Entwurf eines IDW Prüfungsstandards: Aufsichtliche Prüfung der Einhaltung von Anforderungen der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz (Digital Operational Resilience Act, DORA) im Finanzsektor im Rahmen der Abschlussprüfung (Aufsichtliche DORA-Prüfung im Rahmen der Abschlussprüfung) (IDW EPS 528 (08.2025))

Stand: 07.08.2025[1]

Der Bankenfachausschuss (BFA), der Versicherungsfachausschuss (VFA) sowie der Fachausschuss Investment (FAIN) haben den nachfolgenden Entwurf eines IDW Prüfungsstandards: Aufsichtliche Prüfung der Einhaltung von Anforderungen der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, DORA) im Finanzsektor im Rahmen der Abschlussprüfung (Aufsichtliche DORA-Prüfung im Rahmen der Abschlussprüfung) (IDW EPS 528 (08.2025)) verabschiedet.

Nach dem Finanzmarktdigitalisierungsgesetz (FinmadiG) prüft der Abschlussprüfer bei Finanzunternehmen (Institute (§ 29 Abs. 1 Satz 2 Nr. 2 Buchst. m KWG, § 24 Abs. 1 Satz 3 Nr. 5 ZAG, § 40 Abs. 1 Satz 3 Nr. 5 KMAG und § 78 Abs. 1 Satz 3 Nr. 5 Buchst. h WpIG), Versicherungsunternehmen (§ 35 Abs. 1 Satz 1 Nr. 10 VAG) sowie externe Kapitalverwaltungsgesellschaften und bestimmte Investmentvermögen (§ 38 Abs. 3 Satz 2 Nr. 9 KAGB, § 121 Abs. 3 Satz 1 Nr. 2 Buchst. h und § 136 Abs. 3 Satz 2 Nr. 8 KAGB)) die Einhaltung von aufsichtlichen Anforderungen an die digitale operationale Resilienz im Finanzsektor nach der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, DORA) und berichtet hierüber im Prüfungsbericht. Bei der Umsetzung der DORA-Anforderungen ist gemäß Artikel 4 DORA der Grundsatz der Verhältnismäßigkeit (Proportionality principle) zu beachten. Der vorliegende Entwurf eines IDW Prüfungsstandards stellt die Berufsauffassung dar, nach welchen Grundsätzen Abschlussprüfer unbeschadet ihrer Eigenverantwortlichkeit den vorstehenden Pflichten nachkommen. Insoweit legt er die besondere Vorgehensweise bei der Erfüllung der mit dem FinmadiG eingeführten vorstehenden Pflichten des Abschlussprüfers für die Aufsichtliche DORA-Prüfung dar und verdeutlicht die Relevanz entsprechender Tätigkeiten von Abschlussprüfern, insb. für die Aufsicht sowie die gesetzlichen Vertreter und das Aufsichtsorgan des Finanzunternehmens.

Der Standardentwurf berücksichtigt bereits – ausgehend von dem von der BaFin am 06.12.2024 zur Konsultation gestellten Entwurf einer Verordnung zur Änderung der Wertpapierinstituts-Prüfungsberichtsverordnung (WpIPrüfbV)[2] – erwartete Änderungen der aufsichtlichen Vorgaben an den Abschlussprüfer durch die von der BaFin angekündigte Novelle ande-

---

1 Verabschiedet vom Bankenfachausschuss (BFA), vom Versicherungsfachausschuss (VFA) sowie vom Fachausschuss Investment (FAIN) am 21.07.2025. Billigende Kenntnisnahme durch den Hauptfachausschuss (HFA) am 07.08.2025.

2 https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Konsultation/2024/kon_11_24_Konsultation_WpIPruefbV_SchwarmfdPV.html (letzter Abruf: 27.07.2025).

rer Prüfungsberichtsverordnungen für andere Finanzunternehmen. Die Auswirkungen von erwarteten Änderungen der Prüfungsberichtsverordnungen auf die Pflichten des Abschlussprüfers nach den vorgenannten Prüfungspflichten des KWG, KMAG, ZAG, WpIG, VAG sowie KAGB sind zur Abgrenzung von der derzeitigen Pflichtenlage unterstrichen.

Änderungs- oder Ergänzungsvorschläge zu dem Entwurf werden schriftlich an die Geschäftsstelle des IDW (Postfach 32 05 80, 40420 Düsseldorf oder stellungnahmen@idw.de) bis zum 31.10.2025 erbeten. Die Änderungs- oder Ergänzungsvorschläge werden im Internet auf der IDW Website veröffentlicht, wenn dies nicht ausdrücklich vom Verfasser abgelehnt wird.

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

1. Vorbemerkungen

1.1. Anwendungsbereich und Zielsetzung

1 Mit der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, DORA)[3] hat die Europäische Union eine finanzsektorübergreifende europäische Regulierung für die Themen digitale operationale Resilienz, IKT-Risiken und Cybersicherheit geschaffen. Die Verordnung ist am 16.01.2023 in Kraft getreten und findet ab dem 17.01.2025 Anwendung. Ab diesem Zeitpunkt sind die DORA-Anforderungen von allen Finanzunternehmen im Anwendungsbereich des Artikels 2 DORA zu erfüllen.

2 Nach § 1a Abs. 2a Satz 1 KWG i.d.F. des Finanzmarktdigitalisierungsgesetzes (FinmadiG) werden auch sonstige, rein national regulierte Institute (z.B. Leasing- und Factoring-Institute) den DORA-Anforderungen unterstellt. § 1a Abs. 2a Satz 2 KWG regelt zudem Erleichterungen für diese Institute im Hinblick auf DORA in solchen Bereichen, in denen diese Anforderungen unter dem Gesichtspunkt der Proportionalität für diese typischerweise weniger großen, komplexen und systemrelevanten Finanzunternehmen unangemessen wären. Da sich die unmittelbar von DORA betroffenen Finanzunternehmen bereits seit dem Abschluss der Verhandlungen zur DORA auf die neue Rechtslage vorbereiten konnten, sehen die Übergangsvorschriften in § 65a Abs. 3 Satz 1 KWG für diese Finanzunternehmen vor, dass § 1a Abs. 2a KWG ab dem 01.01.2027 anzuwenden ist. Die Anforderungen an das Meldewesen nach Kapitel III DORA sind jedoch gemäß § 65a Abs. 3 Satz 2 KWG auch bei diesen Instituten ab dem 17.01.2025 zu beachten.

3 Mit dem FinmadiG wird für Finanzunternehmen die Prüfung von bestimmten DORA-Anforderungen durch den Abschlussprüfer als Erweiterung der Jahresabschlussprüfung eingeführt. Die Übergangsvorschriften zum FinmadiG sehen vor, dass die Prüfungspflicht in Bezug auf DORA erstmals für ein nach dem 31.12.2024 beginnendes Geschäftsjahr Anwendung findet.

4 Für die betreffenden Finanzunternehmen sind die Prüfungspflichten wie folgt geregelt:

Beaufsichtigtes Finanzunternehmen	Prüfungspflicht
Kreditinstitute § 29 Abs. 1 Satz 2 Nr. 2 Buchst. m KWG	Bei der Prüfung des Jahresabschlusses hat der Abschlussprüfer insb. festzustellen, ob das Institut die folgenden Anzeigepflichten und Anforderungen erfüllt hat: Die Anforderungen nach den Artikeln 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA, auch i.V.m. einer Delegierten Verordnung nach den Artikeln 15, 16, 20, 28 oder Artikel 30 DORA.
Zahlungsinstitute / E-Geld-Institute (nachfolgend auch Institute) § 24 Abs. 1 Satz 3 Nr. 5 ZAG	Der Prüfer hat zu prüfen, ob das Institut seinen Verpflichtungen nach den Artikeln 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA, auch i.V.m. einer Delegierten Verordnung nach den Artikeln 15 und 20 DORA, nachgekommen ist.

[3] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. EU Nr. L 333 vom 27.12.2022, S. 1).

Wertpapierinstitute § 78 Abs. 1 Satz 3 Nr. 5 Buchst. h WpIG	Bei der Prüfung des Jahresabschlusses hat der Abschlussprüfer insb. festzustellen, ob das Wertpapierinstitut die folgenden Anzeigepflichten und Anforderungen erfüllt hat: sofern davon betroffene Geschäfte vom Wertpapierinstitut erbracht werden, die Anforderungen nach den Artikeln 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA, auch i.V.m. einer Delegierten Verordnung nach den Artikeln 15, 16, 20, 28 oder Artikel 30 DORA.
Institute mit Kryptowerte-Dienstleistungen nach dem KMAG § 40 Abs. 1 Satz 3 Nr. 5 KMAG	Der Abschlussprüfer hat zu prüfen, ob das Institut seinen Verpflichtungen nach den Artikeln 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA, auch i.V.m. einer Delegierten Verordnung nach den Artikeln 15 und 20 DORA, nachgekommen ist, soweit diese Verpflichtungen auf das Institut anzuwenden sind.
Versicherungsunternehmen § 35 Abs. 1 Satz 1 Nr. 10 VAG	Bei der Prüfung des Jahresabschlusses hat der Prüfer festzustellen, ob das Versicherungsunternehmen folgende Anzeigepflichten und Anforderungen erfüllt hat: die Vorgaben nach den Artikeln 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA, auch i.V.m. einer Delegierten Verordnung nach den Artikeln 15, 16, 20, 28 oder Artikel 30 DORA.
Erlaubnispflichtige externe Kapitalverwaltungsgesellschaft § 38 Abs. 3 Satz 2 Nr. 9 KAGB	Der Prüfer hat festzustellen, ob die erlaubnispflichtige externe Kapitalverwaltungsgesellschaft die Anforderungen nach den Artikeln 5 bis 14, 17 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA, auch i.V.m. einer Delegierten Verordnung nach den Artikeln 15, 20, 28 oder Artikel 30 DORA, erfüllt hat.
Investmentaktiengesellschaft mit veränderlichem und fixem Kapital § 121 Abs. 3 Satz 1 Nr. 2 Buchst. h KAGB bzw. § 148 i.V.m. § 121 Abs. 3 Satz 1 Nr. 2 Buchst. h KAGB	Der Abschlussprüfer hat bei Investmentaktiengesellschaften mit veränderlichem Kapital zu prüfen, ob bei der Verwaltung des Vermögens der Investmentaktiengesellschaft mit veränderlichem Kapital die Anforderungen nach den Artikeln 5 bis 14, 17 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA, auch i.V.m. einer Delegierten Verordnung nach den Artikeln 15, 20, 28 oder Artikel 30 DORA, beachtet worden sind.
Offene und geschlossene Investmentkommanditgesellschaft § 136 Abs. 3 Satz 2 Nr. 8 KAGB bzw. § 159 i.V.m. § 136 Abs. 3 Satz 2 Nr. 8 KAGB	Der Abschlussprüfer hat bei seiner Prüfung festzustellen, ob die offene Investmentkommanditgesellschaft die Anforderungen nach den Artikeln 5 bis 14, 17 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA, auch i.V.m. einer Delegierten Verordnung nach den Artikeln 15, 20, 28 oder Artikel 30 DORA, erfüllt hat.

Für erlaubnispflichtige externe Kapitalverwaltungsgesellschaften, Investmentaktiengesellschaften mit veränderlichem Kapital sowie offene und geschlossene Investmentkommanditgesellschaften ist die Einhaltung des Artikels 16 DORA für den vereinfachten IKT-Risikomanagementrahmen nicht Gegenstand der Prüfung. Auf diesen abweichenden Prüfungsgegenstand wird im Weiteren nur Bezug genommen, soweit dies erforderlich ist.

5 Die Prüfungspflichten betreffen die folgenden Regelungsbereiche:

Regelungsbereich	Prüfungspflichtige Anforderungen
Informations- und Kommunikationstechnologie (IKT) - Risikomanagement	Artikel 5 bis 14 DORA
Vereinfachter IKT-Risikomanagementrahmen	Artikel 16 DORA Für externe Kapitalverwaltungsgesellschaften, Investmentaktiengesellschaften mit veränderlichem Kapital sowie offene Investmentkommanditgesellschaften ist die Einhaltung des Artikels 16 DORA für den vereinfachten IKT-Risikomanagementrahmen nicht Gegenstand der Prüfung.
Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (IKT-Vorfallsmeldewesen)	Artikel 17 bis 19 und 23 DORA
Testen der digitalen operationalen Resilienz	Artikel 24 und 25 DORA
Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos (IKT-Drittparteirisikomanagement)	Artikel 28 bis 30 DORA
Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen	Artikel 45 Abs. 3 DORA

Die BaFin hat eine Aufsichtsmitteilung zur Unterstützung bei der Umsetzung der DORA-Anforderungen an das IKT-Risikomanagement und das IKT-Drittparteienrisikomanagement veröffentlicht.[4]

Nach Artikel 4 DORA haben die Finanzunternehmen bei der Umsetzung der DORA-Anforderungen den Grundsatz der Verhältnismäßigkeit (Proportionality principle) zu beachten (vgl. Anlage).

Die Anforderungen nach den Artikeln 26 und 27 DORA zu den von Finanzunternehmen vorzunehmenden sog. „Threat-Led Penetration Testing“ (TLPT) sind nicht prüfungspflichtig.

6 Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) legt in diesem *IDW Prüfungsstandard* die Berufsauffassung dar, nach welchen Grundsätzen Abschlussprüfer unbeschadet ihrer Eigenverantwortlichkeit eine Prüfung von DORA-Anforderungen bei den in der Tz. 4 genannten Finanzunternehmen durchführen und über diese Prüfung berichten (Aufsichtliche DORA-Prüfung).

[4] https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/Aufsichtsmitteilung/dl_2024_07_08_Aufsichtsmitteilung_Umsetzungshinweise_DORA.pdf?__blob=publicationFile&v=2 (letzter Abruf: 27.07.2025).

A6 Dieser *IDW Prüfungsstandard* berücksichtigt die in *IDW PS 526 (10.2023)*[5] dargestellten einschlägigen Anforderungen für die Durchführung aufsichtlicher Prüfungen im Rahmen der Abschlussprüfung von Instituten nach § 29 KWG.

7 Die vom IDW für die Prüfung von Abschlüssen herausgegebenen Grundsätze ordnungsmäßiger Abschlussprüfung sind auf die Prüfung von historischen Finanzinformationen ausgerichtet und können somit prüfungsmethodologisch nicht bei der Prüfung der DORA -Anforderungen wie z.B. der organisatorischen Vorgaben an das IKT-Risikomanagement oder IKT-Vorfallsmeldewesen angewendet werden. Angesichts der Besonderheiten der aufsichtlichen Anforderungen an Finanzunternehmen sowie der (Berichts-)Vorgaben an Abschlussprüfer legt dieser *IDW Prüfungsstandard* daher eigenständige Prüfungsanforderungen zur Erfüllung der Pflichten des Abschlussprüfers bei der Prüfung der Artikel 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA fest. Die Prüfungsanforderungen dieses *IDW Prüfungsstandards* berücksichtigen abschließend solche Prüfungsanforderungen des ISAE 3000 (Revised) „Assurance Engagements Other than Audits or Reviews of Historical Financial Information“, die unter Beachtung der aufsichtlichen Regelungen und deren Besonderheiten bei der Erfüllung der jeweiligen Prüfungspflichten (vgl. Tz. 3 f.) i.V.m. der jeweiligen Prüfungsberichtsverordnung herangezogen werden können.

Die jeweiligen Prüfungsberichtsverordnungen (d.h. PrüfbV, ZahlPrüfbV, WpIPrüfbV, PrüfV und KAPrüfbV) der einzelnen Finanzunternehmen wurden bislang nicht angepasst und berücksichtigen nicht die neuen Prüfungspflichten in Bezug auf die DORA-Anforderungen. Anders als bei Versicherungsunternehmen ist bei Kredit-, Zahlungs-/E-Geld- und Wertpapierinstituten sowie externen Kapitalverwaltungsgesellschaften und bestimmten Investmentvermögen eine Beurteilung der IT-Systeme bereits gegenwärtig Teil der aufsichtlichen Prüfungspflichten im Rahmen der Abschlussprüfung. Die Prüfungsberichtsverordnungen von Finanzunternehmen, bei denen die IT-Systeme bereits nach der Rechtslage vor Inkrafttreten des FinmadiG Gegenstand der aufsichtlichen Prüfungen sind, sehen branchenübergreifend vor, dass der Abschlussprüfer verpflichtet ist, insb. darzustellen und zu beurteilen, ob die organisatorischen, personellen und technischen Vorkehrungen zur Sicherstellung der Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit der aufsichtlich relevanten Daten angemessen sind und wirksam umgesetzt werden (vgl. insb. § 13 Abs. 1 PrüfbV, § 10a Abs. 1 ZahlPrüfbV und § 15 Abs. 1 WpIPrüfbV).

8 Die BaFin hat am 06.12.2024 den Entwurf einer Verordnung zur Änderung der Wertpapierinstituts-Prüfungsberichtsverordnung (WpIPrüfbV) und der Schwarmfinanzierungsdienstleister-Prüfungsverordnung (SchwarmfdPV) zur Konsultation gestellt[6]. Die Neufassung des § 15 Abs. 1 WpIPrüfbV sieht vor, dass der Abschlussprüfer eines Wertpapierinstituts im Prüfungsbericht verpflichtet ist, zusammenfassend über die IKT-Organisation und IKT-Systeme, die wesentliche Geschäftsprozesse unterstützen, zu berichten. Zudem sind wesentliche Änderungen an diesen IKT-Systemen und die entsprechenden IKT-Projekte im Prüfungsbericht darzustellen. Nach der Neufassung des § 15 Abs. 1 Satz 2 WpIPrüfbV ist der Abschlussprüfer ver-

[5] *IDW Prüfungsstandard: Pflichten des Abschlussprüfers nach § 29 KWG (IDW PS 526 (10.2023))* (Stand: 05.10.2023).

[6] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Konsultation/2024/kon_11_24_Konsultation_WpIPruefbV_SchwarmfdPV.html (letzter Abruf: 27.07.2025).

pflichtet, darzustellen und zu beurteilen, ob die organisatorischen, personellen und technischen Vorkehrungen zur Sicherstellung der Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit der IKT-Systeme, die wesentliche Geschäftsprozesse unterstützen oder aufsichtsrechtlich relevante Daten verarbeiten, angemessen sind und wirksam umgesetzt werden. Werden externe IKT-Ressourcen eingesetzt, so erstrecken sich die vorgenannten Berichtspflichten auch auf diese IKT-Ressourcen sowie deren Einbindung im Wertpapierinstitut. Der Abschlussprüfer ist gemäß § 15 Abs. 2 WpIPrüfbV verpflichtet zu beurteilen, ob das Wertpapierinstitut die Anforderungen der Artikel 5 bis 14, 16, 17 bis 19, 24 und 25, 28 bis 30 und 45 Abs. 3 DORA auch i.V.m. einer Delegierten Verordnung nach Artikel 15, 16, 20, 28 oder 30 DORA, angemessen und wirksam einhält. Dabei ist, soweit anwendbar, insb. einzugehen auf

1. das IKT-Risikomanagement gemäß Artikel 5 bis 14 und 16 DORA,
2. die Dokumentation des IKT-Risikomanagementrahmens gemäß Artikel 6 Abs. 5 Satz 1 oder Artikel 16 Abs. 2 Satz 1 DORA,
3. die IKT-Geschäftsfortführungsleitlinie nach Artikel 11 Abs. 1 Satz 1 DORA,
4. die Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle gemäß Artikel 17 bis 19 DORA,
5. das Testen der digitalen operationalen Resilienz gemäß Artikel 24 und 25 DORA,
6. das Management des IKT-Drittparteienrisikos gemäß Artikel 28 bis 30 DORA und
7. die Einhaltung der Meldepflicht in Bezug auf Vereinbarungen über den Austausch von Informationen gemäß Artikel 45 Abs. 3 DORA.

Die Anforderungen an die Berichterstattung nach der Neufassung des § 15 WpIPrüfbV verpflichten den Abschlussprüfer somit insb., eine Beurteilung der Angemessenheit und Wirksamkeit der organisatorischen, personellen und technischen Vorkehrungen zur Einhaltung der DORA-Anforderungen vorzunehmen.

Vorbehaltlich etwaiger Änderungen der Prüfungsberichtsverordnungen in Bezug auf die Prüfung der DORA-Anforderungen wird in diesem IDW Prüfungsstandard davon ausgegangen, dass vom Abschlussprüfer bei allen prüfungspflichtigen Finanzunternehmen (Tz. 4) eine entsprechende Beurteilung über die Angemessenheit und Wirksamkeit der organisatorischen, personellen und technischen Vorkehrungen und Berichterstattung erwartet wird.

9 Die gesetzlichen Vertreter sind für die Einhaltung der an das beaufsichtigte Finanzunternehmen gerichteten aufsichtlichen Anforderungen verantwortlich. Die Mitglieder des Aufsichtsorgans sind für die Wahrnehmung ihrer Überwachungsfunktion verantwortlich, einschließlich der Überwachung der gesetzlichen Vertreter bei der Erfüllung der an das beaufsichtigte Finanzunternehmen gerichteten aufsichtlichen Anforderungen.

10 Dieser *IDW Prüfungsstandard* ist erstmals anzuwenden für Aufsichtliche DORA-Prüfungen in Bezug auf Berichtszeiträume (vgl. Tz. 11 g.), die nach dem 31.12.2024 beginnen, mit der Ausnahme von Rumpfgeschäftsjahren, die vor dem 31.12.2025 enden. Eine vorzeitige Anwendung ist zulässig.

1.2. Definitionen

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

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

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

c. Aufsichtliche Vorgabe: eine nach Maßgabe der jeweiligen Prüfungspflichten (vgl. Tz. 3) i.V.m. der jeweiligen Prüfungsberichtsverordnung (d.h. in PrüfbV, ZahlPrüfbV, WpIPrüfbV, PrüfV bzw. KAPrüfbV) konkretisierte Verpflichtung eines Abschlussprüfers, dort bezeichnete Aufsichtliche DORA-Prüfungen durchzuführen. Darunter sind jeweils die für den Berichtszeitraum gültigen, veröffentlichten aufsichtlichen Vorgaben an den Abschlussprüfer zu verstehen. Im Unterschied zu einer an beaufsichtigte Finanzunternehmen gerichteten, aufsichtlichen Anforderung ist Adressat einer aufsichtlichen Vorgabe der Abschlussprüfer.

d. Aufsichtliche Wirksamkeitsprüfung (nachfolgend: „Wirksamkeitsprüfung“): Beurteilung, ob die durch das Finanzunternehmen vorgegebenen Prozesse, Regelungen und Verfahren innerhalb des Berichtszeitraums wie vorgesehen eingehalten wurden.

e. Beanstandungen: negative Prüfungsfeststellungen des Abschlussprüfers (Feststellung eines Normverstoßes i.S. der jeweiligen Prüfungsberichtsverordnung).

f. Berichtsstichtag: Stichtag, auf den sich die zu treffenden Aussagen des Abschlussprüfers beziehen, soweit sie sich nicht auf einen Berichtszeitraum erstrecken.

g. Berichtszeitraum: Der Zeitraum, auf den sich die Prüfung erstreckt (Berichtszeitraum), ist i.d.R. das am Bilanzstichtag endende Geschäftsjahr (Berichtsjahr). Der Bilanzstichtag ist der Stichtag des Jahresabschlusses oder des konsolidierten Abschlusses.

h. Indikatoren: aus dem Grundsatz der Proportionalität abgeleitete Maßstäbe zur Würdigung des „Soll-Objekts“ und – sofern einschlägig – Anhaltspunkte zur Planung von Wirksamkeitsprüfungen.

i. Mangel: Abweichung (des Finanzunternehmens) von den aufsichtlichen Anforderungen oder organisatorischen Vorgaben.

j. Organisatorische Vorgaben („Soll-Objekt“): vom Finanzunternehmen konkretisierte Ausgestaltung der aufsichtlichen Anforderungen in der Aufbau- und Ablauforganisation in Bezug auf die Anforderungen nach den Artikeln 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA.

k. Proportionalität: ein auf der Verhältnismäßigkeit beruhender aufsichtlicher Grundsatz, der sich auf Ebene des einzelnen Finanzunternehmens auf die Angemessenheit der organisatorischen Vorkehrungen bezieht.

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

m. Prüfungsnachweise: Informationen, die der Abschlussprüfer nutzt, um begründete Schlussfolgerungen (Prüfungsfeststellungen) zu ziehen.

1.3. Aussageart

12 Die bei der Prüfung der Artikel 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA anzuwendende Aussageart „Aufsichtliche DORA-Prüfung" umfasst „Organisationsprüfungen". Danach hat der Abschlussprüfer Würdigungen und Prüfungshandlungen unter Beachtung der aufsichtlichen Vorgaben und unter Ausübung seines pflichtgemäßen Ermessens vorzunehmen und über durchgeführte Prüfungshandlungen und deren Ergebnisse (Prüfungsfeststellungen) zu berichten (vgl. Abschn. 2.3.1.).

13 Während im Rahmen der Jahresabschlussprüfung nach § 317 HGB jeweils ein Gesamturteil zum Abschluss und zum Lagebericht abzugeben ist, hat der Abschlussprüfer die nach den aufsichtlichen Vorgaben geforderten Aussagen einzeln zu treffen und in einer Zusammenfassenden Schlussbemerkung gemäß der jeweiligen Prüfungsberichtsverordnung zu allen wichtigen Fragen so Stellung zu nehmen, dass die Berichtsadressaten, insb. die Aufsicht, aus ihr ein Gesamturteil gewinnen können. Des Weiteren hat der Abschlussprüfer – sofern dies nach einer entsprechenden Prüfungsberichtsverordnung vorgeschrieben ist – Beanstandungen zu klassifizieren.

14 Auch wenn die Aufsichtliche Prüfung und die Prüfung des Abschlusses insoweit unterschiedliche Ziele verfolgen, ergeben sich bei der Durchführung der Aufsichtlichen DORA-Prüfung durch den Abschlussprüfer Vorteile, insb. durch die Nutzung der Erkenntnisse aus der Prüfung des Abschlusses sowie ggf. anderen Prüfungen und vice versa.

2. Planung und Durchführung der Aufsichtlichen DORA-Prüfung

2.1. Allgemeine Berufspflichten, Auftragsannahme und Qualitätssicherung

15 Die Unabhängigkeitsanforderungen sowie die allgemeinen Berufsgrundsätze der WPO und der Berufssatzung, insb. die Ausübung des pflichtgemäßen Ermessens und der kritischen Grundhaltung, sind bei der Aufsichtlichen DORA-Prüfung zu beachten.

16 Da die Pflichten des Abschlussprüfers (vgl. Tz. 3 f.) bei der Abschlussprüfung zu erfüllen sind, gelten für die Auftragsannahme die für den Abschlussprüfer einschlägigen Prüfungsstandards bzw. ISA [DE] des IDW.

17 Die für die Qualitätssicherung der Auftragsabwicklung auf Praxisebene einschlägigen Anforderungen der *IDW QMS 1 (09.2022)*[7] und *IDW QMS 2 (09.2022)*[8] sind zu beachten.

---

[7] *IDW Qualitätsmanagementstandard: Anforderungen an das Qualitätsmanagement in der Wirtschaftsprüfungspraxis (IDW QMS 1 (09.2022))* (Stand: 28.09.2022).

[8] *IDW Qualitätsmanagementstandard: Auftragsbegleitende Qualitätssicherung (IDW QMS 2 (09.2022))* (Stand: 28.09.2022).

2.2. Planung der Aufsichtlichen DORA-Prüfung

18 Der Abschlussprüfer hat die Aufsichtliche DORA-Prüfung in sachlicher, personeller und zeitlicher Hinsicht so zu planen, dass sie in sachgerechter Weise durchgeführt werden kann.

19 Hierzu hat der Abschlussprüfer die Zielsetzungen der Aufsichtlichen DORA-Prüfung (vgl. Tz. 6) sowie die darauf bezogene Aussageart bei der Planung und Durchführung zu berücksichtigen.

20 Der Abschlussprüfer hat den in den aufsichtlichen Vorgaben enthaltenen Handlungsanweisungen in Bezug auf Art und Umfang der Aufsichtlichen DORA-Prüfung sowie zur Berichterstattung – soweit einschlägig – nachzukommen. Zudem hat der Abschlussprüfer etwaige ergänzende Prüfungsinhalte oder Schwerpunkte in der Planung für die Aufsichtliche DORA-Prüfung (insb. § 30 KWG, § 35a VAG, § 24 Abs. 4 ZAG, § 40 Abs. 3 KMAG, § 78 Abs. 4 WpIG sowie §§ 38, 121 und 136 KAGB) zu berücksichtigen.

21 Der Abschlussprüfer hat im Rahmen der Planung der konkreten Tätigkeiten insb. die Größe des Finanzunternehmens, den Geschäftsumfang sowie die Komplexität und den Risikogehalt der betriebenen Geschäfte zu berücksichtigen (Grundsätze der risikoorientierten Prüfung und Wesentlichkeit; vgl. auch § 3 PrüfbV, § 2 ZahlPrüfbV, § 3 WpIPrüfbV sowie § 2 KAPrüfbV). Daher hat der Abschlussprüfer dem Grundsatz der Proportionalität Rechnung zu tragen (vgl. Tz. 27).

A21 *Für die Aufsichtliche DORA-Prüfung relevante Informationen können sich auch aus Medienberichten oder anderen (externen) Quellen, bspw. Informationen über neue Technologien, Schadensfälle oder Cyberbedrohungen ergeben.*

22 Wurde im Berichtszeitraum eine Prüfung mit Bezug zu den Artikeln 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 oder 45 Abs. 3 DORA gemäß

- Kreditinstitute: § 44 Abs. 1 Satz 2 KWG oder Artikel 12 Nr. 1 der Verordnung (EU) Nr. 1024/2013 des Rates vom 15.10.2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank (vgl. § 4 Abs. 4 PrüfbV)
- Versicherungsunternehmen: § 294 Abs. 1 bis 5 und Abs. 8, § 306 Abs. 1 Satz 1 Nr. 1 VAG
- Zahlungs-/E-Geld-Institute: § 19 Abs. 1 Satz 3 ZAG (vgl. § 3 Abs. 3 ZahlPrüfbV)
- Wertpapierinstitute: § 5 Abs. 4 Satz 2 WpIG (vgl.§ 4 Abs. 7 WpIPrüfbV)
- Externe Kapitalverwaltungsgesellschaften, Investmentaktiengesellschaften mit veränderlichem Kapital sowie offene Investmentkommanditgesellschaften: § 14 KAGB i.V.m. § 44 Abs. 1 Satz 2 KWG (vgl. § 3 Abs. 2 KAPrüfbV)

durchgeführt, hat der Abschlussprüfer die Ergebnisse dieser Prüfung bei der Aufsichtlichen DORA-Prüfung eigenverantwortlich zu nutzen. Der Abschlussprüfer hat anhand des Prüfungsberichts ein Verständnis von den Tätigkeiten (einschließlich der Ergebnisse) des Sonderprüfers zu gewinnen und die Eignung der Tätigkeit des Sonderprüfers als Prüfungsnachweis für die Aufsichtliche DORA-Prüfung zu würdigen.

A22 *Bei den Prüfungen mit Bezug zu den Artikeln 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 oder 45 Abs. 3 DORA, die vom Prüfer genutzt werden, kann es sich auch um Prüfungen von IKT-*

Dienstleistern handeln, über die dem Finanzunternehmen Nachweise zur Durchführung der Prüfung (einschließlich der Ergebnisse) (insb. der Prüfungsbericht) vorliegen.

23 Wenn der Abschlussprüfer feststellt, dass sich die Tätigkeit des Sonderprüfers als Prüfungsnachweis für die Aufsichtliche DORA-Prüfung eignet und keine Beanstandungen seitens des Sonderprüfers zu bestimmten Teilgebieten getroffen wurden, darf der Abschlussprüfer in diesen Teilgebieten die Aufsichtliche DORA-Prüfung auf bedeutsame Veränderungen beschränken, die seit dem Ende des Berichtszeitraums der Sonderprüfung (vgl. Tz. 22) bis zum Berichtsstichtag eingetreten sind. Für den Fall, dass Beanstandungen getroffen wurden, ist zu prüfen, ob die Mängel fortbestehen oder beseitigt wurden (für Details siehe Tz. 59).

A23 Bei der Beurteilung, ob sich die Tätigkeit einer aufsichtlichen Sonderprüfung als Prüfungsnachweis für die Aufsichtliche DORA-Prüfung eignen, kann es notwendig sein zu berücksichtigen, dass sich eine solche Sonderprüfung i.d.R. nur auf einzelne Anforderungen eines Teilgebiets bezieht und zu diesen ggf. nur im Falle von Beanstandungen Feststellungen getroffen werden. Wenn die Tätigkeiten des Sonderprüfers nicht ausreichend im Sonderprüfungsbericht dargestellt sind, kann es für den Abschlussprüfer notwendig sein festzustellen, dass sich die Tätigkeit des Sonderprüfers nicht als Prüfungsnachweis für die Aufsichtliche DORA-Prüfung eignet und daher nicht genutzt werden kann.

24 Auf der Grundlage der durchgeführten Tätigkeiten und der erlangten Informationen hat der Abschlussprüfer vor Beendigung der Aufsichtlichen DORA-Prüfung zu würdigen, ob

a. die der Planung zugrunde gelegten Annahmen unverändert zutreffen und
b. die Ergebnisse aus Aufsichtlichen Prüfungen der Sachgebiete nicht zueinander im Widerspruch stehen.

25 Die im Rahmen der Jahresabschlussprüfung einzuholende schriftliche Erklärung der gesetzlichen Vertreter („Vollständigkeitserklärung“) hat sich auch auf die Aufsichtliche DORA-Prüfung zu erstecken.

A25.1 *Die Vollständigkeitserklärung kann nur zur Unterstützung sonstiger Prüfungsnachweise dienen.*

A25.2 *Es liegen Muster und Module des IDW für eine Vollständigkeitserklärung vor. Die Verwendung, Ergänzung oder Abänderung dieser Muster liegen im pflichtgemäßen Ermessen des Abschlussprüfers.*

2.3. Durchführung der Aufsichtlichen DORA-Prüfung

2.3.1. Organisationsprüfung

2.3.1.1. Aufbau der Aufsichtlichen DORA-Prüfung

26 In den Fällen, in denen Aussagen des Abschlussprüfers zur Angemessenheit und – sofern vom Abschlussprüfer gefordert – zur Wirksamkeit von organisatorischen Vorkehrungen erwartet werden (Organisationsprüfungen) (vgl. Tz. 7), hat der Abschlussprüfer bei der Aufsichtlichen DORA-Prüfung die folgenden Schritte durchzuführen:

a. Würdigung des „Soll-Objekts“: Erfassung und Würdigung der Eignung der aus den aufsichtlichen Anforderungen durch das Finanzunternehmen als erforderlich abgeleiteten

organisatorischen Vorgaben (d.h. vom Finanzunternehmen konkretisierte Ausgestaltung der aufsichtlichen Anforderungen in der Aufbau- und Ablauforganisation) (vgl. Abschn. 2.3.1.2.)

b. Angemessenheitsprüfung: Beurteilung der angemessenen Umsetzung der organisatorischen Vorgaben in Prozesse, Regelungen und Verfahren (vgl. Abschn. 2.3.1.3.)

c. Wirksamkeitsprüfung: Beurteilung der Einhaltung von vorgegebenen Prozessen, Regelungen und Verfahren (vgl. Abschn. 2.3.1.4.).

A26 *Die Würdigung des „Soll-Objekts" und die Angemessenheitsprüfung sind miteinander verbunden und werden deshalb häufig innerhalb eines Arbeitsschritts im Rahmen der Aufsichtlichen Prüfung erfolgen, einheitlich dokumentiert und in einem Ergebnis zur Angemessenheitsprüfung zusammengefasst.*

27 Ausgehend von den Grundsätzen der risikoorientierten Prüfung und der Wesentlichkeit und somit dem Prinzip der Proportionalität hat der Abschlussprüfer für das Finanzunternehmen und in Bezug auf die Sachgebiete anhand geeigneter Indikatoren Risiko- und Wesentlichkeitseinschätzungen vorzunehmen, welche als Basis für die Aufsichtliche DORA-Prüfung dienen.

A27 *Beispiele für geeignete Indikatoren sind in der Anlage dargestellt. Die Risiko- und Wesentlichkeitseinschätzungen des Abschlussprüfers anhand geeigneter Indikatoren beeinflussen die Prüfungsintensität. Während z.B. ein niedrigeres Gesamtrisikoprofil einen geringeren Umfang der Prüfungshandlungen bei einem Finanzunternehmen bzw. für einzelne Regelungsbereiche zur Folge haben kann, kann ein höheres Risiko z.B. in Bezug auf kritische oder wichtige Funktionen (Artikel 3 Nr. 22 DORA) des Finanzunternehmens es notwendig machen, dass der Abschlussprüfer seine Prüfungshandlungen bei einem Finanzunternehmen bzw. in den betroffenen Regelungsbereich ausweitet.*

28 Ist eine Änderung der aufsichtlichen Anforderungen bzw. der organisatorischen Vorkehrungen zur Einhaltung der DORA-Anforderungen im Berichtszeitraum erfolgt, so hat der Abschlussprüfer dies in Abhängigkeit von den jeweiligen Umständen bei der Planung und Durchführung der Aufsichtlichen DORA-Prüfung zu berücksichtigen.

2.3.1.2. Würdigung des „Soll-Objekts"

29 Der Abschlussprüfer hat zu würdigen, ob das Finanzunternehmen aus den für sein Geschäftsmodell einschlägigen aufsichtlichen Anforderungen an die organisatorischen, personellen und technischen Vorkehrungen zur Einhaltung der Anforderungen der Artikel 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 oder 45 Abs. 3 DORA passende erforderliche organisatorische Vorgaben abgeleitet hat.

A29.1 *Die organisatorischen, personellen und technischen Vorkehrungen betreffen insb. die Sicherstellung der Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit der IKT-Systeme, die wesentliche Geschäftsprozesse unterstützen oder aufsichtsrechtlich relevante Daten verarbeiten.*

A29.2 *Die erforderlichen organisatorischen Vorgaben schlagen sich in einer durch Prozesse, Regelungen und Verfahren vom Finanzunternehmen konkretisierten Ausgestaltung der aufsichtlichen Anforderungen in der Aufbau- und Ablauforganisation nieder.*

A29.3 *Die Verantwortung für die Angemessenheit des Soll-Objekts liegt bei den gesetzlichen Vertretern des Finanzunternehmens.*

30 Der Abschlussprüfer hat sich als Grundlage für seine Würdigung des Soll-Objekts ein umfassendes Bild von den Prozessen, Regelungen und Verfahren des Finanzunternehmens zu machen, welche der Umsetzung der aufsichtlichen Anforderungen dienen.

A30 *Informationsquellen des Abschlussprüfers zur Erlangung eines umfassenden Bildes von den Prozessen, Regelungen und Verfahren des Finanzunternehmens können z.B. sein:*

- *Geschäfts-, IT- bzw. DOR-Strategie*
- *Darstellung der IKT-bezogenen Aufbauorganisation*
- *Übersicht der schriftlich fixierten Ordnung bzw. Organisationshandbuch zur IKT*
- *Übersicht aller bedeutsamen Unternehmensfunktionen sowie ermittelte kritische oder wichtige Funktionen*
- *Darstellung der Netzwerk- bzw. IKT-Architektur oder IT-Infrastruktur*
- *Darstellung des Inventars der bedeutsamen Informations- und IKT-Assets sowie deren Verbindungen und Interdependenzen untereinander*
- *Dokumentation des IKT-Informationsregisters*
- *Übersicht der bedeutsamen IKT-Projekte*
- *Berichte des IKT-Risikomanagers*
- *Berichte der internen Revision bzw. externen Prüfer*
- *Übersicht zu geplanten und tatsächlich durchgeführten Schulungs- und Awareness-Maßnahmen*
- *Übersicht der IKT-Drittdienstleister*
- *im Fall von Nutzung von IKT-Dienstleistungen: Vereinbarungen und Verträge mit dem IKT-Drittdienstleister*
- *Berichte der IKT-Drittdienstleister*
- *Berichte des Notfallmanagers*
- *Berichte und Meldungen an Aufsichtsbehörden.*

31 Der Abschlussprüfer hat bei der Würdigung des Soll-Objekts die Erfahrungen und Erkenntnisse zu nutzen, die er im Rahmen der Prüfung des Abschlusses sowie sonstiger Prüfungstätigkeiten beim Finanzunternehmen erlangt hat.

32 Die Würdigung des Soll-Objekts hat auf Basis geeigneter Maßstäbe (Indikatoren) zu erfolgen. Bei der Bestimmung von Maßstäben im Rahmen von Aufsichtlichen Prüfungen hat der Abschlussprüfer stets auch die Zwecksetzung der aufsichtlichen Anforderungen in seine Würdigungen einzubeziehen.

A32 *Beispiele für geeignete Indikatoren sind in der Anlage dargestellt.*

2.3.1.3. Angemessenheitsprüfung

33 Die Angemessenheitsprüfung dient der Beurteilung, ob das Finanzunternehmen die aus den aufsichtlichen Anforderungen abgeleiteten erforderlichen organisatorischen Vorgaben angemessen in Prozesse, Regelungen und Verfahren umgesetzt hat, um die aufsichtlichen Anforderungen zu erfüllen.

34 Der Abschlussprüfer hat zur Gewinnung von Prüfungsnachweisen und zum Treffen von Prüfungsfeststellungen im Rahmen der Angemessenheitsprüfung geeignete Prüfungshandlungen durchzuführen.

A34 *Dabei können folgende Prüfungshandlungen in Betracht kommen:*

- *Befragungen (bspw. des für die Kontrollfunktion Verantwortlichen, der Internen Revision, von Mitarbeitern aus relevanten operativen Bereichen)*
- *Einsichtnahme in Unterlagen der schriftlich fixierten Ordnung, z.B. Richtlinien und Organisationshandbücher mit Ausführungen zum IKT-Risikomanagementrahmen, Festlegung der kritischen oder wichtigen Funktionen und der daraus abgeleiteten Maßnahmen (z.B. jährliche Notfalltests, Ausstiegsstrategie, Authentifizierungsmethoden etc.) sowie zu der Sicherheitskonzeption für Räumlichkeiten oder physischen Anlagen, sofern dies in Bezug auf bestimmte IKT-Assets geboten ist*
- *Beobachtung bzw. Nachvollzug von Aktivitäten und Arbeitsabläufen (Walkthrough) im Finanzunternehmen (z.B. Nachvollzug der Überprüfung des IKT-Risikomanagementrahmens, Nachvollzug der Ermittlung und Klassifizierung aller IKT-gestützten Unternehmensfunktionen, Nachvollzug des Umgangs mit schwerwiegenden IKT-bezogenen Vorfällen)*
- *Einsichtnahme am System (z.B. um die Kritikalitätseinstufung der IKT-Assets im Asset-Inventar oder Authentifizierungsmechanismen im Active Directory nachzuvollziehen)*
- *Einsichtnahme in Berichte der zweiten und dritten Verteidigungslinie (z.B. zentrales Auslagerungsmanagement, Bericht zur Überprüfung des IKT-Risikomanagementrahmens und Berichte der Internen Revision).*

2.3.1.4. Wirksamkeitsprüfung

35 Der Abschlussprüfer hat – soweit aufsichtliche Vorgaben dies fordern (vgl. Tz. 7 f.) – die Wirksamkeit der Prozesse, Regelungen und Verfahren im Berichtszeitraum zu beurteilen. Führt die Angemessenheitsprüfung zu dem Ergebnis, dass Vorkehrungen des Finanzunternehmen zur Einhaltung der Artikel 5 bis 14, 16 bis 19, 23 bis 25, 28 bis 30 und 45 Abs. 3 DORA nicht angemessen sind, ist insoweit keine Wirksamkeitsprüfung durchzuführen (zu den Folgen für die Berichterstattung vgl. Abschn. 2.4).

36 Im Rahmen von Wirksamkeitsprüfungen hat der Abschlussprüfer geeignete Prüfungshandlungen durchzuführen, um Prüfungsnachweise zur Wirksamkeit der Prozesse, Regelungen und Verfahren zu gewinnen. Art und Umfang (u.a. eine nachvollziehbare Auswahl von Elementen) der Prüfungshandlungen liegen im Ermessen des Abschlussprüfers (vgl. Tz. 12 und 21).

A36.1 *Gegenstand der Wirksamkeitsprüfungen können Kontrollen oder andere Maßnahmen zur wirksamen Durchführung von Prozessen und Verfahren bzw. zur Einhaltung von Regelungen*

sein. Bei Wirksamkeitsprüfungen können insb. folgende Prüfungshandlungen in Betracht kommen:

- *Befragungen von Mitgliedern der Leitungsebene und von Mitarbeitern auf den relevanten organisatorischen Ebenen und insb. mit Bezug zu den kritischen oder wichtigen Funktionen des Finanzunternehmens*
- *Durchsicht von Unterlagen (z.B. Risikoanalysen, IKT-Drittparteienverträge, Pentestberichte, IT-Notfalltests), die die Durchführung von Prozessen, Regelungen und Verfahren dokumentieren*
- *Nachvollzug von Prozessabläufen der organisatorischen Vorkehrungen zur Einhaltung der DORA-Anforderungen einschließlich Qualitätssicherungsmaßnahmen*
- *Nachvollzug von Tätigkeiten zur Einhaltung der DORA-Anforderungen (insb. in Bezug auf die Festlegung der kritischen oder wichtigen Funktionen des Finanzunternehmens und der daraus abgeleiteten Maßnahmen)*
- *Einsichtnahme in den Bericht zur Überprüfung des IKT-Risikomanagementrahmens der Kontrollfunktion*
- *Nachvollzug der Einhaltung der Sicherheitskonzepte für Räumlichkeiten oder physische Anlagen, soweit dies in Bezug auf bestimmte IKT-Assets geboten ist (einschließlich Einsichtnahme in die Protokollierungen hinsichtlich der Personen, die physischen Zugang zu sicherheitsrelevanten Anlagen oder Räumlichkeiten haben)*
- *Einsichtnahme in die Prüfungsdokumentation der Internen Revision.*

A36.2 *Es kann Fälle geben, in denen Prüfungshandlungen zur Beurteilung der Angemessenheit der Prozesse, Regelungen und Verfahren gleichzeitig sachgerechte Prüfungsnachweise zur Beurteilung von deren Wirksamkeit darstellen. Dies kann dann der Fall sein, wenn*

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

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

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

A36.3 *Das Ergebnis einer Wirksamkeitsprüfung kann Anlass sein, das Ergebnis einer Angemessenheitsprüfung nochmals kritisch zu würdigen (z.B. bei einer auffälligen Anzahl von Mängeln).*

A36.4 *Bei einzelnen DORA-Sachgebieten, in denen sich die Rahmenbedingungen nicht verändert haben und im Rahmen der Angemessenheitsprüfung keine Änderung von Prozessen, Regelungen und Verfahren festgestellt werden, darf bei der Wirksamkeitsprüfung auf die diesbezüglichen Ergebnisse in vorangegangenen Aufsichtlichen Prüfungen zurückgegriffen werden, sofern diese nicht länger als zwei Jahre zurückliegen und dabei keine nennenswerten Beanstandungen getroffen wurden.*

2.4. Prüfungsnachweise

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

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

b. der Abschlussprüfer Zweifel an der Verlässlichkeit der als Nachweise zu nutzenden Informationen hat,

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

38 Bei als Prüfungsnachweisen zu nutzenden Informationen, die durch das Finanzunternehmen erstellt wurden, hat der Abschlussprüfer zu beurteilen, ob die Informationen für die Zielsetzung des Abschlussprüfers ausreichend verlässlich sind. Je nach den Umständen schließt dies erforderlichenfalls ein

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

b. die Beurteilung, ob die Informationen für die Zielsetzung des Abschlussprüfers ausreichend genau und detailliert sind.

39 Falls als Prüfungsnachweise zu nutzende Informationen unter Verwendung der Tätigkeiten eines Sachverständigen der gesetzlichen Vertreter erstellt wurden, hat der Abschlussprüfer, soweit notwendig, unter Berücksichtigung der Bedeutung der Tätigkeit dieses Sachverständigen für die Zwecke des Abschlussprüfers

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

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

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

40 Wenn die Tätigkeiten eines Sachverständigen des Abschlussprüfers als Prüfungsnachweise zu nutzen sind, hat der Abschlussprüfer auch

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

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

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

d. die Angemessenheit der Tätigkeiten des Sachverständigen für die Zwecke des Abschlussprüfers zu beurteilen.

41 Wenn die Tätigkeiten eines anderen Prüfers zu nutzen sind oder im Hinblick auf IKT-Dienstleister genutzt werden sollen, hat der Abschlussprüfer zu beurteilen, ob diese Tätigkeiten für die Zwecke des Abschlussprüfers angemessen sind und inwieweit sie ausreichend sind.

42 Im Falle von Beanstandungen eines anderen Prüfers oder Sachverständigen sind diese darauf hin zu würdigen, welche Auswirkungen sie auf die Aufsichtliche DORA-Prüfung haben und ob und inwieweit sich die Notwendigkeit ergänzender Prüfungshandlungen ergibt.

43 Soweit der Abschlussprüfer plant, Tätigkeiten der Internen Revision im Rahmen der Aufsichtlichen DORA-Prüfung zu nutzen, hat der Abschlussprüfer zu beurteilen,

a. inwieweit die Stellung der Internen Revision innerhalb des Finanzunternehmens sowie relevante Regelungen und Maßnahmen die Objektivität der Internen Revisoren fördern,
b. wie kompetent die Interne Revision in Bezug auf DORA-Anforderungen ist,
c. ob die Interne Revision einer systematischen und geregelten Vorgehensweise, einschließlich Qualitätssicherung, folgt und
d. ob die Tätigkeiten der Internen Revision für die Zwecke der Aufsichtlichen DORA-Prüfung (insb. bzgl. IKT-Risikomanagement, IKT-Verfallsmeldewesen, Testen der digitalen operationalen Resilienz sowie IKT-Drittparteienrisikomanagement) angemessen sind.

2.5. Dokumentation

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

a. Die für das jeweilige Sachgebiet prägenden Merkmale, ggf. unter Verweis auf die Merkmale, die für das Finanzunternehmen übergreifend prägend sind (vgl. Tz. 57, Anlage)
b. Art, zeitliche Einteilung und Umfang der auf dieser Grundlage nach pflichtgemäßem Ermessen bestimmten Prüfungshandlungen, die durchgeführt wurden, um diesen *IDW Prüfungsstandard* einzuhalten
c. die Ergebnisse der durchgeführten Prüfungshandlungen und die erlangten Nachweise sowie
d. die den bedeutsamen Prüfungsfeststellungen zugrunde liegenden Sachverhalte, Schlussfolgerungen und Beurteilungen nach pflichtgemäßem Ermessen.

45 Wenn der Abschlussprüfer während der Prüfungsdurchführung Informationen erlangt, die im Widerspruch zu den bisher erlangten Informationen für eine Prüfungsfeststellung stehen, hat er zu dokumentieren, wie er diese widersprüchlichen Informationen bei der abschließenden Beurteilung des Sachverhalts und die Auswirkung auf die Prüfungsfeststellung berücksichtigt hat.

46 Der Abschlussprüfer hat die Auftragsdokumentation in einer Auftragsakte zusammenzustellen und den redaktionellen Prozess der Zusammenstellung der Dokumentation der Aufsichtlichen DORA-Prüfung spätestens mit dem Abschluss der Auftragsdokumentation für die Abschlussprüfung abzuschließen.

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

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

a. Die genauen Gründe für die Anpassungen oder Ergänzungen sowie

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

3. Berichterstattung

3.1. Grundsätze aufsichtlicher Berichterstattung

49 Der Abschlussprüfer hat über die Gegenstände und Ergebnisse seiner Tätigkeiten zu berichten. Art und Umfang der Berichterstattung liegen im pflichtgemäßen Ermessen des Abschlussprüfers unter Beachtung der aufsichtlichen Vorgaben. Der Umfang der Berichterstattung hat der Bedeutung und dem Risikogehalt der dargestellten Vorgänge zu entsprechen (vgl. insb. § 4 Abs. 1 PrüfbV, § 3 Abs. 1 ZahlPrüfbV, § 2 Abs. 1 PrüfV, § 4 Abs. 1 WpIPrüfbV, § 3 Abs. 4 KAPrüfbV). Die Ausführungen des Abschlussprüfers haben sich auf sämtliche Vorschriften zu erstecken, deren Einhaltung zu prüfen ist (vgl. Tz. 4 f.). Bei der inhaltlichen Ausgestaltung der Berichterstattung darf der Abschlussprüfer davon ausgehen, dass es sich bei den Adressaten um sachverständige Dritte handelt.

50 Die Ergebnisse der Aufsichtlichen DORA-Prüfung hat der Abschlussprüfer im Prüfungsbericht darzulegen.

51 Aussagen des Abschlussprüfers zu aufsichtlichen Vorgaben sind nicht Gegenstand des Bestätigungsvermerks[9] und stellen als solche auch keine in den Bestätigungsvermerk aufzunehmenden besonders wichtigen Prüfungssachverhalte (Key Audit Matters) dar.

52 Die geforderten Aussagen und Berichtspflichten hat der Abschlussprüfer aus den anzuwendenden aufsichtlichen Vorgaben (vgl. Tz. 7 f.) abzuleiten. Der Abschlussprüfer hat im Prüfungsbericht zusammenfassend über die IKT-Organisation und IKT-Systeme, die wesentliche Geschäftsprozesse unterstützen, zu berichten. Wesentliche Änderungen an diesen IKT-Systemen und die entsprechenden IKT-Projekte sind im Prüfungsbericht darzustellen. Der Abschlussprüfer hat darzustellen und zu beurteilen, ob die organisatorischen, personellen und technischen Vorkehrungen zur Sicherstellung der Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit der IKT-Systeme, die wesentliche Geschäftsprozesse unterstützen oder aufsichtsrechtlich relevante Daten verarbeiten, angemessen sind und wirksam umgesetzt werden. Werden externe IKT-Ressourcen eingesetzt, so erstrecken sich die vorgenannten Berichtspflichten auch auf diese IKT-Ressourcen sowie deren Einbindung im Finanzunternehmen. Er hat zu beurteilen, ob das Finanzunternehmen die Anforderungen der Artikel 5 bis 14,

[9] Vgl. *IDW Prüfungsstandard: Bildung eines Prüfungsurteils und Erteilung eines Bestätigungsvermerks (IDW PS 400 n.F. (03.2025))* (Stand: 12.03.2025), Tz. 66 und Tz. A70.

16, 17 bis 19, 24 und 25, 28 bis 30 und 45 Abs. 3 DORA, auch i.V.m. einer Delegierten Verordnung nach Artikel 15, 16, 20, 28 oder 30 DORA, angemessen und wirksam einhält. Dabei ist, soweit anwendbar, insb. einzugehen auf

1. das IKT-Risikomanagement gemäß Artikel 5 bis 14 und 16 DORA,
2. die Dokumentation des IKT-Risikomanagementrahmens gemäß Artikel 6 Abs. 5 Satz 1 oder Artikel 16 Abs. 2 Satz 1 DORA,
3. die IKT-Geschäftsfortführungsleitlinie nach Artikel 11 Abs. 1 Satz 1 DORA,
4. die Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle gemäß Artikel 17 bis 19 DORA,
5. das Testen der digitalen operationalen Resilienz gemäß Artikel 24 und 25 DORA,
6. das Management des IKT-Drittparteienrisikos gemäß Artikel 28 bis 30 DORA und
7. die Einhaltung der Meldepflicht in Bezug auf Vereinbarungen über den Austausch von Informationen gemäß Artikel 45 Abs. 3 DORA.

Die aufsichtlichen Vorgaben dürfen zu Sachgebieten zusammengefasst werden; dabei ist den Grundsätzen der Transparenz und Lesbarkeit des Berichts Rechnung zu tragen.

53 Beziehen sich die Aussagen des Abschlussprüfers zu aufsichtlichen Anforderungen an das beaufsichtigte Finanzunternehmen auf vom Berichtsstichtag abweichende Stichtage bzw. Berichtszeiträume, sind diese anzugeben.

3.2. Allgemeine Berichtsangaben

54 Der Abschlussprüfer hat in seiner Berichterstattung darauf hinzuweisen, dass die gesetzlichen Vertreter des beaufsichtigten Finanzunternehmens die Verantwortung für die Einhaltung der aufsichtlichen Anforderungen sowie für die Richtigkeit und Vollständigkeit der dem Abschlussprüfer erteilten Auskünfte und Erläuterungen sowie zur Verfügung gestellten Unterlagen tragen. Der Abschlussprüfer hat zudem darauf hinzuweisen, dass er die Aufgabe hat, die erteilten Auskünfte und Erläuterungen sowie die zur Verfügung gestellten Unterlagen im Rahmen seiner Tätigkeiten aufgrund aufsichtlicher Vorgaben zu berücksichtigen und zu würdigen.

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

56 Der Abschlussprüfer hat zur Erläuterung von Art und Umfang der Aufsichtlichen DORA-Prüfung die Grundsätze zu nennen, nach denen diese durchgeführt wurde *(IDW EPS 528 (08.2025))*.

57 Der Abschlussprüfer hat i.S. einer allgemeinen Erläuterung auch auf Merkmale des Finanzunternehmens (vgl. Anlage) einzugehen, die für aufsichtliche Anforderungen übergreifend prägend sind. Eine Darstellung der Prozesse, Regelungen und Verfahren des beaufsichtigten Finanzunternehmens zur Einhaltung aufsichtlicher DORA-Anforderungen ist notwendig, soweit dies gemäß der aufsichtlichen Vorgabe ausdrücklich vorgesehen oder zum Verständnis der aus der Tätigkeit des Abschlussprüfers getroffenen Prüfungsfeststellungen erforderlich ist. Dies gilt sowohl für positive Prüfungsfeststellungen als auch im Falle von Beanstandungen von Mängeln.

A57 *Die Erläuterungen dienen dazu, den Adressaten in die Lage zu versetzen, Konsequenzen für die eigene Überwachungsaufgabe zu ziehen.*

58 Der Abschlussprüfer hat – sofern dies nach einer entsprechenden Prüfungsberichtsverordnung vorgeschrieben ist – Beanstandungen zu klassifizieren.

59 Der Abschlussprüfer hat bei der Berichterstattung im Rahmen einer Prüfung in einer Zusammenfassenden Schlussbemerkung zu allen wichtigen Fragen bzw. wesentlichen Aspekten der Prüfung Stellung zu nehmen (vgl. § 7 Abs. 1 PrüfbV, § 8 Abs. 2 WpIPrüfbV, § 6 ZahlPrüfbV, § 44 Abs. 1 Nr. 2 PrüfV sowie § 5 Abs. 1 und § 26 Abs. 2 KAPrüfbV). Im Prüfungsbericht sind die Maßnahmen zur Beseitigung der bei der letzten Aufsichtlichen DORA-Prüfung festgestellten Mängel zu beurteilen. Gleiches gilt für Maßnahmen zur Beseitigung von Mängeln, die bei Sonderprüfungen (vgl. Tz. 22) festgestellt wurden, soweit diese regulatorische Anforderungen betreffen, zu denen der Abschlussprüfer nach den aufsichtlichen Vorgaben (vgl. Tz. 3 sowie jeweils erlassene Prüfungsberichtsverordnung) Feststellungen zu treffen hat. Über die Mängel ist in den Folgejahren so lange zu berichten, bis sie beseitigt wurden.

A59.1 *Ab wann ein Mangel als beseitigt anzusehen ist, kann von der Art des Mangels abhängen und unterliegt der Würdigung im jeweiligen konkreten Sachzusammenhang. Die Ausübung des pflichtgemäßen Ermessens des Wirtschaftsprüfers kann an folgenden Beispielen verdeutlicht werden:*

- *Manche Mängel können ihrer Art nach nicht behoben werden (z.B. Unterlassen einer termingebundenen Tätigkeit). Teilweise kann die Berichterstattung über die Mängelverfolgung darin bestehen, darzulegen, dass das Versäumte nachgeholt worden ist (z.B. eine Nachmeldung). In anderen Fällen lässt sich das Versäumte nicht mehr nachholen (z.B. temporärer oder dauerhafter Ausfall des Protokollierungs-Tools für Administratoren, Rücksicherung der Datensicherung direkt in die Produktion anstatt in die Testumgebung). In diesem Fall ist eine weitere Berichterstattung entbehrlich.*
- *Gegebenenfalls können Informations-, Schulungs- oder Personalmaßnahmen angemessene Maßnahmen zur Beseitigung von Mängeln sein.*
- *Wird im Rahmen einer Angemessenheits- und Wirksamkeitsprüfung ein systematischer Mangel festgestellt, so kann dieser als behoben anzusehen sein, wenn die Ursache nachweislich beseitigt und die angepasste Vorgehensweise nachvollziehbar in der operativen Anwendung ist. Eine konzeptionelle Erarbeitung, ein Beschluss oder eine Kommunikation im Hinblick auf eine zukünftige Behebung stellen für sich allein in diesem Fall noch nicht die (vollständige) Ausräumung eines Mangels dar.*

A59.2 *Bei teilweise abgestellten Mängeln kann der Fortschritt bei der Ausräumung im Rahmen einer Folgeklassifizierung berücksichtigt werden.*

60 Über im Berichtszeitraum vollständig beseitigte Mängel ist im Prüfungsbericht auch dann zu berichten, wenn die Beanstandung im Berichtszeitraum erstmals getroffen wurde.

61 Kommt der Abschlussprüfer zu dem Schluss, dass ein Mangel nicht innerhalb eines angemessenen Zeitraums (vollständig) abgestellt wurde, hat er im Falle einer Klassifizierung von Feststellungen (vgl. Tz. 58) in Abhängigkeit von der Bedeutung des Mangels und dem erreichten Grad der Ausräumung abzuwägen, ob dadurch eine höhere Klassifizierung („eskalierte Klassifizierung“ von Beanstandungen) veranlasst ist. In manchen Fällen ist eine zusätzliche Beanstandung aufgrund einer unzureichenden Abarbeitung von Mängeln durch das Finanzunternehmen einschlägig.

62 Auf aufsichtlich „bedeutsame Vorgänge“ i.S. der Prüfungsberichtsverordnungen (vgl. § 4 Abs. 3 PrüfbV, § 3 Abs. 2 Satz 2 ZahlPrüfbV, § 4 Abs. 3 WpIPrüfbV, § 25 Abs. 2 PrüfV, § 3 Abs. 4 KAPrüfbV), die nach dem Berichtsstichtag eingetreten und dem Prüfer bekannt geworden sind, hat der Abschlussprüfer im Bericht einzugehen.

63 Unabhängig von der Darstellung in einer Zusammenfassenden Schlussbemerkung hat der Abschlussprüfer zu würdigen, inwieweit schwerwiegende Verstöße von gesetzlichen Vertretern oder Arbeitnehmern gegen Gesetz, Gesellschaftsvertrag oder Satzung vorliegen, die eine gesonderte Berichterstattung gemäß § 321 Abs. 1 Satz 3 HGB erforderlich machen.[10]

3.3. Besondere Berichtsangaben

64 Die Berichterstattung zur Organisationsprüfung umfasst die folgenden Elemente:

a. Benennung der ggf. nach Sachgebieten zusammengefassten aufsichtlichen Anforderungen an das beaufsichtigte Finanzunternehmen

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

c. Angabe der Prüfungsfeststellungen (zur Klassifizierung vgl. Tz. 58).

A64 *Eine Auflistung oder nur reine Wiedergabe aufsichtlicher Anforderungen ist weder erforderlich noch sinnvoll.*

3.4. Kommunikation mit dem beaufsichtigten Finanzunternehmen

65 Anlässlich der mündlichen Berichterstattung an das Aufsichtsorgan im Rahmen der Abschlussprüfung des Finanzunternehmens hat der Abschlussprüfer zumindest auf die bedeutsamen Prüfungsfeststellungen in der Zusammenfassenden Schlussbemerkung i.S. der Prüfungsberichtsverordnungen einzugehen.

A65 *Die Berichterstattung dient auch dazu, das Aufsichtsorgan in die Lage zu versetzen, sich ein eigenes Bild von der Einhaltung der aufsichtlichen Anforderungen durch das beaufsichtigte*

[10] Vgl. *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Erstellung von Prüfungsberichten (IDW PS 450 n.F. (10.2021))* (Stand: 12.03.2025), Tz. 48 ff.

Finanzunternehmen zu machen. Der Abschlussprüfer unterstützt das Aufsichtsorgan damit bei der Wahrnehmung seiner Überwachungsfunktion.

3.5. Besondere Redepflicht gegenüber den Aufsichtsbehörden

66 Der Abschlussprüfer hat bei Aufsichtlichen Prüfungen eine besondere Redepflicht zu beachten, wenn ihm Tatsachen bekannt werden, die schwerwiegende Verstöße gegen aufsichtliche Anforderungen darstellen, deren Einhaltung Gegenstand der Tätigkeit des Abschlussprüfers ist, oder wenn er bei der Durchführung behindert wird.[11]

67 Im Rahmen der besonderen Redepflicht sind ungeachtet der allgemeinen aufsichtlichen Berichtspflichten die betreffenden Sachverhalte zu erläutern und sich hieraus ergebende wesentliche Konsequenzen aufzuzeigen. Auf etwaige Unwägbarkeiten hat der Abschlussprüfer dabei einzugehen.

A67.1 *Neben Einschätzungsrisiken können Unwägbarkeiten aus fehlender oder beschränkter Informationsbereitstellung bestehen.*

A67.2 *Bei Verdachtsfällen bzgl. bewusster Verstöße gegen aufsichtliche Anforderungen oder sonstige Normen durch das beaufsichtigte Finanzunternehmens können Redepflichten des Abschlussprüfers entstehen. Aufgrund der Vorgaben ist die gesetzliche Redepflicht unverzüglich, d.h. vor Abschluss der Aufsichtlichen Prüfung, i.d.R. schriftlich gegenüber der Aufsichtsbehörde (z.B. BaFin und ggf. zuständige Hauptverwaltung der Deutschen Bundesbank) auszuüben. In Zweifelsfragen bzw. bei besonders schwerwiegenden oder eilbedürftigen Tatbeständen kann eine mündliche Vorababstimmung bzw. Vorabinformation erforderlich sein, um die seitens der Aufsichtsbehörde ggf. erforderlichen Maßnahmen zur Beseitigung von drohenden Gefahren oder Missständen ohne großen Zeitverlust einleiten zu können.*

[11] Vgl. u.a. § 29 Abs. 3 KWG, § 24 Abs. 2 ZAG, § 78 Abs. 3 WpIG, § 40 Abs. 2 KMAG, § 35 Abs. 4 VAG, § 38 Abs. 3 Satz 3 Nr. 9 KAGB, § 121 Abs. 3 Satz 5 KAGB, § 136 Abs. 3 Satz 5 KAGB bzw. Artikel 12 Abs. 1 Verordnung (EU) Nr. 537/2014.

Anlage – Indikatoren

Artikel 4 DORA sieht den Grundsatz der Verhältnismäßigkeit (Proportionality principle) vor. Nach Artikel 4 Abs. 1 DORA wenden die Finanzunternehmen die in Kapitel II (Artikel 5 bis 16 DORA) festgelegten Vorschriften im Einklang mit dem Grundsatz der Verhältnismäßigkeit an, wobei ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte Rechnung zu tragen ist. Darüber hinaus muss gemäß Artikel 4 Abs. 2 DORA die Anwendung der Kapitel III (Artikel 17 bis 23 DORA) und IV (Artikel 24 bis 27 DORA) sowie des Kapitels V Abschn. I (Artikel 28 bis 30 DORA) der DORA durch die Finanzunternehmen in einem angemessenen Verhältnis zu ihrer Größe und ihrem Gesamtrisikoprofil sowie zu der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte stehen, wie dies in den einschlägigen Vorschriften jener Kapitel ausdrücklich vorgesehen ist.

Für das Management des IKT-Drittparteienrisiko konkretisiert Artikel 28 Abs. 1 Buchst. b DORA zudem, dass das Finanzunternehmen dem Grundsatz der Verhältnismäßigkeit Rechnung trägt, wobei Folgendes zu berücksichtigen ist:

- die Art, das Ausmaß, die Komplexität und die Relevanz IKT-bezogener Abhängigkeiten,
- die Risiken infolge vertraglicher Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die mit IKT-Drittdienstleistern geschlossen wurden, wobei die Kritikalität oder Relevanz der jeweiligen Dienstleistungen, Prozesse oder Funktionen sowie die potenziellen Auswirkungen auf die Kontinuität und Verfügbarkeit von Finanzdienstleistungen und -tätigkeiten auf Einzel- und Gruppenebene zu berücksichtigen sind.

Ausgehend von dem in den Prüfungsberichtsverordnungen (vgl. insb. § 3 PrüfbV, § 2 Abs. 2 ZahlPrüfbV, § 3 WpIPrüfbV und § 2 Abs. 2 KAPrüfbV) verankerten Grundsatz der Proportionalität wurde beispielhaft nachfolgender Indikatorenkatalog für die vier Oberkriterien (Größe, Geschäftsumfang, Komplexität, Risikogehalt) erarbeitet. Zur Abrundung wurde ein weiteres Kriterium „Weitere übergeordnete Eigenschaften des Finanzunternehmens eingefügt. Die Risiko- und Wesentlichkeitseinschätzungen des Abschlussprüfers anhand geeigneter Indikatoren dienen als Basis für die Aufsichtliche DORA-Prüfung und beeinflussen u.a. die Prüfungsintensität (vgl. Tz. 27).

	Prinzip der Proportionalität
Umsetzung des Proportionalitätsbegriffs aus den Prüfungsberichtsverordnungen	**Proportionalität: Angemessenheit der Umsetzung der organisatorischen Vorkehrungen auf Ebene des Finanzunternehmens**
Betriebenes Geschäft	Übergreifend: Welche Auswirkungen ergeben sich aus den Dienstleistungen, Tätigkeiten und Geschäften des Finanzunternehmens in Bezug auf die Umsetzung der DORA-Anforderungen? ● Art des betriebenen Geschäfts (Produkte und Operating Model)

	● Kundengruppen (Retail und/oder Commercial, B2C/B2B) ● Monetäres Volumen wesentlicher KPIs ● Anzahl der Geschäftstransaktionen und Transaktionsgeschwindigkeit
Umfang/Organisation	● Komplexität der Geschäftsorganisation (Anzahl Gesellschaften, Shared Servicecenter, lokale oder globale Organisation) ● Grad der Nutzung von IKT-Drittdienstleistern (konzerninterne Servicegesellschaft, externe Services sowie Nutzung von Cloud Services) ● Organisation der IKT (Verortung in der Gesamtorganisation, aufbauorganisatorische Gliederung, organisatorische Zuordnung des Information Systems Officer (CISO)) ● Ablauforganisation (z.B. agile Organisation, DevOps etc.) ● Volumen (ausreichende Kapazitäten) ● Anzahl der Transaktionen ● Transaktionsfrequenz
Komplexität der Infrastruktur	● Anzahl/Art der Technologien (Hardware, Betriebssysteme, Datenbanken, Programmiersprachen) ● Komplexität der Anwendungslandschaft (redundante Systeme, Anteil Host-basierter Systeme, Eigenentwicklungen vs. Standardsoftware) ● Projektlandschaft (Änderungshäufigkeit, Decommissioning-Programme) ● Alter der Systeme/Infrastruktur (Wartung vorhanden) ● Die IT-Systeme werden zentral oder dezentral betrieben
Risikogehalt	● Risiken aus der Mitarbeiterstruktur in der IKT (Alter, Know-how, Weiterbildungen) und Anzahl sowie Anteil an der Gesamtbelegschaft ● Fluktuation auf Führungspositionen in der IKT ● Anzahl abgebrochener Projekte im Verhältnis zu allen Projekten (nach Größenclustern) ● Auffälligkeiten hinsichtlich Systemausfälle, Incidents, Data breaches, Cyberangriffe etc. ● Hinweise auf Verstöße aus internen und externen Prüfungen ● IKT-Risiken
Größe des Finanzunternehmens	● Die (reine) Größe wirkt häufig indirekt über die anderen Indikatoren, z.B. Komplexität ● Angemessene IKT-Ausstattung in Bezug auf die Größe/Geschäftsfelder/Kundengruppen/Produkte des Finanzunternehmens

Weitere übergeordnete Eigenschaften des Finanzunternehmens	● Qualität der IKT ● Hinweise auf Verstöße, z.B. Beanstandungen aus internen oder externen Prüfungen ● Anfälligkeit für Datenmanipulation und Datendiebstahl ● Häufige Organisationsänderungen ● Häufige Ressourcenengpässe ● Hoher Turnover bei Schlüsselpositionen ● Häufiger Wechsel bei der Kontrollfunktion