrung einschließlich der Aufbewahrungsregeln und -fristen ● Datenbereitstellung für Prüfungszwecke (Zugriffsarten Z1 bis Z3) sowie die Vorgehensweise im Rahmen der Erst- bzw. Zweitqualifikation steuerrelevanter Daten ● Schnittstellenbeschreibungen bzw. eine Darstellung der Beziehungen zwischen den einzelnen Anwendungsmodulen ● Organisationsanweisungen und Benutzerhandbücher ● Schlüsselverzeichnis.**)**	
6.	**Bestandteile und Inhalte der Verfahrensdokumentation: Technische Systemdokumentation** Die technische Systemdokumentation hat insb. die folgenden Bestandteile/Inhalte (ggf. je DV-System und Anwendung) zu enthalten: ● Die technische Systemdokumentation beinhaltet im Wesentlichen eine Darstellung der eingesetzten DV-Systeme. ● Vollständiger Systemüberblick muss möglich sein ● Überblick über alle im DV-System vorhandenen Informationen, die aufzeichnungs- und aufbewahrungspflichtige Unterlagen betref-	**Angemessenheit:** Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob die folgenden Bestandteile/Inhalte (je DV-System und IT-Anwendung) enthalten sind: ● Aufgabenstellung der IT-Anwendungen im Kontext der eingesetzten Module/Fachanwendungen ● Beschreibungen der eingesetzten Softwarekomponenten (einschließlich Customizing-Maßnahmen und Systemanpassungen, Systemkonfiguration, Parametereinstellungen, Anwenderoberflächen, Infrastrukturkomponenten) sowie eine Beschreibung der zum Systemverständnis erforderlichen eingesetzten Hardwarekomponenten (z.B.	160

Basiselement: Verfahrensdokumentation			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	fen; z.B. Beschreibungen zu Tabellen, Feldern, Verknüpfungen und Auswertungen.	Speicher- und Erfassungssysteme, Server) ● Darstellung der Schnittstellen und der Funktionsweise der Schnittstellen ● Beschreibung der programminternen Verarbeitungsregeln aus technischer Sicht (z.B. Datenflussdiagramme, Ablaufpläne und Protokollierungen) ● Datenorganisation und Datenstrukturen (Datensatzaufbau bzw. Tabellenaufbau bei Datenbanken) ● Beschreibung der programminternen Verarbeitungsregeln und der implementierten Eingabe- und Verarbeitungskontrollen ● Beschreibung programminterner Fehlerbehandlungsverfahren.	
7.	**Bestandteile und Inhalte der Verfahrensdokumentation (Betriebsdokumentation)** Die Betriebsdokumentation hat die folgenden Bestandteile/Inhalte (ggf. je DV-System und Anwendung) zu enthalten: ● Anweisungen und Dokumentationen zum grundsätzlichen IT-Betrieb und zur IT-Sicherheit ● Beschreibung der technischen Betriebsprozesse im geordneten Regelbetrieb sowie eine Beschreibung zum Notbetrieb ● Beschreibungen zur Datensicherheit und zur Datenintegrität (Transaktions- und Konsistenzsicherung, Protokollierung, Ausfallsicherheit) ● Beschreibung zum Berechtigungskonzept einschließlich Benutzerverwaltung sowie zum Zugriffs- und Zugangsschutz.	**Angemessenheit:** Einsichtnahme in die Bestandteile/Inhalte der Verfahrensdokumentation in Bezug auf die ● Anweisungen und Dokumentationen zum grundsätzlichen IT-Betrieb und zur IT-Sicherheit ● Beschreibung der technischen Betriebsprozesse im geordneten Regelbetrieb sowie eine Beschreibung zum Notbetrieb ● Beschreibungen zur Datensicherheit und zur Datenintegrität (Transaktions- und Konsistenzsicherung, Protokollierung, Ausfallsicherheit) ● Beschreibung zum Berechtigungskonzept einschließlich Benutzerverwaltung sowie zum Zugriffs- und Zugangsschutz. **(Die Prüfung der Wirksamkeit der Maßnahmen erfolgt im Rahmen der Prüfung der Ergänzungselementen (1) bis (4))**	160

Basiselement: Verfahrensdokumentation			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
8.	**Bestandteile und Inhalte der Verfahrensdokumentation (Internes Kontrollsystem)** Die Beschreibung des Internen Kontrollsystems (IKS) ist Bestandteil der Verfahrensdokumentation. Folgende Themen sind bspw. in die Verfahrensdokumentation aufzunehmen: ● Zugangs- und Zugriffsberechtigungskontrollen (Rn. 100, 103) ● Funktionstrennungen (Rn. 100) ● Erfassungs- und Eingabekontrollen (Rn. 40, 88, 100) ● Übertragungskontrollen (Rn. 88) ● Verarbeitungskontrollen (Rn. 60, 88,100) ● Abstimmungskontrollen bei der Dateneingabe (Rn. 100) ● Plausibilitätskontrollen (Rn. 40) ● Vollständigkeitskontrollen (Rn. 77) ● Schutzmaßnahmen gegen die beabsichtigte und unbeabsichtigte Verfälschung von Programmen, Daten und Dokumenten (Rn. 100) ● Datensicherung (Rn. 106)	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob bei der Darstellung der Kontrollen in der Verfahrensbeschreibung folgende Aspekte aufgegriffen werden: – Die Verfahrensdokumentation enthält die Beschreibung von grundsätzlichen Zielen und vom Aufbau des (steuerlichen) IKS. – Die Verfahrensdokumentation enthält Ausführungen zu den in den GoBD genannten Kontrollen. – Die Verfahrensdokumentation enthält Ausführungen zur Art der Kontrolle (manuell oder automatisch) und deren Häufigkeit (ereignisbasiert oder feste Frequenz). – Die zur Verfahrensdokumentation gehörenden Berechtigungskonzepte enthalten Aspekte der Funktionstrennung. ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob die Kontrollmaßnahmen inhaltlich zutreffend und vollständig dargestellt sind. **(Die Prüfung der Wirksamkeit der Maßnahmen erfolgt im Rahmen der Prüfung der Ergänzungselemente (1) bis (4))**	102

Generelle IT-Kontrollen

Die konkrete Umsetzung und Ausgestaltung der generellen IT-Kontrollen ist abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie der eingesetzten IT-Infrastruktur (vgl. GoBD, Rn. 100). Die hier beispielhaft dargestellten Prüfungshandlungen beziehen sich auf die Beurteilung der Einhaltung der Anforderungen aus den GoBD. Die beispielhafte Darstellung von Prüfungshandlungen für geschäftsprozessbezogene

IT-Kontrollen insb. bei den Anwendungsbezogenen IT-Kontrollen finden sich in den jeweiligen Prozessprozessen (Ergänzungselemente (1) bis (4)).

Die Prüfung der Angemessenheit und Wirksamkeit der generellen IT-Kontrollen richtet sich auf die für die Prüfung der für die jeweiligen Geschäftsprozesse (Ergänzungselemente (1) bis (4)) GoBD-relevanten Kontrollaktivitäten in den folgenden Bereichen:

- Changemanagement (Programm- und Datenänderungsverfahren)
- Zugang und Zugriff auf IT-Systeme (Datensicherheit)
- Prozesse zum Betrieb der IT-Infrastruktur (IT-Betrieb).

Die Prüfungshandlung zur Beurteilung der Angemessenheit der für die jeweiligen Geschäftsprozesse (Ergänzungselemente (1) bis (4)) eingerichteten Kontrollen einschließlich der generellen IT-Kontrollen (IKS) stützt sich auf die Inhalte der Verfahrensdokumentation.

Die im Folgenden dargestellten beispielhaften Prüfungshandlungen für die Beurteilung des Programmänderungs-Verfahrens (Change Management) im Rahmen einer kontinuierlichen Anpassung des DV-Systems beziehen sich auf die Autorisierung und Protokollierung von Änderungen sowie die Angemessenheit von Test- und Freigabeprozeduren. Hiervon nicht umfasst sind Test- und Freigabeprozeduren für die Beurteilung eines Systemwechsels.[8]

Sofern im Prüfungszeitraum Veränderungen am DV-System durchgeführt werden bzw. erfolgen sollen (bspw. ein Systemwechsel (vgl. GoBD, Rn. 142), bietet sich die Durchführung einer gesonderten projektbegleitenden Prüfung gemäß *IDW PS 850 n.F.* an.

Die in diesem *IDW Prüfungshinweis* dargestellten beispielhaften Prüfungshandlungen für die Beurteilung der Maßnahmen zum Zugangs- und Zugriffsschutz auf IT-Systeme betreffen die baulichen und technischen Maßnahmen zur Verhinderung eines nicht autorisierten Zugangs zu Hardware, Datenbanken oder Netzwerkkomponenten. Diese physischen Maßnahmen werden ergänzt um Zugriffsschutzkonzepte, die den logischen Zugriff auf Betriebssysteme und Datenbanken nur besonders autorisierten Mitarbeitern gestatten. Ferner sind innerhalb der IT-Anwendungen Zugriffe in einer Weise einzurichten, dass Mitarbeitern nur die zur Erfüllung ihrer Aufgaben erforderlichen Rechte zugewiesen werden (need to know) sowie die Funktionstrennung auch auf Ebene der IT-Systeme umgesetzt ist (segregation of duties).

Die Maßnahmen zur Einrichtung und Aufrechterhaltung eines angemessenen IT-Betriebs umfassen alle Aktivitäten, die für einen geordneten, sicheren und störungsfreien Betrieb von IT-Anwendungen erforderlich sind.

Art und Umfang der Maßnahmen sind abhängig von der Größe, der Komplexität und den technischen Gegebenheiten der IT-Infrastruktur.

---

[8] Vgl. *IDW PS 850 n.F.*, Tz. 27 ff. Liegt derzeit vor als *Entwurf einer Neufassung des IDW Prüfungsstandards: Projektbegleitende Prüfung bei Einsatz von Informationstechnologie an (IDW PS 850 n.F.)* (Stand: 26.03.2021).

Typische IT-Prozesse sind neben dem Change Management etwa das Incident- und Problemmanagement sowie die Jobsteuerung, die Produktionsüberwachung und der Netzbetrieb.

Basiselement: Generelle IT-Kontrollen			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
9.	**Change Management (Programm- und Datenänderungsverfahren)** Einrichtung eines Prozesses zur Programm- und Datenänderung bzw. Pflege unter Berücksichtigung der folgenden Anforderungen: ● Autorisierung von Programmänderung ● Test- und Freigabeprozeduren.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation hinsichtlich Aktualität, Vollständigkeit der Inhalte und angemessener Abbildung des Change-Prozesses ● Inaugenscheinnahme der Unterlagen und Beobachtung der Verfahren hinsichtlich Aktualität, Vollständigkeit der Inhalte und angemessener Abbildung geforderter Freigabe von Programmänderungen durch die Fachabteilungen. **Wirksamkeit:** ● Nachvollzug der Einhaltung des angewiesenen Entwicklungs-, Test-, und Freigabeverfahrens anhand im Prüfungszeitraum durchgeführter Programmänderungen.	100, 107 - 112
10.	**Zugangsschutz (Datensicherheit)** ● Für die Einhaltung der Ordnungsvorschriften des § 146 AO hat der Steuerpflichtige Zugangsberechtigungskontrollen auf Basis entsprechender Zugangsberechtigungskonzepte einzurichten ● Der Steuerpflichtige hat sein DV-System gegen Verlust zu sichern und gegen unberechtigte Eingaben und Veränderungen (z.B. durch Zugangskontrollen) zu schützen.	**Angemessenheit:** ● Einsichtnahme in Verfahrensdokumentationen zur physischen Sicherheit von Daten und Informationssystemen bzgl. Vollständigkeit, Aktualität, Vorhandensein von Schutzmaßnahmen gegen unbefugten Zugang zu Räumlichkeiten und Gebäuden einschließlich Monitoring-Kontrollen (z.B. Kameraüberwachung oder Auswertung von Zugangsprotokollen von Türen) sowie Verfahren zur Beantragung und Genehmigung von physischem Zutritt ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob ausreichende Maßnahmen zum Schutz gegen äußere Gewalt (Wasser, Feuer etc.) vorgesehen sind	100, 103

Basiselement: Generelle IT-Kontrollen			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		● Beobachtung der Existenz der Zutrittskontrollen durch die Begehung von Gebäuden oder Räumlichkeiten. **Wirksamkeit:** ● Abgleich der im Zutrittssystem eingerichteten Personen mit den in der Organisationsanweisung benannten Personen ● Nachvollzug der Übereinstimmung der tatsächlichen Zutrittskontrollen mit den definierten Verfahren und Maßnahmen in den entsprechenden Dokumentationen ● Nachvollzug anhand von Listen der Mitarbeiter, die relevante Serverräume betreten dürfen, ob diese Listen regelmäßig auf deren Vollständigkeit, Inhalte und Aktualität überprüft werden ● Nachvollzug der Nachweise über die Überprüfung von Einlassprotokollen.	
11.	**Zugriffsschutz (Datensicherheit)** ● Für die Einhaltung der Ordnungsvorschriften des § 146 AO hat der Steuerpflichtige Zugriffsberechtigungskontrollen auf Basis entsprechender Zugriffsberechtigungskonzepte einzurichten ● Der Steuerpflichtige hat sein DV-System gegen Verlust zu sichern und gegen unberechtigte Eingaben und Veränderungen (z.B. durch Zugriffskontrollen) zu schützen.	**Zugriffsschutz** **Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Regelungen zur Überwachung privilegierter Mitarbeiter (z.B. Zugriff auf die Einrichtung der rechnungslegungsrelevanten Anwendungen oder auf Datenbanken) enthalten sind ● Einsichtnahme in relevante Dokumentationen des Rollen- und Rechtekonzepts sowie in die Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen im Hinblick auf Administratorberechtigungen.	100, 103

Basiselement: Generelle IT-Kontrollen			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob eine personalisierte und für die Aufgabenwahrnehmung notwendige Zuweisung vorgesehen ist. **Wirksamkeit:** ● Abgleich von im System abgebildeten Usern mit weitreichenden/kritischen Berechtigungen mit der Liste aller User mit weitreichenden/kritischen Berechtigungen (bspw. Super-, System-, Admin-, Notfall-User) ● Abgleich von auf Datenbank-/und Betriebssystemebene abgebildeten Usern mit der Liste aller User mit direktem Zugriff auf Betriebssystem- und Datenbankebene.	
12.	**IT-Betrieb (Datensicherungs- und Wiederherstellungsverfahren)** Sicherung der Verfügbarkeit des IT-Systems insb. durch die Sicherung der Daten, Datensätze, elektronischer Unterlagen und Dokumente vor Verlust.	**Angemessenheit:** ● Einsichtnahme in den Teil der Verfahrensdokumentationen der die Richtlinien, Verfahren und Maßnahmen von Backup- und Recovery-Prozeduren einschließlich der Zuordnung von Aufgaben zu qualifizierten Mitarbeitern enthält ● Einsichtnahme in Listen/Dokumentationen der Mitarbeiter mit Zugriffsrechten, um festzustellen, ob es Regelungen zur Verwaltung von Protokollierungs- und Überwachungsfunktionalitäten gibt. ● Einsichtnahme in die Richtlinien und Vorgaben, um festzustellen, ob bei Veränderungen sichergestellt wird, dass die DV-Systeme in die Datensicherung einbezogen werden ● Einsichtnahme in die Systemeinstellungen, um festzustellen, ob automatische Datensicherungen überwacht werden und ob fehlerhafte Datensicherungen gemeldet und entsprechende Maßnahmen eingeleitet werden.	100, 103, 104 106

Basiselement: Generelle IT-Kontrollen			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		Wirksamkeit: Nachvollzug anhand von Logfiles, ● ob die Datensicherungen vorgenommen wurden, ● ob der Zugriff auf die gesicherten Daten auf autorisiertes Personal beschränkt ist, ● ob automatisierte IT-Kontrollen zur Sicherung von Daten (Backups) und Wiederherstellung von Daten (Restore) durchgeführt wurden.	
13.	**IT-Betrieb (Outsourcing)** Für die Ordnungsmäßigkeit elektronischer Bücher und sonst erforderlicher elektronischer Aufzeichnungen i.S. der Rn. 3 bis 5, einschließlich der eingesetzten Verfahren, ist allein der Steuerpflichtige verantwortlich. Dies gilt auch bei einer teilweisen oder vollständigen organisatorischen und technischen Auslagerung von Buchführungs- und Aufzeichnungsaufgaben auf Dritte.	**Angemessenheit:** Einsichtnahme in die Verfahrensbeschreibung zum Outsourcing und der Inhalte von Vertragsunterlagen/SLAs mit den externen Dienstleistern, um festzustellen, ob Kontroll- und Überwachungsmaßnahmen für die Dienstleistungen vorgesehen sind. **Wirksamkeit:** Nachvollzug der Kontroll- und Überwachungsmaßnahmen für die Dienstleistungen.	21, 100, 103, 106

Ergänzungselement (1): Belegeingang

Die GoBD-Anforderungen an den Belegeingang werden tabellarisch wie folgt gegliedert:

I. Generelle GoBD-Vorgaben für den Belegeingang
II. Die spezifischen GoBD-Vorgaben für die bildliche Erfassung von eingehenden Papierbelegen
III. Die spezifischen GoBD-Vorgaben für den elektronischen Belegeingang
IV. Die spezifischen GoBD-Vorgaben für die Rechnungseingangsprüfung.

I. Generelle Anforderungen (unabhängig von der Art und Form der eingehenden Belege)

Handels- oder Geschäftsbriefe und Buchungsbelege können originär elektronisch oder in Papierform empfangen werden. In Papierform empfangene Dokumente werden anschließend digitalisiert und damit bildlich erfasst (z.B. gescannt oder fotografiert). Für die im Rahmen des

Belegeingangs implementierten Kontrollen sind die nachfolgend dargestellten generellen GoBD-Vorgaben zu beachten. Diese sind bei der Prüfung des GoBD-relevanten IT-Systems sowohl für die Belegverarbeitung in Papierform als auch in originär elektronischer Form relevant.

Ergänzungselement (1): I. Generelle Anforderungen (unabhängig von der Art und Form der eingehenden Belege)			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
14.	**Vermeidung doppelter Erfassung** Ein und derselbe Geschäftsvorfall darf nicht mehrfach aufgezeichnet werden.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob und welche Maßnahmen die Mehrfacherfassung eines Belegs durch Abgleich spezifischer Informationen, wie z.B. der Rechnungsnummer, ausschließen (Identifikation von Duplikaten) ● Inaugenscheinnahme von Eskalations- oder Fehlerbehebungsverfahren bei Doppelerfassung nebst Protokollierung. ● Einsichtnahme in Schulungs- und Fortbildungsunterlagen **Wirksamkeit:** ● Nachvollzug von Systemeinstellungen zu Warnhinweisen oder Fehlermeldungen bei einer möglichen Doppelerfassung ● Nachvollzug, ob die Systemeinstellungen eine doppelte Erfassung verhindern ● Nachvollzug, ob Belege oder Buchungen zu Belegen mehrfach erfasst wurden.	41
15.	**Richtigkeit** Geschäftsvorfälle sind in Übereinstimmung mit den tatsächlichen Verhältnissen und im Einklang mit den rechtlichen Vorschriften inhaltlich zutreffend durch Belege abzubilden, der Wahrheit entsprechend aufzuzeichnen und bei	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob es Regelungen und Vorgaben zur Prüfung der tatsächlichen und rechtlichen Einstufung der Geschäftsvorfälle gibt (z.B. Rechnungsprüfung)	44

Ergänzungselement (1): I. Generelle Anforderungen (unabhängig von der Art und Form der eingehenden Belege)			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	kontenmäßiger Abbildung zutreffend zu kontieren.	● Inaugenscheinnahme der Eskalations- oder Fehlerbehebungsverfahren bei Belegmängeln nebst Protokollierung ● Befragung der fachlichen Mitarbeiter zur Belegprüfung ● Einsichtnahme in Schulungs- und Fortbildungsunterlagen. **Wirksamkeit:** Nachvollzug der Zuordnung von Belegen zu bestimmten Geschäftsvorfällen (z.B. Eingangsrechnung) und Abgleich der Belege mit den erfassten Daten (Richtigkeit der Erfassung).	
16.	**Systematische Erfassung und Aufbewahrung nach bestimmten Ordnungsprinzipien** ● Systematische Erfassung und übersichtliche, eindeutige und nachvollziehbare Buchungen ● Die geschäftlichen Unterlagen dürfen nicht planlos gesammelt und aufbewahrt werden ● Bücher und Aufzeichnungen sind nach bestimmten Ordnungsprinzipien zu führen ● Sammlung und Aufbewahrung der Belege hat so zu erfolgen, dass die Geschäftsvorfälle leicht und identifizierbar feststellbar und für einen die Lage des Vermögens darstellenden Abschluss unverlierbar sind ● Die einzelnen Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung lückenlos verfolgen lassen (progressive und retrograde Prüfbarkeit).	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob es Regelungen und Vorgaben zur Erfassung, Indexierung sowie Be- und Verarbeitung der Eingangsbelege gibt ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob es Regelungen und Vorgaben gibt, nach denen die eingehenden Belege sortiert und nach einem spezifischen Ordnungsprinzip (Indexierung) der elektronischen Aufbewahrung zugeführt werden ● Einsichtnahme in die Systemeinstellungen, nach denen die eingehenden elektronischen Belege bzw. digitalisierte Belege nach einem spezifischen Ordnungsprinzip aufbewahrt werden. **Wirksamkeit:** ● Nachvollzug der Ablage der Belege in der Archivumgebung und Nachvollzug der Ordnungsprinzipien (Indexierung) der Ablage	32, 53, 54

Ergänzungselement (1): I. Generelle Anforderungen (unabhängig von der Art und Form der eingehenden Belege)			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		● Nachvollzug anhand der Belege im Hinblick auf die progressive und retrograde Prüfbarkeit ● Nachvollzug der Ordnungsprinzipien der Ablage anhand einzelner Belege.	
17.	**Unveränderbarkeit (Bewegungsdaten)** ● Eine Buchung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. ● Veränderungen und Löschungen von und an elektronischen Buchungen oder Aufzeichnungen müssen protokolliert werden. ● Spätere Änderungen sind ausschließlich so vorzunehmen, dass sowohl der ursprüngliche Inhalt als auch die Tatsache, dass Veränderungen vorgenommen wurden, erkennbar bleiben. ● Alle Informationen (Programme und Datenbestände), die einmal in den Verarbeitungsprozess eingeführt werden (Beleg, Grundaufzeichnung, Buchung), dürfen nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben, gelöscht, geändert oder verfälscht werden. ● Bereits in den Verarbeitungsprozess eingeführte Informationen (Beleg, Grundaufzeichnung, Buchung) dürfen nicht ohne Kenntlichmachung durch neue Daten ersetzt werden.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, wie mit Änderungen und Löschungen an den Bewegungsdaten verfahren wird. ● Einsichtnahme in eine ggf. vorliegende Softwarebescheinigung, ob und wie die Anwendungen die Unveränderbarkeit der Bewegungsdaten sicherstellt. ● Einsichtnahme in die Parametrisierung der IT-Anwendung, um festzustellen, ob und wie Veränderungen grundsätzlich ausgeschlossen werden oder nach Änderungen jederzeit der ursprüngliche Inhalt eingesehen werden kann (Festschreibung, Versionierung, Protokollierung) ● Einsichtnahme in die Parametrisierung der Softwareanwendungen, um festzustellen, ob und wie ein Löschen oder Überschreiben von Dokumenten grundsätzlich ausgeschlossen ist oder entsprechend protokolliert wird ● Inaugenscheinnahme der Konfiguration der Softwareanwendungen zur Verarbeitung und Archivierung. **Wirksamkeit:** ● Einspielen unterschiedlicher Belegtypen und Nachvollzug, ob eine Veränderung vorgenommen wurde bzw. ohne Kenntlichmachung vorgenommen werden kann	58, 59, 107, 108, 111

Ergänzungselement (1): I. Generelle Anforderungen (unabhängig von der Art und Form der eingehenden Belege)			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		● Nachvollzug der Änderungen an Belegen sowie der korrespondierenden Indexierung anhand der Protokollierung.	
18.	**Unveränderbarkeit (Geschäftsprozessbezogene Stammdaten)** ● Bei einer Änderung von Stammdaten muss die eindeutige Bedeutung in den entsprechenden Bewegungsdaten erhalten bleiben ● Ggf. müssen Stammdatenänderungen ausgeschlossen oder Stammdaten mit Gültigkeitsangaben historisiert werden, um mehrdeutige Verknüpfungen zu verhindern.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, wie mit Änderungen und Löschungen von Stammdaten bzw. Systemparametern verfahren wird ● Einsichtnahme in die Softwarebescheinigung, um festzustellen, ob die Anwendungen der Anforderung an die Unveränderbarkeit gerecht werden ● Einsichtnahme in die Parametrisierung der Anwendung, um festzustellen, ob und wie Stammdatenänderungen protokolliert und historisiert werden. Dies gilt auch für Systemeinstellungen, Schlüssel, Berechtigungen und Daten, die die Berechnungen in den Anwendungen steuern. **Wirksamkeit:** Nachvollzug der Änderung von Stammdaten anhand der entsprechenden Änderungsprotokolle.	111

II. Bildliche Erfassung der eingehenden Papierbelege

Handels- oder Geschäftsbriefe und Buchungsbelege können in Papierform empfangen und anschließend digitalisiert und damit bildlich erfasst (z.B. gescannt oder fotografiert) werden. Eine bildliche Erfassung kann hierbei mit den verschiedensten Arten von Geräten (z.B. Smartphones, Multifunktionsgeräten oder Scan-Straßen) erfolgen, wenn die Anforderungen der GoBD erfüllt sind. Nach der bildlichen Erfassung dürfen Papierdokumente vernichtet werden, soweit sie nicht nach außersteuerlichen oder steuerlichen Vorschriften im Original aufzubewahren sind.

Ergänzungselement (1): II. Bildliche Erfassung der eingehenden Papierbelege			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
19.	**Anforderungen und Inhalt einer Organisationsanweisung** Regelungen dazu, ● wer erfassen darf, ● zu welchem Zeitpunkt erfasst wird oder erfasst werden soll, ● welches Schriftgut erfasst wird, ● ob eine bildliche oder inhaltliche Übereinstimmung mit dem Original erforderlich ist, ● wie die Qualitätskontrolle auf Lesbarkeit und Vollständigkeit und ● wie die Protokollierung von Fehlern zu erfolgen hat.	**Angemessenheit:** ● Einsichtnahme in die Organisationsanweisung für die bildliche Erfassung von Belegen, um festzustellen, ob diese die notwendigen Vorgaben und Kontrollen enthalten ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Regelungen existieren, die sicherstellen, dass die Organisationsanweisung den zuständigen Mitarbeitern bekannt und verfügbar ist.	136
20.	**Vollständigkeit** ● Geschäftsvorfälle sind vollzählig und lückenlos aufzuzeichnen. ● Zusammenspiel von technischen (einschließlich programmierten) und organisatorischen Kontrollen ● Durch Erfassungs-, Übertragungs- und Verarbeitungskontrollen ist sicherzustellen, dass alle Geschäftsvorfälle vollständig erfasst oder übermittelt werden und danach nicht unbefugt und nicht ohne Nachweis des vorausgegangenen Zustandes verändert werden können. ● Die Durchführung der Kontrollen ist zu protokollieren.	**Angemessenheit:** ● Beobachtung des kompletten Prozesses vom Eingang der Papierbelege, zu deren bildlicher Erfassung sowie letztendlicher elektronischer Archivierung ● Inaugenscheinnahme von Schnittstellenkontrollen nebst Protokollierung ● Inaugenscheinnahme von Eskalations- oder Fehlerbehebungsverfahren nebst Protokollierung ● Einsichtnahme in Schulungs- und Fortbildungsunterlagen. **Wirksamkeit:** ● Nachvollzug der vorgesehenen technischen und organisatorischen Kontrollen, welche die vollständige Übertragung des bildlich erfassten Belegs bis hin zur elektronischen Aufbewahrung gewährleisten (z.B. Fehlermeldungen bzw. Fehlerordnung, Protokollierung aller Erfassungsvorgänge, Lückenanalyse oder Mehrfachbelegungsanalysen etc.) ● Nachvollzug von Eskalations- oder Fehlerbehebungsverfahren einschließlich Protokollierung	36, 40, 88

Ergänzungselement (1): II. Bildliche Erfassung der eingehenden Papierbelege			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		● Nachvollzug der Schnittstellen und der entsprechenden Schnittstellenprotokolle auf Vollständigkeit der Übertragung.	
21.	**Belegsicherung** ● Jeder Geschäftsvorfall ist zeitnah, d.h. möglichst unmittelbar nach seiner Entstehung, in einer Grundaufzeichnung oder in einem Grundbuch zu erfassen. ● Durch organisatorische Vorkehrungen ist sichergestellt, dass die Unterlagen bis zu ihrer Erfassung nicht verloren gehen. ● Die Belege in Papierform oder in elektronischer Form sind zeitnah, d.h. möglichst unmittelbar nach Eingang oder Entstehung, gegen Verlust zu sichern. ● Werden neben bildhaften Urschriften auch elektronische Meldungen bzw. Datensätze ausgestellt (identische Mehrstücke derselben Belegart), ist die Aufbewahrung der tatsächlich weiterverarbeiteten Formate (buchungsbegründende Belege) ausreichend, sofern diese über die höchste maschinelle Auswertbarkeit verfügen.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob es Vorgaben zur Sicherung der eingehenden Belege und deren zeitgerechte Erfassung gibt ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Kontrollen vorgesehen sind, welche eine zeitnahe bildliche Erfassung der eingehenden Papierbelege vorschreiben ● Durchführung eines Walk-Through-Tests durch Einsichtnahme in die Unterlagen zum gesamten Prozess vom Eingang der Papierbelege und deren bildliche Erfassung einschließlich deren elektronische Archivierung ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, wie mit identischen Mehrstücken derselben Belegart umzugehen ist ● Einsichtnahme in die Verfahrensdokumentation in Bezug auf die technischen und organisatorischen Maßnahmen zur Sicherung der eingehenden Belege und deren zeitgerechte Erfassung bzw. Sicherung ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, wie mit identischen Mehrstücken derselben Belegart umzugehen ist ● Inaugenscheinnahme von Schnittstellenkontrollen nebst Protokollierung ● Inaugenscheinnahme in Eskalations- oder Fehlerbehebungsverfahren nebst Protokollierung	46, 50, 67, 76

Ergänzungselement (1): II. Bildliche Erfassung der eingehenden Papierbelege			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		● Einsichtnahme in Schulungs- und Fortbildungsunterlagen. **Wirksamkeit:** ● Nachvollzug des Belegjournals auf zeitliche Unterschiede zwischen Erfassungs- und Belegdatum ● Nachvollzug der Belegsicherung anhand der entsprechenden Protokolle ● Nachvollzug des Empfangsdatums und der Erfassung in den Belegeingangssystemen und der Speicherung in den weiteren Systemen.	
22.	**Maßnahmen vor der bildlichen Erfassung (Aufbereitung)** Sicherstellung einer erfassungsgerechten Aufbereitung der Buchungsbelege.	**Angemessenheit:** ● Einsichtnahme in die Organisationsanweisung, um festzustellen, welche Aufbereitungsmaßnahmen an den Papierbelegen vor der bildlichen Erfassung vorzunehmen sind ● Einsichtnahme in die Organisationsanweisung, um festzustellen, welche Maßnahmen zum Umgang mit Rückseiten, Sonderformaten oder bspw. geösten/ gebundenen Dokumenten vorgesehen sind. ● Beobachtung der Aufbereitungsmaßnahmen an den Papierbelegen, die vor der bildlichen Erfassung vorgenommen werden. **Wirksamkeit:** ● Nachvollzug der Aufbereitungsmaßnahmen, ob diese tatsächlich vorgenommen werden ● Nachvollzug der korrekten Aufbereitung anhand archivierter Belege.	75
23.	**Ordnungsgemäße bildliche Erfassung** ● Papierdokumente werden durch bildliche Erfassung in elektronische Dokumente umgewandelt	**Angemessenheit:** ● Einsichtnahme in die Organisationsweisung zur bildlichen Erfassung, um festzustellen, ob die notwendigen Kontrollmaßnahmen sachgerecht berücksichtigt sind, insb.	75, 136, 137

Ergänzungselement (1): II. Bildliche Erfassung der eingehenden Papierbelege			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● Qualitätskontrolle auf Lesbarkeit und Vollständigkeit ● Protokollierung von Fehlern ● Vollständige Farbwiedergabe, wenn der Farbe Beweisfunktion zukommt.	– Authentifizierungsmechanismen (insb. beim mobilen Scannen), – Maßnahmen zur korrekten Dokumententrennung (z.B. bei Stapelerfassung) existieren, – Maßnahmen zur Rückseitenerfassung, – Maßnahmen zur ggf. erforderlichen Farberfassung, – Maßnahmen zur Qualitätskontrolle, – Prozess zur Identifikation von Belegen mit dem Erfordernis einer bildlichen Erfassung in Farbe, – Maßnahmen zur Eskalation fehlerhafter bzw. nicht verarbeitbarer Dokumente. ● Beobachtung des Verarbeitungsprozesses der bildlichen Erfassung und Abgleich mit der Arbeitsanweisung ● Inaugenscheinnahme/Beobachtung von Eskalations- oder Fehlerbehebungsverfahren nebst Protokollierung ● Einsichtnahme in Schulungs- und Fortbildungsunterlagen. **Wirksamkeit:** ● Nachvollzug der bildlichen Erfassung von Dokumenten und der Durchführung der notwendigen Kontrollschritte ● Nachvollzug von Eskalations- oder Fehlerbehebungsverfahren einschließlich Protokollierung.	
24.	**Lesbarkeit (Bildliche Wiedergabe)** Das bildlich erfasste Dokument ist so aufzubewahren, dass die Wiedergabe mit dem Original bildlich übereinstimmt, wenn es lesbar gemacht wird.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob und welche Maßnahmen vorgesehen sind zur	130

Ergänzungselement (1): II. Bildliche Erfassung der eingehenden Papierbelege			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		– originalgetreuen Übertragung des Abbilds auf das Speichersystem, – originalgetreuen Übertragung des Belegbilds ins Unternehmen (mobile bildliche Erfassung), – Sicherung der Lesbarkeit über die Dauer der Aufbewahrungsfrist. ● Inaugenscheinnahme der Systemeinstellungen zur Sicherung der originalgetreuen Übertragung ● Inaugenscheinnahme der Systemeinstellungen zur Sicherung der Lesbarkeit über die Dauer der Aufbewahrungsfrist. **Wirksamkeit:** Nachvollzug der Lesbarkeit von digitalisierten Belegen in der Archivumgebung.	
25.	**Weiterbearbeitung (der Papierbelege nach der bildlichen Erfassung)** ● Im Anschluss an den Erfassungsvorgang darf die weitere Bearbeitung nur mit dem elektronischen Dokument erfolgen ● Papierbelege sind dem weiteren Bearbeitungsgang zu entziehen ● Erneute Digitalisierung, sofern Papierbeleg bearbeitet wird und Herstellung eines Bezugs zur ersten elektronischen Erfassung.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation bzw. die Arbeitsanweisung, um festzustellen, wie mit Papierbelegen nach der Digitalisierung umgegangen wird. ● Beobachtung des Prozesses, wie mit Papierbelegen nach der Digitalisierung umgegangen wird ● Beobachtung des Prozesses, bei welchem nach dem Scanvorgang der ursprüngliche Papierbeleg weiterhin bearbeitet wird. **Wirksamkeit:** Nachvollzug der digitalisierten Belege auf nachträgliche Annotationen.	139
26.	**OCR-Verarbeitung** Erfolgt eine Anreicherung der Bildinformationen, z.B. durch OCR, sind die dadurch gewonnenen Informationen	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob es Regelungen zur Vorgehensweise bei der OCR-Erkennung gibt.	131

Ergänzungselement (1): II. Bildliche Erfassung der eingehenden Papierbelege			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	nach Verifikation und Korrektur ebenfalls aufzubewahren.	● Inaugenscheinnahme der Einstellungen bzw. Parametrisierung der IT-Anwendungen für den OCR-Prozess einschließlich OCR-Erkennung zur OCR-Verarbeitung ● Inaugenscheinnahme der Einstellungen der IT-Anwendungen zur Indexierung. **Wirksamkeit:** ● Aufruf von Belegen und Nachvollzug der OCR-Erkennung ● Nachvollzug der Änderungsprotokollierung zur OCR-Erkennung.	
27.	**Vernichtung von Papierbelegen** Nach der bildlichen Erfassung dürfen Papierdokumente vernichtet werden, soweit sie nicht nach außersteuerlichen oder steuerlichen Vorschriften im Original aufzubewahren sind.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, welche Papierbelege wann und wie nach dem bildlichen Erfassen vernichtet werden können ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, welche Papierdokumente weiterhin im Papieroriginal aufzubewahren sind und nicht vernichtet werden dürfen. **Wirksamkeit:** Nachvollzug des Vorhandenseins von Papierbelegen, welche im Original aufzubewahren sind.	160

III. Elektronischer Belegeingang

Handels- oder Geschäftsbriefe und Buchungsbelege können originär elektronisch empfangen werden. Dabei ist regelmäßig zwischen unstrukturierten Informationen (Bildformate) und strukturierten Informationen (Daten) zu unterscheiden. Unabhängig davon hat die Weiterverarbeitung und Archivierung stets originär elektronisch zu erfolgen.

Ergänzungselement (1): III. Elektronischer Belegeingang			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
28.	**Vollständigkeit** **Eingang originär elektronischer Belege** ● Geschäftsvorfälle sind vollzählig und lückenlos aufzuzeichnen. ● Zusammenspiel von technischen (einschließlich programmierten) und organisatorischen Kontrollen ● Durch Erfassungs-, Übertragungs- und Verarbeitungskontrollen ist sicherzustellen, dass alle Geschäftsvorfälle vollständig erfasst oder übermittelt werden und danach nicht unbefugt und nicht ohne Nachweis des vorausgegangenen Zustandes verändert werden können. ● Die Durchführung der Kontrollen ist zu protokollieren.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, wie mit empfangenen originär elektronischen Belegen verfahren wird, welche Kontrollen für die Vollständigkeit eingerichtet sind und welche IT-Systeme dabei eingesetzt werden ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob die dargestellten digitalen Eingangswege mit den tatsächlichen Eingangswegen übereinstimmen ● Inaugenscheinnahme der Systemeinstellungen der IT-Anwendung für originär digital empfangene Dokumente (z.B. Mail-Empfang, EDI und EDI-Konverter, Internet-Anwendungen etc.) ● Inaugenscheinnahme von Schnittstellenkontrollen und Schnittstellenprotokolle zur vollzähligen und lückenlosen Verarbeitung ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Eskalations- oder Fehlerbehebungsverfahren nebst Protokollierung vorgesehen sind. **Wirksamkeit:** ● Nachvollzug der vorgesehenen technischen und organisatorischen Kontrollen, welche die vollständige Übertragung des originär elektronischen Belegs bis hin zur elektronischen Aufbewahrung gewährleisten (z.B. Fehlermeldungen bzw. Fehlerordnung, Protokollierung aller Erfassungsvorgänge, Lückenanalyse oder Mehrfachbelegungsanalysen etc.) ● Nachvollzug von Eskalations- oder Fehlerbehebungsverfahren einschließlich Protokollierung	36, 40, 88

Ergänzungselement (1): III. Elektronischer Belegeingang			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		● Nachvollzug der Schnittstellen und der entsprechenden Schnittstellenprotokolle auf Vollständigkeit der Übertragung.	
29.	**Belegsicherung** ● Jeder Geschäftsvorfall ist zeitnah, d.h. möglichst unmittelbar nach seiner Entstehung, in einer Grundaufzeichnung oder in einem Grundbuch zu erfassen. ● Durch organisatorische Vorkehrungen ist sichergestellt, dass die Unterlagen bis zu ihrer Erfassung nicht verloren gehen. ● Die Belege in Papierform oder in elektronischer Form sind zeitnah, d.h. möglichst unmittelbar nach Eingang oder Entstehung, gegen Verlust zu sichern. ● Werden neben bildhaften Urschriften auch elektronische Meldungen bzw. Datensätze ausgestellt (identische Mehrstücke derselben Belegart), ist die Aufbewahrung der tatsächlich weiterverarbeiteten Formate (buchungsbegründende Belege) ausreichend, sofern diese über die höchste maschinelle Auswertbarkeit verfügen.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob es Vorgaben zur Sicherung der digital eingehenden Belege und deren zeitgerechte Erfassung gibt ● Inaugenscheinnahme der Einstellungen/Konfiguration des bzw. der elektronischen Empfangswege ● Erhebung, ob für Belege, die per Mail empfangen werden, ein zentrales Mail-Postfach (Funktionspostfach) eingerichtet wurde. **Wirksamkeit:** ● Nachvollzug des Prozesses für jeden digitalen Eingangsweg ● Nachvollzug anhand des Empfangsdatums und der Erfassung in den Belegeingangssystemen und der Speicherung in den weiteren Systemen.	46, 50, 67, 82
III.a Elektronische Belege in unstrukturierter Form			
30.	**Lesbarkeit** **Bildliche Wiedergabe** Es ist sichergestellt, dass die Wiedergabe oder die Daten mit den empfangenen Handels- oder Geschäftsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, welche technischen und organisatorischen Maßnahmen zur Sicherstellung einer lesbaren bildlichen Wiedergabe vorgesehen sind ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, welche technischen und organisatorischen Maßnahmen zur vollständigen und richtigen Übertragung	118

Ergänzungselement (1): III. Elektronischer Belegeingang			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		der Datei auf das Speichersystem vorgesehen sind. **Wirksamkeit:** Nachvollzug der Lesbarkeit der elektronischen Belege in der Archivumgebung.	
31.	**OCR-Verarbeitung** Erfolgt eine Anreicherung der Bildinformationen, z.B. durch OCR, sind die dadurch gewonnenen Informationen nach Verifikation und Korrektur und Speicherung ebenfalls aufzubewahren.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation zur Vorgehensweise bei der Indexierung / OCR-Erkennung ● Inaugenscheinnahme der Einstellungen der IT-Anwendungen zur Indexierung ● Inaugenscheinnahme der Einstellungen der IT-Anwendungen für das OCR-Verfahren. **Wirksamkeit:** ● Nachvollzug der Änderungsprotokollierung zur OCR-Erkennung und zur Indexierung ● Aufruf von Belegen und Nachvollzug der OCR-Erkennung bzw. Indexierung.	131
III.b Elektronische Belege in strukturierter Form			
32.	**Lesbarkeit** ● Es ist sichergestellt, dass die Wiedergabe oder die Daten mit den empfangenen Handels- oder Geschäftsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation in Bezug auf die technischen und organisatorischen Maßnahmen zur Visualisierung von elektronischen Belegen in strukturierter Form ● Beobachtung/Inaugenscheinnahme des Prozesses anhand eines Dokuments. **Wirksamkeit:** Nachvollzug des Verfahrens zur Lesbarkeit bzw. Visualisierung von elektronischen Belegen anhand eines Dokuments.	118

IV. Rechnungseingangsprüfung

Entsprechend § 14 Abs. 1 UStG müssen bei einer Rechnung die Echtheit der Herkunft, die Unversehrtheit ihres Inhalts und ihre Lesbarkeit gewährleistet werden. Echtheit der Herkunft (Authentizität) bedeutet die Sicherheit der Identität des Rechnungsausstellers. Unversehrtheit des Inhalts (Integrität) bedeutet, dass die nach dem Umsatzsteuergesetz erforderlichen Rechnungsangaben nicht geändert wurden. Dabei legt jedes Unternehmen in eigener Verantwortung fest, in welcher Weise die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit der Rechnung gewährleistet werden. Dies lässt sich regelmäßig durch ein sog. „innerbetriebliches Kontrollverfahren mit Prüfpfad“ erfüllen, welches nach herrschender Meinung dem Prozedere der Rechnungseingangsprüfung gleichzusetzen ist.

Ergänzungselement (1): IV. Rechnungseingangsprüfung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
33.	**Unversehrtheit des Inhalts (Integrität)** ● Für umsatzsteuerrechtliche Zwecke können weitere Angaben erforderlich sein. ● Dazu gehören bspw. die Rechnungsangaben nach §§ 14, 14a UStG und § 33 UStDV.	**Angemessenheit:** Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob folgende Kontrollen vorgesehen sind: ● Rechnungseingangsprüfung – Kontrollen, die gewährleisten, dass alle umsatzsteuerlichen Pflichtangaben i.S.v. §§ 14, 14a UStG, §§ 33, 34 UStDV gegeben sind einschließlich Prüfpfad – Eskalations- oder Fehlerbehebungsverfahren beim Feststellen von Mängeln. **Wirksamkeit:** ● Nachvollzug der formellen Rechnungseingangsprüfung einschließlich Prüfpfad ● Nachvollzug der Rechnungsprüfung in den Fällen, in denen die formelle Rechnungseingangsprüfung fehlgeschlagen ist.	78
34.	**Echtheit der Herkunft (Authentizität)** ● Für umsatzsteuerrechtliche Zwecke können weitere Angaben erforderlich sein.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob folgende Kontrollen vorgesehen sind:	78

Ergänzungselement (1): IV. Rechnungseingangsprüfung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● Dazu gehören bspw. die Rechnungsangaben nach §§ 14, 14a UStG bzw.§ 33 UStDV.	– Sachliche Rechnungseingangsprüfung sowie Abgleich mit der Dokumentation und umgekehrt – Vorhandensein eines Vier-Augen-Prinzips einschließlich Prüfpfad – Vorhandensein eines Eskalations- oder Fehlerbehebungsverfahrens beim Feststellen von Mängeln. ● Einsichtnahme in Schulungs- und Fortbildungsunterlagen. **Wirksamkeit:** ● Nachvollzug der sachlichen Rechnungseingangsprüfung einschließlich Prüfpfad ● Nachvollzug der Rechnungsprüfung in den Fällen, in denen die sachliche Rechnungseingangsprüfung fehlgeschlagen ist.	

Ergänzungselement (2): Elektronischer Belegausgang

Handels- oder Geschäftsbriefe und Buchungsbelege können originär elektronisch übermittelt werden. Dabei ist regelmäßig zwischen unstrukturierten Informationen (Bildformate) und strukturierten Informationen (Daten) zu unterscheiden. Unabhängig davon hat die Weiterverarbeitung und Aufbewahrung stets originär elektronisch zu erfolgen.

Ergänzungselement (2): Elektronischer Belegausgang			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
Generelle Vorschriften (grundsätzlich bei allen Prozessschritten zum Ausgang elektronischer Belege zu beachten)			
35.	**Vollständigkeit (Technische/Organisatorische Kontrollen)** ● Geschäftsvorfälle sind vollzählig und lückenlos aufzuzeichnen	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob geeignete Kontrollen zu folgenden	36, 40, 88

Ergänzungselement (2): Elektronischer Belegausgang			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● Zusammenspiel von technischen (einschließlich programmierten) und organisatorischen Kontrollen ● Durch Erfassungs-, Übertragungs- und Verarbeitungskontrollen ist sicherzustellen, dass alle Geschäftsvorfälle vollständig erfasst oder übermittelt werden und danach nicht unbefugt und nicht ohne Nachweis des vorausgegangenen Zustandes verändert werden können ● Die Durchführung der Kontrollen ist zu protokollieren.	Aspekten der elektronischen Belegerstellung vorgesehen sind: – Elektronische Belege enthalten alle gesetzlich geforderten und mit dem Empfänger bilateral vereinbarten Angaben. – Elektronische Belege werden in einem gesetzlich zulässigen sowie vom Empfänger akzeptierten Format generiert. – Elektronische Belege werden vollständig ins Archiv übertragen. – Elektronische Belege werden vollständig und richtig an Dritte übersandt. ● Inaugenscheinnahme von Schnittstellenkontrollen nebst Protokollierung ● Inaugenscheinnahme von Eskalations- oder Fehlerbehebungsverfahren nebst Protokollierung ● Einsichtnahme in die Schulungs- und Fortbildungsunterlagen. **Wirksamkeit:** ● Nachvollzug des Prozesses zur Erzeugung der elektronischen Belege bis zur elektronischen Archivierung ● Nachvollzug von Eskalations- oder Fehlerbehebungsverfahren einschließlich Protokollierung.	
36.	**Vermeidung doppelter Erfassung** Ein und derselbe Geschäftsvorfall darf nicht mehrfach aufgezeichnet werden.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Maßnahmen zur Verhinderung der Mehrfacherfassung eines Belegs durch Abgleich spezifischer Informationen, wie z.B. der Rechnungsnummer (Identifikation von Duplikaten), vorhanden sind. ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob	41

Ergänzungselement (2): Elektronischer Belegausgang			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		Eskalations- oder Fehlerbehebungsverfahren bei einer doppelten Erfassung nebst Protokollierung vorgesehen sind. ● Einsichtnahme in Schulungs- und Fortbildungsunterlagen. **Wirksamkeit:** ● Nachvollzug, ob die Systemeinstellungen eine doppelte Erstellung verhindern ● Nachvollzug von Systemeinstellungen zu Warnhinweisen oder Fehlermeldungen bei einer möglichen Doppelerstellung ● Nachvollzug, dass jeweils nur ein Beleg gefunden wird (z.B. im Archivsystem).	
37.	**Richtigkeit** Geschäftsvorfälle sind in Übereinstimmung mit den tatsächlichen Verhältnissen und im Einklang mit den rechtlichen Vorschriften inhaltlich zutreffend durch Belege abzubilden, der Wahrheit entsprechend aufzuzeichnen und bei kontenmäßiger Abbildung zutreffend zu kontieren.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Kontrollen zur korrekten Erzeugung von Belegen vorgesehen sind ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Eskalations- und Fehlerbehebungsverfahren bei fehlerhaften Belegen nebst Protokollierung vorgesehen sind. ● Befragung der fachlichen Mitarbeiter zur Belegerstellung ● Einsichtnahme in Schulungs- und Fortbildungsunterlagen. **Wirksamkeit:** Nachvollzug der Übereinstimmung von Belegen zur Leistungserbringung.	44
38.	**Belegsicherung** ● Jeder Geschäftsvorfall ist zeitnah, d.h. möglichst unmittelbar nach seiner Entstehung, in einer Grundaufzeichnung oder in einem Grundbuch zu erfassen.	**Angemessenheit:** Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob die Sicherung der ausgehenden Belege und deren zeitgerechte Erfassung vorgesehen sind.	46, 50, 76, 82

Ergänzungselement (2): Elektronischer Belegausgang			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● Durch organisatorische Vorkehrungen ist sichergestellt, dass die Unterlagen bis zu ihrer Erfassung nicht verloren gehen. ● Die Belege in Papierform oder in elektronischer Form sind zeitnah, d.h. möglichst unmittelbar nach Eingang oder Entstehung, gegen Verlust zu sichern ● Werden neben bildhaften Urschriften auch elektronische Meldungen bzw. Datensätze ausgestellt (identische Mehrstücke derselben Belegart), ist die Aufbewahrung der tatsächlich weiterverarbeiteten Formate (buchungsbegründende Belege) ausreichend, sofern diese über die höchste maschinelle Auswertbarkeit verfügen.	**Wirksamkeit:** ● Falls die ausgehenden Dokumente in den Erstellungsprogrammen (Fakturierungsprogramm) gespeichert werden, ist nachzuvollziehen, ob folgende Systemeinstellungen vorgenommen wurden: – Historisierung der Stammdaten – Historisierung der AGB´s – Historisierung der Layouts. ● Nachvollzug des Belegjournals auf zeitliche Unterschiede zwischen Erfassungs- und Belegdatum ● Nachvollzug der Belegsicherung anhand der entsprechenden Protokolle ● Nachvollzug anhand der Reproduktion eines versendeten Dokuments, ob seit der Versendung des Dokuments Veränderungen an den Stammdaten, rechnungsrelevanten Schlüsseln oder des Layouts erfolgt sind.	
39.	**Systematische Erfassung und Aufbewahrung nach bestimmten Ordnungsprinzipien** ● Systematische Erfassung und übersichtliche, eindeutige und nachvollziehbare Buchungen ● Die geschäftlichen Unterlagen dürfen nicht planlos gesammelt und aufbewahrt werden. ● Bücher und Aufzeichnungen sind nach bestimmten Ordnungsprinzipien zu führen. ● Die Sammlung und Aufbewahrung der Belege hat so zu erfolgen, dass die Geschäftsvorfälle leicht und identifizierbar feststellbar und für einen die Lage des Vermögens darstellenden Abschluss unverlierbar sind.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Vorgaben und Maßnahmen existieren, nach denen die ausgehenden elektronischen Belege nach einem spezifischen Ordnungsprinzip aufbewahrt werden ● Einsichtnahme in die Systemeinstellungen, um festzustellen, ob die ausgehenden elektronischen Belege nach einem spezifischen Ordnungsprinzip aufbewahrt werden. **Wirksamkeit:** ● Nachvollzug der Ablage der Belege in der Archivumgebung und Nachvollzug der Ordnungsprinzipien (Indexierung) der Ablage	32, 53, 54

Ergänzungselement (2): Elektronischer Belegausgang			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● Die einzelnen Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung lückenlos verfolgen lassen (progressive und retrograde Prüfbarkeit).	● Nachvollzug anhand der Belege im Hinblick auf die progressive und retrograde Prüfbarkeit ● Nachvollzug der Ordnungsprinzipien der Ablage anhand einzelner Belege.	
40.	**Unveränderbarkeit (Bewegungsdaten)** ● Eine Buchung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. ● Veränderungen und Löschungen von und an elektronischen Buchungen oder Aufzeichnungen müssen protokolliert werden. ● Spätere Änderungen sind ausschließlich so vorzunehmen, dass sowohl der ursprüngliche Inhalt als auch die Tatsache, dass Veränderungen vorgenommen wurden, erkennbar bleiben. ● Alle Informationen (Programme und Datenbestände), die einmal in den Verarbeitungsprozess eingeführt werden (Beleg, Grundaufzeichnung, Buchung), dürfen nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben werden.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, wie mit Änderungen und Löschungen an den Bewegungsdaten verfahren wird. ● Einsichtnahme in einer ggf. vorliegenden Softwarebescheinigung, um festzustellen, ob und wie die Anwendungen den Anforderungen an die Unveränderbarkeit gerecht wird ● Einsichtnahme in die Parametrisierung der Softwareanwendungen, um festzustellen, ob und wie Veränderungen grundsätzlich ausgeschlossen werden oder nach Änderungen jederzeit der ursprüngliche Inhalt eingesehen werden kann (Festschreibung, Versionierung, Protokollierung) ● Einsichtnahme in die Parametrisierung der Softwareanwendungen, um festzustellen, ob und wie ein Löschen oder Überschreiben von elektronisch erzeugten Dokumenten ausgeschlossen ist oder entsprechend protokolliert wird ● Inaugenscheinnahme der Konfiguration der Softwareanwendungen zur Verarbeitung und Archivierung. **Wirksamkeit:** ● Erzeugen und Archivierung unterschiedlicher Belegtypen mit anschließendem Nachvollzug, ob eine Veränderung vorgenommen wurde bzw. ohne Kenntlichmachung vorgenommen werden kann	58, 59, 107, 108, 111

Ergänzungselement (2): Elektronischer Belegausgang			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		● Nachvollzug der Änderungen an Belegen sowie der korrespondierenden Indexierung anhand der Protokollierung.	
41.	**Unveränderbarkeit (Prozessbezogene Stammdaten)** ● Bei einer Änderung von Stammdaten muss die eindeutige Bedeutung in den entsprechenden Bewegungsdaten erhalten bleiben ● Ggf. müssen Stammdatenänderungen ausgeschlossen oder Stammdaten mit Gültigkeitsangaben historisiert werden, um mehrdeutige Verknüpfungen zu verhindern.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, wie mit Änderungen und Löschungen von Stammdaten bzw. Systemparametern verfahren wird ● Einsichtnahme in ggf. vorliegende Softwarebescheinigung, ob und wie die Anwendungen die Anforderungen an die Unveränderbarkeit konzeptionell umsetzen ● Einsichtnahme in die Parametrisierung der IT-Anwendung, um festzustellen, ob und wie Stammdatenänderungen protokolliert und historisiert werden. Dies gilt auch für Systemeinstellungen, Schlüssel, Berechtigungen und Daten, die die Berechnungen in den Anwendungen steuern. **Wirksamkeit:** Nachvollzug, ob die Protokollierung der Änderungen von Stammdaten während des Prüfungszeitraums aktiviert war (anhand entsprechender Änderungsprotokolle).	111
Elektronische Belege in unstrukturierter Form			
42.	**Lesbarkeit (Bildliche Wiedergabe)** Es ist sichergestellt, dass die Wiedergabe oder die Daten mit den empfangenen Handels- oder Geschäftsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob es technische und organisatorische Maßnahmen zur Sicherstellung einer lesbaren Wiedergabe gibt ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob und welche technischen und organisatorischen Maßnahmen zur Sicherstellung der Lesbarkeit existieren.	118

Ergänzungselement (2): Elektronischer Belegausgang			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		Wirksamkeit: Nachvollzug der Lesbarkeit der elektronischen Belege in der Archivumgebung.	
Elektronische Belege in strukturierter Form			
43.	**Lesbarkeit** Es ist sichergestellt, dass die Wiedergabe oder die Daten mit den empfangenen Handels- oder Geschäftsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob technische und organisatorische Maßnahmen zur Visualisierung von elektronischen Belegen in strukturierter Form existieren ● Beobachtung/Inaugenscheinnahme des Verfahrens zur Lesbarkeit bzw. Visualisierung von elektronischen Belegen anhand eines Dokuments. **Wirksamkeit:** Nachvollzug der Lesbarkeit der elektronischen Belege in der Archivumgebung.	118
44.	**Reproduzierbarkeit** Bei Einsatz eines Fakturierungsprogramms muss unter Berücksichtigung von bestimmten Voraussetzungen keine bildhafte Kopie der Ausgangsrechnung (z.B. in Form einer PDF-Datei) ab Erstellung gespeichert bzw. aufbewahrt werden, wenn jederzeit auf Anforderung ein entsprechendes Doppel der Ausgangsrechnung erstellt werden kann.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob technische und organisatorische Maßnahmen zur Reproduzierbarkeit der ursprünglichen Rechnung existieren ● Beobachtung des Verfahrens zur Reproduktion von elektronischen Belegen. **Wirksamkeit:** Nachvollzug der Reproduktion von elektronischen Belegen.	76

Ergänzungselement (3): Elektronische Aufbewahrung

Sind aufzeichnungs- und aufbewahrungspflichtige Daten, Datensätze, elektronische Dokumente und elektronische Unterlagen im Unternehmen entstanden oder dort elektronisch eingegangen, sind sie auch in dieser Form aufzubewahren und dürfen vor Ablauf der Aufbewahrungsfrist nicht gelöscht werden.

Zur Erfüllung der gesetzlichen Aufbewahrungspflichten muss beim Einsatz von Archivierungsverfahren über den gesamten Prozess der Archivierung sichergestellt sein, dass alle Dokumente und Daten gemäß dem Archivierungskonzept erfasst werden, für welche die elektronische Archivierung zulässig bzw. notwendig ist oder festgelegt wurde. Ferner muss sichergestellt werden, dass die Daten und Dokumente für die Dauer der Aufbewahrungspflicht innerhalb angemessener Zeit wiedergegeben werden können.

Bei einer Verlagerung ins Ausland gilt auf der Basis einer Änderung der Abgabenordnung durch das Jahressteuergesetz 2020 (JStG 2020) Folgendes:

Soweit die elektronischen Bücher oder sonstigen erforderlichen elektronischen Aufzeichnungen in einem anderen Mitgliedstaat der Europäischen Union geführt und aufbewahrt werden, ist auf Grundlage von § 146 Abs. 2a AO sicherzustellen, dass der Datenzugriff der Finanzverwaltung nach § 147 Abs. 6 AO in vollem Umfang möglich ist. Eines Antrags, wie vor der Novellierung durch das JStG 2020 gefordert, bedarf es in diesen Fällen nicht mehr. Die Antragspflicht besteht jedoch fort, soweit die Verlagerung in einen Drittstaat erfolgt. In diesen Fällen bedarf es auf Grundlage des durch das JStG 2020 neu gefassten § 147 Abs. 2b AO auch weiterhin eines schriftlichen oder elektronischen Antrags beim zuständigen Finanzamt.

Ergänzungselement (3): Elektronische Aufbewahrung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
45.	**Geordnete Ablage und Indexierung** ● Die aufbewahrungspflichtigen Unterlagen müssen geordnet aufbewahrt werden. ● Ein bestimmtes Ordnungssystem ist nicht vorgeschrieben. ● Ein elektronisches Dokument ist mit einem nachvollziehbaren und eindeutigen Index zu versehen. ● Der Erhalt der Verknüpfung zwischen Index und elektronischem Dokument muss während der gesamten Aufbewahrungsfrist gewährleistet sein.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Regelungen und Vorgaben existieren, welche Dokumente und Daten bzw. Dateien aufzubewahren bzw. zu archivieren sind ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob alle GoBD-relevanten Dokumente, Daten und Dateien berücksichtigt sind	117, 122

Ergänzungselement (3): Elektronische Aufbewahrung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● Es ist sicherzustellen, dass das elektronische Dokument unter dem zugeteilten Index verwaltet werden kann.	● Einsicht in Verfahrensdokumentationen bzgl. der Indexierung der aufzubewahrenden bzw. zu archivierenden Dokumente, Daten und Dateien (Aufbewahrung bzw. Archivierungsvorgang) ● Einsicht in die Einstellungen in den IT-Systemen, in denen die Dokumente, Daten und Dateien aufbewahrt werden (z.B. Archivsystem), ob die Indexierung geändert werden kann und die Änderungen protokolliert werden ● Inaugenscheinnahme der Vorgaben für die Indexstrukturen, bspw. numerische Zuordnung, Dokumentarten, Datum etc. ● Nachvollzug des Aufbewahrungs- bzw. Archivierungsvorgangs anhand eines Vorgangs. **Wirksamkeit:** ● Nachvollzug der Anzeige von Belegen in der Archivumgebung ● Nachvollzug der Auffindbarkeit von Dokumenten, Daten oder Dateien anhand der Indexierung.	
46.	**Unveränderbarkeit** ● Die Unveränderbarkeit der Daten, Datensätze, elektronischen Dokumente und elektronischen Unterlagen kann – hardwaremäßig (z.B. unveränderbare und fälschungssichere Datenträger) – softwaremäßig (z.B. Sicherungen, Sperren, Festschreibung, Löschmerker, automatische Protokollierung, Historisierungen, Versionierungen) – organisatorisch (z.B. Zuständigkeiten und Arbeitsanweisungen) gewährleistet werden.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob und wie die Unveränderbarkeit durch die Hardware (z.B. Festplatten), durch Einstellungen in der Anwendung (z.B. Dokumentenmanagementsystem) oder organisatorisch (z.B. Berechtigungskonzept) gewährleistet wird ● Einsichtnahme in die Verfahrensdokumentation zu den Einstellungen in den IT-Systemen, in denen die Dokumente Daten oder Dateien aufbewahrt bzw. archiviert werden, die dazu dienen festzustellen, ob und wie Änderungsaktionen an Da-	110

Ergänzungselement (3): Elektronische Aufbewahrung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● Die Ablage von Daten und elektronischen Dokumenten in einem Dateisystem erfüllt die Anforderungen der Unveränderbarkeit regelmäßig nicht, soweit nicht zusätzliche Maßnahmen ergriffen werden, die eine Unveränderbarkeit gewährleisten.	ten, Dokumenten und Systemeinstellungen sowie den beteiligten Personen nachvollziehbar sind ● Einsichtnahme in die Systemeinstellungen, um festzustellen, dass die Vorgaben der Verfahrensdokumentation eingehalten werden ● Einsichtnahme in eine ggf. vorhandene Softwarebescheinigung, dass die Anwendung über ausreichende Protokollfunktionen verfügt, die gewährleisten, dass Änderungsaktionen an Daten, Dokumenten und Systemeinstellungen sowie der beteiligten Personen nachvollziehbar bleiben bzw. Löschungen nicht möglich sind ● Einsichtnahme in eine ggf. vorhandene Softwarebescheinigung, dass Löschungen bzw. Hardware-Änderungen nicht zulässig sind ● Einsichtnahme in die Systemeinstellungen in Bezug auf die Einrichtung zur Gewährleistung der Unveränderbarkeit bei administrativem Zugriff. **Wirksamkeit:** ● Nachvollzug, ob Belege im Ursprungsformat aufbewahrt werden ● Nachvollzug, ob Änderungen protokolliert wurden ● ggf. Durchführung von Tests im Testsystem, ob archivierte Dokumente, Daten und Dateien ohne Protokollierung geändert bzw. gelöscht werden können.	
47.	**Protokollierung der Aktivitäten (Audit-Trail)** Bei elektronischen Unterlagen ist ihr ● Eingang, ● ihre Archivierung ● und ggf. Konvertierung ● sowie die weitere Verarbeitung	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um die Vorgaben für die Einrichtung der Protokollfunktion festzustellen ● Einsichtnahme in das Archivsystem zu den Einstellungen der entsprechenden Protokollfunktionen.	117

Ergänzungselement (3): Elektronische Aufbewahrung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	zu protokollieren. Es muss jedenfalls sichergestellt sein, dass ein sachverständiger Dritter innerhalb angemessener Zeit prüfen kann.	**Wirksamkeit:** ● Nachvollzug der Erfassung, Archivierung und Konvertierung von Dokumenten anhand von Protokollen.	
48.	**Aufbewahrung elektronischer Belege im Ursprungsformat** Elektronische Unterlagen sind im Ursprungsformat elektronisch aufzubewahren. Eine Umwandlung in ein anderes Format ist dann zulässig, wenn die maschinelle Auswertbarkeit nicht eingeschränkt wird und keine inhaltlichen Veränderungen vorgenommen werden.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation zu den GoBD-Vorgaben für die Aufbewahrung und Archivierung originär elektronischer Dokumente, Daten bzw. Dateien ● Inaugenscheinnahme der Systemeinstellungen, ob die GoBD-Vorgaben in der Verfahrensdokumentation entsprechend umgesetzt worden sind. **Wirksamkeit:** ● Nachvollzug des Aufbewahrungs- bzw. Archivierungsvorgangs sowie Abgleich mit der Dokumentation und umgekehrt.	119, 131, 132, 133
49.	**Umwandlung in ein Inhouse-Format (Grundsatz)** Bei Umwandlung (Konvertierung) aufbewahrungspflichtiger Unterlagen in ein unternehmenseigenes Format (sog. Inhouse-Format) sind ● beide Versionen zu archivieren, ● derselben Aufzeichnung zuzuordnen und ● mit demselben Index zu verwalten sowie ● die konvertierte Version als solche zu kennzeichnen.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob die Vorgaben zur Aufbewahrung des Ursprungsformates den Vorgaben der GoBD entsprechen ● Inaugenscheinnahme der Systemeinstellungen der IT-Anwendungen, die Formatumwandlungen vornehmen. **Wirksamkeit:** Nachvollzug von Dokumenten, Daten und Dateien, die im Rahmen der Verarbeitung bzw. Aufbewahrung oder Archivierung konvertiert wurden	135
50.	**Umwandlung in ein Inhouse-Format (Ersetzendes Konvertieren)** Die Aufbewahrung der konvertierten Fassung ist unter folgenden Voraussetzungen ausreichend: ● Es wird keine bildliche oder inhaltliche Veränderung vorgenommen.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, ob Vorgaben für das ersetzende Konvertieren bestehen	135, 122

Ergänzungselement (3): Elektronische Aufbewahrung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● Bei der Konvertierung gehen keine sonstigen aufbewahrungspflichtigen Informationen verloren. ● Die ordnungsgemäße und verlustfreie Konvertierung wird dokumentiert (Verfahrensdokumentation). ● Die maschinelle Auswertbarkeit und der Datenzugriff durch die Finanzverwaltung werden nicht eingeschränkt; dabei ist es zulässig, wenn bei der Konvertierung Zwischenaggregationsstufen nicht gespeichert, aber in der Verfahrensdokumentation so dargestellt werden, dass die retrograde und progressive Prüfbarkeit sichergestellt ist. Ein elektronisches Dokument ist mit einem nachvollziehbaren und eindeutigen Index zu versehen. ● Der Erhalt der Verknüpfung zwischen Index und elektronischem Dokument muss während der gesamten Aufbewahrungsfrist gewährleistet sein. ● Das elektronische Dokument muss unter dem zugeteilten Index verwaltet werden können.	● Einsichtnahme in Systemeinstellungen in den IT-Anwendungen, die die Umwandlung vornehmen ● Inaugenscheinnahme der Implementierung anhand eines Konvertierungsvorgangs. **Wirksamkeit:** ● Nachvollzug der Konvertierung von Dokumenten, Daten und Dateien, die im Rahmen der Verarbeitung bzw. Aufbewahrung oder Archivierung umgewandelt wurden.	
51.	**Kryptografietechniken** Bei Einsatz von Kryptografietechniken ist sicherzustellen, dass die verschlüsselten Unterlagen im DV-System in entschlüsselter Form zur Verfügung stehen. Werden Signaturprüfschlüssel verwendet, sind die eingesetzten Schlüssel aufzubewahren.	**Angemessenheit:** Einsichtnahme in die Verfahrensdokumentation zu den Vorgaben zur Verschlüsselung und Entschlüsselung von Dokumenten, Daten und Dateien sowie zur Aufbewahrung der verwendeten Schlüssel sowie dem jeweiligen Bezug zu den Dokumenten, Daten und Dateien, die damit verschlüsselt wurden. **Wirksamkeit:** ● Nachvollzug der Entschlüsselung anhand eines Dokuments ● Aufruf von verschlüsselten Dokumenten, Daten oder Dateien.	134

Ergänzungselement (3): Elektronische Aufbewahrung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
52.	**Aufbewahrung der Strukturinformationen** ● Aufbewahrung aller zur maschinellen Auswertung der Daten im Rahmen des Datenzugriffs notwendigen Strukturinformationen in maschinell auswertbarer Form. ● Aufbewahrung der internen und externen Verknüpfungen in unverdichteter, maschinell auswertbarer Form.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob es zur Aufbewahrung bzw. Archivierung der Strukturinformationen zu den Dokumenten, Daten und Dateien, die aufbewahrungspflichtig sind, Vorgaben gibt. ● Inaugenscheinnahme/Beobachtung der Aufbewahrung bzw. Archivierung der Strukturinformationen anhand einer Datensatzbeschreibung ● Interview mit dem Prozessverantwortlichen zur Aufbewahrung von Strukturinformationen. **Wirksamkeit:** ● Aufruf von Strukturinformationen zu aufzubewahrenden Dokumenten, Daten und Dateien ● Nachvollzug der Auswertbarkeit der Strukturinformationen anhand der Datensatzbeschreibung.	128
53.	**Maschinelle Auswertbarkeit** Maschinelle Auswertbarkeit ist bei aufzeichnungs- und aufbewahrungspflichtigen Daten, Datensätzen, elektronischen Dokumenten und elektronischen Unterlagen gegeben, die ● mathematisch-technische Auswertungen ermöglichen, ● eine Volltextsuche ermöglichen, ● auch ohne mathematisch-technische Auswertungen eine Prüfung im weitesten Sinne ermöglichen (z.B. Bildschirmabfragen, die Nachverfolgung von Verknüpfungen und Verlinkungen oder die Textsuche nach bestimmten Eingabekriterien) Die Reduzierung einer bereits bestehenden maschinellen Auswertbarkeit ist nicht zulässig.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Vorgaben für die Dokumentarten, Daten und Dateien, die Anforderungen an die maschinelle Auswertbarkeit festgelegt wurden ● Einsichtnahme in die IT-Systeme, die für die Aufbewahrung oder Archivierung genutzt werden, ob die Einstellungen die maschinelle Auswertbarkeit ermöglichen (z.B. Reports). **Wirksamkeit:** Nachvollzug der maschinellen Auswertbarkeit durch Aufruf und Auswerten von Dokumenten, Daten und Dateien.	126, 128, 129

Ergänzungselement (3): Elektronische Aufbewahrung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
54.	**Datenauslagerung** Im Falle einer Auslagerung von aufzeichnungs- und aufbewahrungspflichtigen Daten aus dem Produktivsystem ist es nur dann nicht erforderlich, die ursprüngliche Hard- und Software des Produktivsystems über die Dauer der Aufbewahrungsfrist vorzuhalten, wenn das Archivsystem oder das andere System in quantitativer und qualitativer Hinsicht die gleichen Auswertungen der aufzeichnungs- und aufbewahrungspflichtigen Daten so ermöglicht, als wären die Daten noch im Produktivsystem.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation zur Durchführung der Auslagerung für steuerlich relevante Datenbestände ● Inaugenscheinnahme der qualitativ und quantitativ gleichen Auswertungsmöglichkeiten nach einer Datenauslagerung anhand der getroffenen Festlegungen durch das Unternehmen ● Inaugenscheinnahme der Zurverfügungstellung qualitativ und quantitativ gleicher Auswertungsmöglichkeiten nach einem vollzogenen Systemwechsel anhand der getroffenen Festlegungen durch das Unternehmen. **Wirksamkeit:** Soweit eine Datenauslagerung stattgefunden hat: ● Nachvollzug der Zurverfügungstellung qualitativ und quantitativ gleicher Auswertungsmöglichkeiten nach einer Datenauslagerung ● Nachvollzug der Zurverfügungstellung qualitativ und quantitativ gleicher Auswertungsmöglichkeiten nach einem vollzogenen Systemwechsel.	142

Ergänzungselement (4): Datenzugriff der Finanzverwaltung

Sind die nach § 147 Abs. 1 AO aufbewahrungspflichtigen Unterlagen mit Hilfe eines Datenverarbeitungssystems erstellt worden, hat die Finanzverwaltung im Rahmen einer steuerlichen Außenprüfung bzw. Umsatzsteuer-Nachschau das Recht, Einsicht in die gespeicherten Daten zu nehmen und das DV-System zur Prüfung dieser Unterlagen zu nutzen. Die steuerliche Außenprüfung kann auch verlangen, dass die Daten nach ihren Vorgaben maschinell ausgewertet oder ihr gespeicherte Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden. Die Entscheidung, von welcher Möglichkeit des

Datenzugriffs die Finanzverwaltung Gebrauch macht, steht in ihrem pflichtgemäßen Ermessen.

Sofern im Prüfungszeitraum Veränderungen am DV-System durchgeführt werden bzw. erfolgen sollen (bspw. ein Systemwechsel (vgl. GoBD, Rn. 142)), bietet sich die Durchführung einer gesonderten projektbegleitenden Prüfung gemäß *IDW PS 850 n.F.*[9] an. Vor diesem Hintergrund umfassen die im Folgenden dargestellten beispielhaften Prüfungshandlungen für die Beurteilung der qualitativen und quantitativen gleichwertigen Auswertungsmöglichkeiten nach einem vollzogenen Systemwechsel (Nr. 6 Datenauslagerung) keine Beurteilung des Systemwechsels selbst.[10]

Ergänzungselement (4): Datenzugriff der Finanzverwaltung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
55.	**Aufzeichnungspflichtige und aufbewahrungspflichtige Unterlagen/Erstqualifikation** ● Gegenstand der Prüfung sind die nach außersteuerlichen und steuerlichen Vorschriften aufzeichnungspflichtigen und die nach § 147 Absatz 1 AO aufbewahrungspflichtigen Unterlagen ● Hierfür sind bspw. die Daten der Finanzbuchhaltung, der Anlagenbuchhaltung, der Lohnbuchhaltung und aller Vor- und Nebensysteme, die aufzeichnungs- und aufbewahrungspflichtige Unterlagen enthalten, für den Datenzugriff bereitzustellen. ● Die für den Datenzugriff betroffenen DV-Systeme sind zu identifizieren. ● Die darin enthaltenen Daten sind zu qualifizieren (Erstqualifizierung) und für den Datenzugriff in geeigneter Weise vorzuhalten. ● Bei unzutreffender Qualifizierung steht der Finanzverwaltung das Recht auf Zweitqualifikation zu.	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob es zur Ausübung des Erstqualifizierungsrechts und damit den Vorgaben für die Klassifizierung nach außersteuerlichen und steuerlichen Vorschriften aufzeichnungspflichtiger Geschäftsvorfälle und der nach § 147 Abs. 1 AO aufbewahrungspflichtigen Unterlagen Regelungen gibt. ● Beobachtung der Vorgehensweise bei der Identifikation aufzeichnungspflichtiger und aufbewahrungspflichtiger Unterlagen (Erstqualifikation) anhand der getroffenen Festlegungen des Unternehmens. **Wirksamkeit:** ● Nachvollzug der Einstufung der DV-Systeme als steuerrelevant anhand der vorgelegten Daten ● Retrograder und progressiver Nachvollzug aufzeichnungspflichtiger Geschäftsvorfälle und deren Belege.	159, 161

[9] Liegt derzeit vor als Entwurf einer Neufassung des *IDW Prüfungsstandards: Projektbegleitende Prüfung bei Einsatz von Informationstechnologie (IDW EPS 850 n.F.)* (Stand: 26.03.2021).

[10] Vgl. *IDW PS 850 n.F.*, Tz. 27 ff.

Ergänzungselement (4): Datenzugriff der Finanzverwaltung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
56.	**Zugriffsmöglichkeit (Grundsatz)** ● Bei der Ausübung des Rechts auf Datenzugriff stehen der Finanzverwaltung nach dem Gesetz drei gleichberechtigte Möglichkeiten zur Verfügung, auch kumulativ. ● Die Entscheidung, von welcher Möglichkeit des Datenzugriffs die Finanzverwaltung Gebrauch macht, steht in ihrem pflichtgemäßen Ermessen. ● Die Finanzverwaltung hat bei Anwendung der Regelungen zum Datenzugriff den Grundsatz der Verhältnismäßigkeit zu beachten.	**Angemessenheit:** Einsichtnahme in die Verfahrensdokumentation, um festzustellen, wie der Finanzverwaltung der Zugriff auf die GoBD-relevanten IT-Systeme, Dokumente und Dateien ermöglicht wird (bzw. wie die drei Zugriffsarten umgesetzt sind). **Wirksamkeit:** Nachvollzug vorhandener Anfragen der Finanzverwaltung und deren Beantwortung durch das Unternehmen in der Vergangenheit.	163, 164, 170
Unmittelbarer Zugriff (Z1-Zugriff)			
57.	**Unmittelbarer Datenzugriff (Z1)** ● Unmittelbarer Zugriff auf das DV-System ● Nutzung der eingesetzten Hard- und Software zur Prüfung der gespeicherten Daten einschließlich der jeweiligen Meta-, Stamm- und Bewegungsdaten sowie der entsprechenden Verknüpfungen ● Nur-Lesezugriff, welcher das Lesen und Analysieren der Daten unter Nutzung der im DV-System vorhandenen Auswertungsmöglichkeiten (z.B. Filtern und Sortieren) nutzt ● Zurverfügungstellung der für den Datenzugriff erforderlichen Hilfsmittel ● Einweisung des Prüfers in das DV-System	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob Maßnahmen (anhand der getroffenen Festlegungen des Unternehmens) existieren zur Sicherstellung der Verfügbarkeit der in den GoBD-relevanten DV-Systemen vorhandenen Auswertungsmöglichkeiten für die Finanzverwaltung ● Einsichtnahme in das Berechtigungskonzept, um festzustellen, ob es Regelungen für die Zugriffe durch den Betriebsprüfer anhand der getroffenen Festlegungen des Unternehmens gibt ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, wie neben der Erstqualifizierung bzw. der Zugriffsmöglichkeit auf GoBD-relevante Daten sichergestellt wird, dass die notwendigen Einschränkungen der Zugriffsrechte der Finanzverwaltung auf den Nur-Lese-Zugriff auf steuerrelevante Informationen (z.B. durch das Berechti-	151, 174

Ergänzungselement (4): Datenzugriff der Finanzverwaltung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● Zugangsberechtigung umfasst die im DV-System genutzten Auswertungsmöglichkeiten (z.B. Filtern, Sortieren, Konsolidieren) für Prüfungszwecke, (z.B. in Revisionstools, Standardsoftware, Backoffice-Produkte) ● Gewährleistung der Unveränderbarkeit des Datenbestandes und des DV-Systems durch die Finanzverwaltung.	gungsmanagement, Anonymisierung/Pseudonymisierung u.a.m.) erfolgt. **Wirksamkeit:** ● Abgleich der in der Prüferumgebung des DV-Systems bestehenden Zugriffsrechte auf IT-Anwendungen mit der Auflistung steuerrelevanter IT-Systeme in der steuerlichen Verfahrensdokumentation und umgekehrt ● Nachvollzug des Umfangs bestehender Zugriffsrechte sowie des Nur-Lese-Zugriffs der für die Finanzverwaltung eingerichteten Benutzer auf der Ebene der steuerrelevanten IT-Anwendungen.	
Mittelbarer Zugriff (Z2-Zugriff)			
58.	**Mittelbarer Datenzugriff (Z2)** ● Mittelbarer Zugriff auf das DV-System über den Steuerpflichtigen oder einen beauftragten Dritten ● Zurverfügungstellung von Hard- und Software ● Unterstützung durch mit dem DV-System vertraute Personen.	**Angemessenheit:** Einsichtnahme in die Verfahrensdokumentation, um festzustellen, wie bei der Inanspruchnahme des mittelbaren Zugriffsrechts durch die Finanzverwaltung vorgegangen wird. **Wirksamkeit:** ● Nachvollzug der Unterstützung in den Außenprüfungen in der Vergangenheit ● Abgleich der für den mittelbaren Zugriff erforderlichen Zugriffsrechte auf IT-Anwendungen mit der Auflistung steuerrelevanter IT-Systeme in der steuerlichen Verfahrensdokumentation und umgekehrt.	154, 175
Datenträgerüberlassung (Z3-Zugriff)			
59.	**Datenträgerüberlassung (Z3)** Überlassung ● der aufzeichnungs- und aufbewahrungspflichtigen Daten,	**Angemessenheit:** ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob es Regelungen zur Vorgehensweise bei der Inanspruchnahme	167, 168, 169, 176, 177, 178

Ergänzungselement (4): Datenzugriff der Finanzverwaltung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● einschließlich der jeweiligen Meta-, Stamm- und Bewegungsdaten sowie ● der internen und externen Verknüpfungen (z.B. zwischen den Tabellen einer relationalen Datenbank) und ● elektronischen Dokumente und Unterlagen auf einem maschinell lesbaren und auswertbaren Datenträger zur Auswertung.	des Rechts auf Datenträgerüberlassung durch die Finanzverwaltung gibt. ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, ob in der Auflistung aller zur Auswertung der Daten notwendigen Informationen (z.B. über die Dateiherkunft, eingesetztes System, die Dateistruktur, die Datenfelder, verwendete Zeichensatztabellen sowie interne und externe Verknüpfungen) in maschinell auswertbarer Form dargestellt werden. ● Einsichtnahme in die Verfahrensdokumentation, um festzustellen, welche Möglichkeiten bestehen, die vom Prüfer geforderten Datenbestände im Prüfungsfall auf einen Datenträger auszugeben ● Inaugenscheinnahme der Auflistung aller zur Auswertung der Daten notwendigen Informationen (z.B. über die Dateiherkunft, eingesetztes System, die Dateistruktur, die Datenfelder, verwendete Zeichensatztabellen sowie interne und externe Verknüpfungen) in maschinell auswertbarer Form. **Wirksamkeit:** ● Nachvollzug des Datenexports und des anschließenden Datenimports in ein Analysesystem ● Nachvollzug der bereitgestellten Datenformate auf Konformität zu Vorgaben der Finanzverwaltung ● Nachvollzug, ob alle zur Auswertung der Dokumente und Daten notwendigen Strukturinformationen in maschinell auswertbarer Form zur Verfügung gestellt werden können ● Nachvollzug der Kontrolle zur Richtigkeit der zu überlassenden Daten	

Ergänzungselement (4): Datenzugriff der Finanzverwaltung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
		(insb. Identität der durch die Finanzverwaltung angeforderten Daten mit den zur Überlassung vorgesehenen Daten) ● Nachvollzug der Bereitstellung entschlüsselter Daten für die Finanzverwaltung.	
Datenauslagerung			
60.	**Datenauslagerung** Im Falle einer Auslagerung von aufzeichnungs- und aufbewahrungspflichtigen Daten aus dem Produktivsystem ist es nur dann nicht erforderlich, die ursprüngliche Hard- und Software des Produktivsystems über die Dauer der Aufbewahrungsfrist vorzuhalten, wenn insb. die folgenden Voraussetzungen erfüllt sind: ● Die aufzeichnungs- und aufbewahrungspflichtigen Daten müssen quantitativ und qualitativ gleichwertig in ein neues System, in eine neue Datenbank, in ein Archivsystem oder in ein anderes System überführt werden. ● Bei einer erforderlichen Datenumwandlung (Migration) darf ausschließlich das Format der Daten (z.B. Datums- und Währungsformat) umgesetzt, nicht aber eine inhaltliche Änderung der Daten vorgenommen werden. ● Die vorgenommenen Änderungen sind zu dokumentieren. ● Das neue System, das Archivsystem oder das andere System muss in quantitativer und qualitativer Hinsicht die gleichen Auswertungen der aufzeichnungs- und aufbewahrungspflichtigen Daten ermöglichen, als wären die Daten noch im Produktivsystem.	**Angemessenheit:** Einsichtnahme in das Konzept / die Dokumentation, um festzustellen, ob Regelungen zur Durchführung der Auslagerung GoBD-relevanter Datenbestände existieren und implementiert wurden. **Wirksamkeit:** Soweit eine Datenauslagerung stattgefunden hat: ● Nachvollzug der Zurverfügungstellung qualitativ und quantitativ gleicher Auswertungsmöglichkeiten nach einer Datenauslagerung.	142, 164

Ergänzungselement (4): Datenzugriff der Finanzverwaltung			
Nr.	**Zusammenfassung der GoBD-Vorgaben**	**Beispielhafte Prüfungshandlungen**	**GoBD-Referenz (Rn #)**
	● Sofern noch nicht mit der Außenprüfung begonnen wurde, ist es im Falle eines Systemwechsels oder einer Auslagerung von aufzeichnungs- und aufbewahrungspflichtigen Daten aus dem Produktivsystem ausreichend, wenn nach Ablauf des 5. Kalenderjahres, das auf die Umstellung folgt, nur noch der Z3-Zugriff zur Verfügung gestellt wird.		

Die nachfolgenden Anlagen enthalten Beispiele für die Formulierung von Prüfungsvermerken bzw. Prüfungsberichten. Die zusätzlichen Bestandteile eines Prüfungsberichts gegenüber einem Prüfungsvermerk sind jeweils wie folgt kenntlich gemacht: [*kursiv*]

Anlage 2: Auftragsart „Prüfung einer Erklärung der gesetzlichen Vertreter zur GoBD-Compliance“ – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Wirksamkeitsprüfung

PRÜFUNGSVERMERK/-BERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS ÜBER DIE PRÜFUNG EINER ERKLÄRUNG DER GESETZLICHEN VERTRETER ZUR GOBD-COMPLIANCE

An die … [Gesellschaft]

Wir haben die in der Anlage 1 beigefügte Erklärung der gesetzlichen Vertreter (im Folgenden „GoBD-Erklärung“) zur Beschreibung der für die Geschäftsprozesse … [Beschreibung der Ergänzungselemente] relevanten Maßnahmen des IT-Systems der … [Name] (im Folgenden des „Unternehmens“) sowie die Angemessenheit und Wirksamkeit dieser Maßnahmen für den Zeitraum vom … [Datum] bis … [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen des IT-Systems sind angemessen, wenn sie die Risiken der Nichteinhaltung der in Anlage 1 des *IDW PH 9.860.4 (07.2021)* dargestellten GoBD-Anforderungen mit hinreichender Sicherheit begegnen. Diese Maßnahmen sind wirksam, wenn sie im geprüften Zeitraum wie vorgesehen durchgeführt wurden.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter sind für die Aufstellung der GoBD-Erklärung verantwortlich. Dies schließt die Verantwortung für die internen Kontrollen ein, die sie als notwendig erachten, um eine GoBD-Erklärung aufzustellen, die frei von wesentlichen – beabsichtigten und unbeabsichtigten – Fehlern ist. Des Weiteren sind die gesetzlichen Vertreter für die Geschäftsprozesse … [Beschreibung der Ergänzungselemente] relevanten Maßnahmen des IT-Systems sowie deren Angemessenheit (d.h. dass die Maßnahmen den Risiken der Nichteinhaltung der in Anlage 1 des *IDW PH 9.860.4 (07.2021)* dargestellten GoBD-Anforderungen mit hinreichender Sicherheit begegnen) und Wirksamkeit dieser Maßnahmen verantwortlich.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen nur mit hinreichender statt absoluter Sicherheit den Risiken der Nichteinhaltung der GoBD-Anforderungen begegnen.

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die GoBD-Erklärung frei von wesentlichen Fehlern ist. Dieses Urteil erstreckt sich auch darauf, ob die in der Beschreibung enthaltenen relevanten Maßnahmen des IT-Systems in allen wesentlichen Belangen

- angemessen waren und
- im geprüften Zeitraum wirksam waren.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in*

der Wirtschaftsprüferpraxis (IDW QS 1) angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Die Prüfung der Einhaltung der Grundsätze der ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD-Compliance) (IDW PH 9.860.4 (07.2021))* durchgeführt. Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit das vorgenannte Urteil abgeben können. Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.4 (07.2021)* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung von Risiken wesentlicher – beabsichtigter oder unbeabsichtigter – Fehler in der GoBD-Erklärung der gesetzlichen Vertreter ein. Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der GoBD-Erklärung eingerichteten internen Kontrollen einschließlich der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens. Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der GoBD-Erklärung der gesetzlichen Vertreter relevante interne Kontrollsystem abzugeben.

Für die Prüfung der Angemessenheit und Wirksamkeit der relevanten Maßnahmen des IT-Systems ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Angemessenheit und Wirksamkeit der Maßnahmen mit hinreichender Sicherheit aufgedeckt werden.

[In einen Prüfungsbericht ist der folgende Abschnitt aufzunehmen: Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

*[Feststellungen zu nicht wesentlichen Mängeln in der Angemessenheit oder Wirksamkeit der umgesetzten Maßnahmen]**]***

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- ist die GoBD-Erklärung der gesetzlichen Vertreter in allen wesentlichen Belangen frei von Fehlern,
- waren die in der GoBD-Erklärung der gesetzlichen Vertreter beschriebenen und vom Unternehmen umgesetzten Maßnahmen in allen wesentlichen Belangen
  - angemessen und
  - im geprüften Zeitraum wirksam.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- ist die GoBD-Erklärung der gesetzlichen Vertreter in allen wesentlichen Belangen frei von Fehlern,
- waren die in der GoBD-Erklärung der gesetzlichen Vertreter beschriebenen und vom Unternehmen umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - angemessen und
  - im geprüften Zeitraum wirksam.]

[Gegebenenfalls Hinweis auf sonstige Sachverhalte

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften IT-Systems

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen nur mit hinreichender statt absoluter Sicherheit die Risiken der Nichteinhaltung der GoBD-Anforderung begegnen.

Die GoBD-Erklärung der gesetzlichen Vertreter wurde zum … [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit dieser Maßnahmen erstrecken sich auf den Zeitraum vom … [Datum] bis … [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Maßnahmen falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungs- und Weitergabebeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ für die umzusetzenden Maßnahmen, die für Zwecke der … [Nennung des Zwecks] konzipiert wurden. Folglich ist die GoBD-Erklärung der gesetzlichen Vertreter für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an das Unternehmen gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden und darf nicht ohne unsere Zustimmung an Dritte mit Ausnahme der Finanzverwaltung weitergegeben werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

[Ort]

[Datum]

[Unterschrift]

Anlagen:

GoBD-Erklärung der gesetzlichen Vertreter (Anlage 1)

Darstellung der durchgeführten Prüfungshandlungen und geprüften Grundsätze, Verfahren und Maßnahmen (Anlage 2)

Allgemeine Auftragsbedingungen

Anlage 3: Auftragsart „Prüfung einer Erklärung der gesetzlichen Vertreter zur GoBD-Compliance“ – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Angemessenheitsprüfung

PRÜFUNGSVERMERK/-BERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS ÜBER DIE PRÜFUNG EINER ERKLÄRUNG DER GESETZLICHEN VERTRETER ZUR GOBD-COMPLIANCE

An die … [Gesellschaft]

Wir haben die in der Anlage 1 beigefügte Erklärung der gesetzlichen Vertreter (im Folgenden „GoBD-Erklärung“) zur Beschreibung der für die Geschäftsprozesse … [Beschreibung der Ergänzungselemente] relevanten Maßnahmen des IT-Systems der … [Name] (im Folgenden des „Unternehmens“) sowie die Angemessenheit dieser Maßnahmen für den Zeitraum vom … [Datum] bis … [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen des IT-Systems sind angemessen, wenn sie den Risiken der Nichteinhaltung der in Anlage 1 des *IDW PH 9.860.4 (07.2021)* dargestellten GoBD-Anforderungen mit hinreichender Sicherheit begegnen.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter sind für die Aufstellung der GoBD-Erklärung verantwortlich. Dies schließt die Verantwortung für die internen Kontrollen ein, die sie als notwendig erachten, um eine GoBD-Erklärung aufzustellen, die frei von wesentlichen – beabsichtigten und unbeabsichtigten – Fehlern ist. Des Weiteren sind die gesetzlichen Vertreter für die Geschäftsprozesse … [Beschreibung der Ergänzungselemente] relevanten Maßnahmen des IT-Systems sowie deren Angemessenheit (d.h. dass die Maßnahmen den Risiken der Nichteinhaltung der in Anlage 1 des … [*IDW PH 9.860.4 (07.2021)*] dargestellten GoBD-Anforderungen mit hinreichender Sicherheit begegnen) verantwortlich.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen nur mit hinreichender statt absoluter Sicherheit den Risiken der Nichteinhaltung der GoBD-Anforderungen begegnen.

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die GoBD-Erklärung frei von wesentlichen Fehlern ist. Dieses Urteil erstreckt sich auch darauf, ob die in der Beschreibung enthaltenen relevanten Maßnahmen des IT-Systems in allen wesentlichen Belangen

- angemessen waren und
- im geprüften Zeitraum implementiert waren.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und

der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Die Prüfung der Einhaltung der Grundsätze der ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD-Compliance) (IDW PH 9.860.4 (07.2021))* durchgeführt. Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit das vorgenannte Urteil abgeben können. Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.4 (07.2021)* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung von Risiken wesentlicher – beabsichtigter oder unbeabsichtigter – Fehler in der GoBD-Erklärung der gesetzlichen Vertreter ein. Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der GoBD-Erklärung eingerichteten internen Kontrollen einschließlich der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens. Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der GoBD-Erklärung der gesetzlichen Vertreter relevante interne Kontrollsystem abzugeben.

Für die Prüfung der Angemessenheit und Wirksamkeit der relevanten Maßnahmen des IT-Systems ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Angemessenheit der Maßnahmen mit hinreichender Sicherheit aufgedeckt werden.

[In einen Prüfungsbericht ist der folgende Abschnitt aufzunehmen: Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

*[Feststellungen zu nicht wesentlichen Mängeln in der Angemessenheit oder Wirksamkeit der umgesetzten Maßnahmen]**]***

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- ist die GoBD-Erklärung der gesetzlichen Vertreter in allen wesentlichen Belangen frei von Fehlern,
- waren die in der GoBD-Erklärung der gesetzlichen Vertreter beschriebenen und vom Unternehmen umgesetzten Maßnahmen in allen wesentlichen Belangen
  - angemessen und
  - im geprüften Zeitraum implementiert.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- ist die GoBD-Erklärung der gesetzlichen Vertreter in allen wesentlichen Belangen frei von Fehlern,
- waren die in der GoBD-Erklärung der gesetzlichen Vertreter beschriebenen und vom Unternehmen umzusetzenden Maßnahmen in allen wesentlichen Belangen
  - angemessen und
  - im geprüften Zeitraum implementiert.]

[Gegebenenfalls Hinweis auf sonstige Sachverhalte

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften IT-Systems

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen nur mit hinreichender statt absoluter Sicherheit die Risiken der Nichteinhaltung der GoBD-Anforderung begegnen.

Die GoBD-Erklärung der gesetzlichen Vertreter wurde zum … [Datum] erstellt. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Maßnahmen falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungs- und Weitergabebeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ für die umzusetzenden Maßnahmen, die für Zwecke der … [Nennung des

Zwecks] konzipiert wurden. Folglich ist die GoBD-Erklärung der gesetzlichen Vertreter für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an das Unternehmen gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden und darf nicht ohne unsere Zustimmung an Dritte mit Ausnahme der Finanzverwaltung weitergegeben werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

[Ort]

[Datum]

[Unterschrift]

Anlagen:

GoBD-Erklärung der gesetzlichen Vertreter (Anlage 1)

Darstellung der durchgeführten Prüfungshandlungen und geprüften Grundsätze, Verfahren und Maßnahmen (Anlage 2)

Allgemeine Auftragsbedingungen

Anlage 4: Auftragsart „Direkte Prüfung der GoBD-Compliance“ – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Wirksamkeitsprüfung

PRÜFUNGSVERMERK/-BERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS ÜBER DIE PRÜFUNG DER MAßNAHMEN ZUR GOBD-COMPLIANCE

An die … [Gesellschaft]

Wir haben die Angemessenheit und Wirksamkeit der für die Geschäftsprozesse … [Beschreibung der Ergänzungselemente] relevanten Maßnahmen des IT-Systems der … [Name] (im Folgenden des „Unternehmens“) für den Zeitraum vom … [Datum] bis … [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen des IT-Systems sind angemessen, wenn sie die Risiken der Nichteinhaltung der in Anlage 1 des *IDW PH 9.860.4 (07.2021)* dargestellten GoBD-Anforderungen mit hinreichender Sicherheit begegnen. Diese Maßnahmen sind wirksam, wenn sie im geprüften Zeitraum wie vorgesehen durchgeführt wurden.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter sind für die Geschäftsprozesse … [Beschreibung der Ergänzungselemente] relevanten Maßnahmen des IT-Systems sowie deren Angemessenheit (d.h. dass die Maßnahmen den Risiken der Nichteinhaltung der in Anlage 1 des *IDW PH 9.860.4 (07.2021)* dargestellten GoBD-Anforderungen mit hinreichender Sicherheit begegnen) und Wirksamkeit dieser Maßnahmen verantwortlich.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen nur mit hinreichender statt absoluter Sicherheit den Risiken der Nichteinhaltung der GoBD-Anforderungen begegnen.

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die relevanten Maßnahmen des IT-Systems in allen wesentlichen Belangen

- angemessen waren und
- im geprüften Zeitraum wirksam waren.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Wir haben unsere Prüfung unter Beachtung des *IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Die Prüfung der Einhaltung der Grundsätze der ordnungsmäßigen Führung und Aufbewahrung von Büchern,*

Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD-Compliance) (IDW PH 9.860.4 (07.2021)) durchgeführt. Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit das vorgenannte Urteil abgeben können. Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.4 (07.2021)* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

Für die Prüfung der Angemessenheit und Wirksamkeit der relevanten Maßnahmen des IT-Systems ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Angemessenheit und Wirksamkeit der Maßnahmen mit hinreichender Sicherheit aufgedeckt werden.

[In einen Prüfungsbericht ist der folgende Abschnitt aufzunehmen: Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

*[Feststellungen zu nicht wesentlichen Mängeln in der Angemessenheit oder Wirksamkeit der umgesetzten Maßnahmen]**]***

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- waren die relevanten Maßnahmen in allen wesentlichen Belangen
  - angemessen und
  - im geprüften Zeitraum wirksam.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- waren die relevanten Maßnahmen in allen wesentlichen Belangen

- angemessen und
- im geprüften Zeitraum wirksam.]

[Gegebenenfalls Hinweis auf sonstige Sachverhalte

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften IT-Systems

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen nur mit hinreichender statt absoluter Sicherheit den Risiken der Nichteinhaltung der GoBD-Anforderungen begegnen.

Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit dieser Maßnahmen erstrecken sich auf den Zeitraum vom … [Datum] bis … [Datum]. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Maßnahmen falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungs- und Weitergabebeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ für die relevanten Maßnahmen, die für Zwecke der … [Nennung des Zwecks] konzipiert wurden. Folglich ist der Prüfungsvermerk/Prüfungsbericht für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an das Unternehmen gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden und darf nicht ohne unsere Zustimmung an Dritte mit Ausnahme der Finanzverwaltung weitergegeben werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

[Ort]

[Datum]

[Unterschrift]

Anlagen:

Darstellung der durchgeführten Prüfungshandlungen und geprüften Maßnahmen (Anlage 1)

Allgemeine Auftragsbedingungen

Anlage 5: Auftragsart „Direkte Prüfung der GoBD-Compliance“ – Formulierungsbeispiel für den Prüfungsvermerk/Prüfungsbericht über die Angemessenheitsprüfung

PRÜFUNGSVERMERK/-BERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS ÜBER DIE PRÜFUNG DER MAßNAHMEN ZUR GOBD-COMPLIANCE

An die … [Gesellschaft]

Wir haben die Angemessenheit der für die Geschäftsprozesse … [Beschreibung der Ergänzungselemente] relevanten Maßnahmen des IT-Systems der … [Name] (im Folgenden des „Unternehmens“) für den Zeitraum vom … [Datum] bis … [Datum] mit hinreichender Sicherheit geprüft. Die Maßnahmen des IT-Systems sind angemessen, wenn sie die Risiken der Nichteinhaltung der in Anlage 1 *IDW PH 9.860.4 (07.2021)* dargestellten GoBD-Anforderungen mit hinreichender Sicherheit begegnen.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter sind für die Geschäftsprozesse … [Beschreibung der Ergänzungselemente] relevanten Maßnahmen des IT-Systems sowie deren Angemessenheit (d.h. dass die Maßnahmen die Risiken der Nichteinhaltung der in Anlage 1 des *IDW PH 9.860.4 (07.2021)* dargestellten GoBD-Anforderungen mit hinreichender Sicherheit begegnen) dieser Maßnahmen verantwortlich.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen nur mit hinreichender statt absoluter Sicherheit die Risiken der Nichteinhaltung der GoBD-Anforderungen begegnen.

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die relevanten Maßnahmen des IT-Systems in allen wesentlichen Belangen

- angemessen waren und
- im geprüften Zeitraum implementiert waren.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Wir haben unsere Prüfung unter Beachtung *des IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises: Die Prüfung der Einhaltung der Grundsätze der ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD-Compliance) (IDW PH 9.860.4 (07.2021))* durchgeführt. Nach diesen Anforderungen haben wir die

Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit das vorgenannte Urteil abgeben können. Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.4 (07.2021)* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

Für die Prüfung der Angemessenheit der relevanten Maßnahmen des IT-Systems ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Angemessenheit und Wirksamkeit der Maßnahmen mit hinreichender Sicherheit aufgedeckt werden.

[In einen Prüfungsbericht ist der folgende Abschnitt aufzunehmen: Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt: [zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen]

Im Rahmen unserer Prüfung haben wir die nachfolgend aufgeführten Feststellungen getroffen, die wir bei der Bildung unseres Urteils berücksichtigt haben; wir geben zu den in diesen Feststellungen dargestellten Sachverhalten keine gesonderten Prüfungsurteile ab.

*[Feststellungen zu nicht wesentlichen Mängel in der Angemessenheit der umgesetzten Maßnahmen]**]***

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- waren die relevanten Maßnahmen in allen wesentlichen Belangen
  - angemessen und
  - im geprüften Zeitraum implementiert.

[Prüfungsurteil mit Einschränkung

Beschreibung der Gründe für die Einschränkung

Nach unserer Beurteilung, mit Ausnahme der Auswirkungen der o.g. Gründe,

- waren die relevanten Maßnahmen in allen wesentlichen Belangen
  - angemessen und
  - im geprüften Zeitraum implementiert.]

[Gegebenenfalls Hinweis auf sonstige Sachverhalte

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Prüfungsvermerks/des Prüfungsberichts erforderlich ist].**]**

Inhärente Grenzen des geprüften IT-Systems

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen nur mit hinreichender statt absoluter Sicherheit die Risiken der Nichteinhaltung der GoBD-Anforderung begegnen.

Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Maßnahmen falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungs- und Weitergabebeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ für die relevanten Maßnahmen, die für Zwecke der [Nennung des Zwecks] konzipiert wurden. Folglich ist der Prüfungsvermerk/Prüfungsbericht für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsvermerk/Prüfungsbericht an das Unternehmen gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden und darf nicht ohne unsere Zustimmung an Dritte mit Ausnahme der Finanzverwaltung weitergegeben werden.

Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk/Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsvermerk/Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 zugrunde liegen.

[Ort]

[Datum]

[Unterschrift]

Anlagen:

Darstellung der durchgeführten Prüfungshandlungen und geprüften Maßnahmen (Anlage 1)

Allgemeine Auftragsbedingungen