GDV Gesamtverband der Versicherer

STELLUNGNAHME

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zum 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 (IDW EPS 528 (08.2025))

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Telefon: +49 30 2020-5000 · Telefax: +49 30 2020-6000
Lobbyregister-Nr. R000774

Rue du Champ de Mars 23, B-1050 Brüssel
Telefon: +32 2 28247-30 · Telefax: +49 30 2020-6140
ID-Nummer 6437280268-55
www.gdv.de

Ansprechpartner
Rechnungslegung/Risikomanagement/Revision

E-Mail
rechnungslegung@gdv.de

Inhalt

1.1 Berücksichtigung von Änderungen der Prüfungsberichteverordnungen ..4
1.2 Bindung an aufsichtsrechtliche Anforderungen ..4
1.3 Klare Abgrenzung von Aufsichtlicher DORA-Prüfung und Abschlussprüfung ..5
1.4 Begriffsdefinitionen und Systematik an DORA anpassen ..5
1.5 Risikoorientierten Ansatz stärken ..6

Einleitung

Eine Prüfpflicht zur Einhaltung der Anforderungen des „Digital Operational Resilience Act“ (DORA-VO) ist in der europäischen DORA-VO nicht verankert. Mit dem Finanzmarktdigitalisierungsgesetz (FinmadiG) wurde unter anderem für Versicherungsunternehmen die Prüfung von bestimmten DORA-Anforderungen durch den Abschlussprüfer als Erweiterung der Jahresabschlussprüfung in § 35 Abs. 1 Satz 1 Nr. 10 VAG auf rein nationaler Ebene eingeführt. Die Übergangsvorschriften zum FinmadiG sehen vor, dass diese Prüfungspflicht erstmals für ein nach dem 31.12.2024 beginnendes Geschäftsjahr Anwendung findet.

Der Bankenfachausschuss (BFA), der Versicherungsfachausschuss (VFA) sowie der Fachausschuss Investment (FAIN) haben am 7. August 2025 den Entwurf eines branchenübergreifenden IDW Prüfungsstandards für eine Aufsichtliche DORA-Prüfung (IDW EPS 528 (08.2025)) verabschiedet. Der Standardentwurf basiert auf den in IDW PS 526 (10.2023) dargestellten einschlägigen Anforderungen an die Durchführung Aufsichtlicher Prüfungen im Rahmen der Abschlussprüfung.

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) legt in diesem Entwurf eines IDW Prüfungsstandards die Berufsauffassung dar, nach welchen Grundsätzen Abschlussprüfer unbeschadet ihrer Eigenverantwortlichkeit eine Prüfung von DORA-Anforderungen bei den betroffenen Finanzunternehmen durchführen und über diese Prüfung berichten (Aufsichtliche DORA Prüfung). Der vorliegende Standardentwurf legt 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. Er soll erstmals für Aufsichtliche DORA-Prüfungen in Bezug auf Berichtszeiträume, die nach dem 31.12.2024 beginnen, mit der Ausnahme von Rumpfgeschäftsjahren, die vor dem 31.12.2025 enden, angewendet werden.

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) ist die Dachorganisation der Versicherer in Deutschland. Die beiliegende Stellungnahme zum vorliegenden branchenübergreifenden Entwurf eines IDW Prüfungsstandards spiegelt die Anliegen der Mitglieder aus der Versicherungsbranche wider.

Kernanliegen

1.1 Berücksichtigung von Änderungen der Prüfungsberichteverordnungen

Bezüglich des Zeitpunkts der Veröffentlichung des Entwurfs sieht der Verband kritisch, dass die jeweiligen Prüfungsberichtsverordnungen (PrüfbV, ZahlPrüfbV, WpIPrüfbV, PrüfV und KAPrüfbV) der einzelnen Finanzunternehmen bislang nicht an die neuen Prüfungsvorgaben der DORA-Anforderungen angepasst wurden. Wie der Entwurf in Rz. 7 richtigerweise klarstellt, sehen die Prüfungsberichtsverordnungen von Finanzunternehmen, *„bei denen die IT-Systeme bereits nach der Rechtslage vor Inkrafttreten des FinmadiG Gegenstand der aufsichtlichen Prüfungen sind“*, branchenübergreifend vor, *„dass der Abschlussprüfer verpflichtet ist, insbesondere 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).“* Damit gelten die Prüfungsberichteverordnungen auch bereits vor dem Inkrafttreten der DORA, berücksichtigen diese also noch nicht. Dies wäre jedoch zwingend Voraussetzung für die Erarbeitung eines IDW Prüfungsstandard innerhalb einer einheitlichen Rechtsordnung. So bestehen Inkonsistenzen innerhalb der Systematik und Begrifflichkeiten (vgl. dazu auch Nr. 1.4). **Der Verband würde eine Klarstellung in Rz. 7 befürworten, dass bisher fehlende Anpassungen in den Prüfungsberichterverordnungen Änderungen an dem Prüfungsstandard erfordern oder ein abweichendes Prüfungsvorgehen rechtfertigen können.**

1.2 Bindung an aufsichtsrechtliche Anforderungen

Die Definition „Aufsichtliche Anforderung“ in Tz. 11 lit a), nach der eine *„durch Gesetz, Verordnung, Richtlinie, eine anderweitige Rechtsnorm oder durch eine Verlautbarung einer nationalen oder europäischen Aufsichtsbehörde konkretisierte Verpflichtung eines beaufsichtigten Finanzunternehmens, eine dort bezeichnete aufsichtliche Regelung einzuhalten“* ist, ist zu weitgehend. **Die Verlautbarungen einer nationalen oder europäischen Aufsichtsbehörde dürften nur insoweit berücksichtigt werden, wie sie sich unmittelbar und zwingend aus einer Rechtsgrundlage ableiten lassen und an die Versicherungsunternehmen adressiert und von diesen verbindlich zu berücksichtigen sind.** Dies ist beispielsweise für europäische Opinions der EIOPA, die sich an die nationalen Aufsichtsbehörden richten, oder unverbindliche Orientierungshilfen der BaFin nicht gegeben. So stellt beispielsweise die seitens der BaFin zur Verfügung gestellte Übersicht der Dokumentationsanforderungen nach DORA eine Hilfestellung für die Unternehmen dar, sie ist aber nicht verbindlich. Dies sollte klargestellt werden.

1.3 Klare Abgrenzung von Aufsichtlicher DORA-Prüfung und Abschlussprüfung

Aus Sicht der geprüften Unternehmen ist es wichtig, im Rahmen der Dokumentenanforderung und ggf. vertiefender Prüfungshandlungen klar zwischen der Aufsichtlichen Prüfung gemäß § 35 Nr. 10 DORA und der Abschlussprüfung zu unterscheiden. Es sollte im Rahmen der Dokumentenanforderung, bei Gesprächen und Prüfungshandlungen immer deutlich kommuniziert werden, innerhalb welcher Prüfung die Aktivitäten stattfinden. Angesichts der getrennt auszuweisenden Prüfungsergebnisse dürfte dies auch für die Prüfer wünschenswert sein. **Das Unterscheidungserfordernis könnte in Rz. 14 bzw. Rz. 31 verankert werden.**

1.4 Begriffsdefinitionen und Systematik an DORA anpassen

Im Hinblick auf die Organisationsprüfung soll für die Würdigung des Soll-Objekts gemäß Rz. A29.1 gelten: *„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.“*

Weiter wird in der Berichterstattung gemäß Rz. 52 gefordert: *„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.“*

Der GDV begrüßt grundsätzlich einen Ansatz, der risikoorientiert nur ausgewählte Elemente in die Prüfung und Berichterstattung einbeziehen möchte. Allerdings sind „wesentliche Geschäftsprozesse“ in der DORA-Verordnung weder genannt noch definiert. Insofern besteht die Gefahr, dass eine über die DORA-Verordnung hinausgehende Konkretisierung bzw. Klarstellung erforderlich ist, um eine uneinheitliche Umsetzung zu vermeiden. Die DORA spricht zudem an keiner von *„IKT-Systemen, die wesentliche Geschäftsprozesse unterstützen“* oder von der *„Sicherstellung der Integrität Vertraulichkeit, Authentizität und Verfügbarkeit der IKT-Systeme, die wesentliche Geschäftsprozesse unterstützen oder aufsichtsrechtlich relevante Daten verarbeiten*“.

Dagegen ist in Art. 3 Nr. 22 der DORA-Verordnung die „kritische oder wichtige Funktion“ bereits definiert. Demnach handelt es sich um eine Funktion *„deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene*

Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde." Der europäische Gesetzgeber hat hier also bereits eine risikoorientierte Kategorie geschaffen und die entsprechende Definition verankert. Auf diesem Wortlaut dürfte die schriftlich fixierte Ordnung sämtlicher Versicherungsunternehmen aufbauen und daran dürften dann auch die praktischen Umsetzungsmaßnahmen ausgerichtet sein. **Der Prüfungsstandard sollte daher diese legislative Systematik der DORA-Verordnung übernehmen und statt auf „wesentliche Geschäftsprozesse" ebenfalls auf „kritische oder wichtige Funktionen" verweisen.**

Hinsichtlich der ebenfalls enthaltenen Anforderung im Hinblick auf *„aufsichtsrechtlich relevante Daten"* besteht eine Redundanz zu § 7 Abs. 1 PrüfV. Hier hat der Prüfer bereits zu darzustellen und zu beurteilen *„[…],ob die organisatorischen, personellen und technischen Vorkehrungen zur Sicherstellung der Integrität, Authentizität und Verfügbarkeit der aufsichtlich relevanten Daten angemessen sind und wirksam umgesetzt werden.*" Dagegen kennt DORA den Terminus der „aufsichtsrechtlich relevanten Daten" ebenfalls nicht. **Der Verband empfiehlt, den Verweis auf aufsichtsrechtlich relevante Daten im vorliegenden Prüfungsstandard zu streichen.**

Weiter wird in Rz. A36.1 als mögliche Prüfungshandlung ausgeführt *„Einsichtnahme in den Bericht zur Überprüfung des IKT-Risikomanagementrahmens der Kontrollfunktion"*. Der maßgebliche Art. 6 Abs. 5 DORA schreibt zwar die Überprüfung und Dokumentation vor, lässt aber offen, wer diese durchzuführen hat. Unter Berücksichtigung der Funktionstrennung wird die Verantwortlichkeit voraussichtlich unterschiedlich in den Unternehmen festgelegt werden. **Der Verband empfiehlt, den Zusatz *„der Kontrollfunktion"* zu streichen.**

1.5 Risikoorientierten Ansatz stärken

Gemäß Rz. A36.4 kann *„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, 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."* **Der Verband begrüßt die Möglichkeit des Rückgriffs auf Ergebnisse vorausgegangener Prüfungen als Ausprägung eines risikoorientierten Prüfungsansatzes, empfiehlt jedoch den Turnus zu erhöhen (z. B. auf fünf Jahre). Dies würde es den Prüfer ermöglichen, sich auf besonders risikoreiche oder wesentlich veränderte Prüfungsfelder zu fokussieren und so den risikoorientierten Prüfungsansatz zu stärken.**

Berlin, den 31.10.2025