GRM Global Regulation Management AG
Baarerstraße 52 | 6300 Zug | Switzerland

Institut der Wirtschaftsprüfer in Deutschland e.V.
Roßstraße 74
40476 Düsseldorf
Vorab per E-Mai an antje.coenen@idw.de

**Dr. Waldemar Grudzien**
Managing Director
Mobil: +49 160 4799964
wgr@globalregulation.com

**Julius Düwel**
Managing Director
Mobil: +49 151 11847321
jdu@globalregulation.com

**Paul Friedrich**
Managing Director
Mobil: +41 798 488477
pfr@globalregulation.com

www.globalregulation.com

Berlin, 31.10.2025

**STELLUNGNAHME ZUM ENTWURF IDW EPS 528 (08.2025)**

Sehr geehrte Frau Coenen,
sehr geehrter Herr Groove,

bitte finden Sie anbei unsere Stellungnahme 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 (Aufsichtliche DORA-Prüfung im Rahmen der Abschlussprüfung) (IDW EPS 528 (08.2025))“.

Zusammenfassend schlagen wir zwei Erweiterungen zu Ihrem Entwurf vor:

1) Eineindeutige Trennung Ihrer genannten Beispiele der Evidenzen für Angemessenheitsprüfungen und Wirksamkeitsprüfungen sowie
2) die Einführung von Evidenzen für Implementierungsprüfungen als Teststufe zwischen Angemessenheitsprüfungen und Wirksamkeitsprüfungen.

Mit diesen Änderungen wird erstens eine eineindeutige und widerspruchsfreie Klassifizierung von Prüfungshandlungen der Angemessenheits- und Wirksamkeitsprüfungen ermöglicht. Zweitens wird das Evidenzwesen an das im Finanzsektor bewährte ToX-3LoD-System angepasst (siehe Abbildung 1):

- ToX steht dabei für die drei Teststufen Test of Design (Angemessenheitsnachweis), Test of Implementation (Implementierungsnachweis) und Test of Effectiveness (Wirksamkeitsnachweis),
- 3LoD steht für die drei Verteidigungslinien (Three Lines of Defence) mit 1st Line als Implementierer, 2nd Line als Regelsetzer und 3rd Line als Interne Revision.

**Zusammenspiel der Teststufen mit den drei Verteidigungslinien**

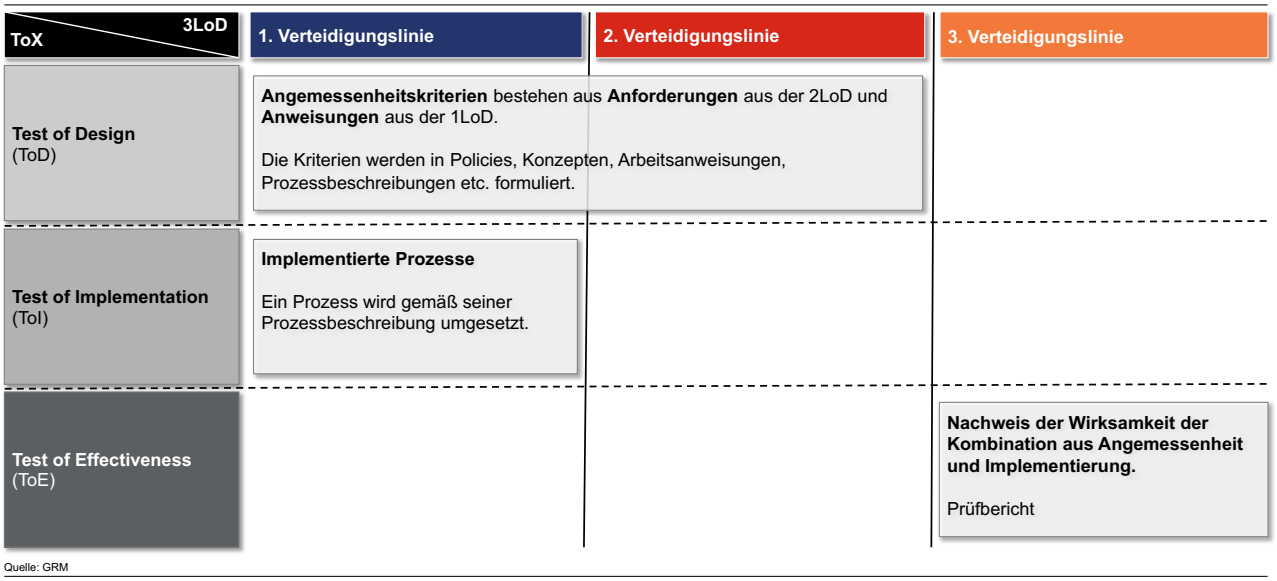


Abbildung 1: ToX-3LoD-System

Zur eindeutigen Trennung der Evidenzen

In der nachfolgenden Tabelle sind die Evidenzen Ihres Entwurfs zusammengestellt. Zur einfachen Navigation sind die Einträge nummeriert und mit ToD resp. ToE abgekürzt. Da im Test of Design einzig die Entwurfskriterien geprüft werden, sind die Einträge ToD-1, ToD-3, ToD-4 und ToD-5 zu Test of Effectiveness hinzuzurechnen. Der Eintrag ToE-3 ist zweideutig beschrieben und könnte durch den Ausdruck „Vorkehrung“ im Sinne von Entwurf auch ToD zugeordnet werden. Auf der Wirksamkeitsseite enthält der Eintrag ToE-2 mit den IKT-Drittparteienverträgen eine ToD-Komponente.

| Nr. | Angemessenheitsprüfung (ToD) | Wirksamkeitsprüfung (ToE) |
|---|---|---|
| 1 | Befragungen (bspw. des für die Kontrollfunktion Verantwortlichen, der Internen Revision, von Mitarbeitern aus relevanten operativen Bereichen) | 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 |
| 2 | 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 | Durchsicht von Unterlagen (z.B. Risikoanalysen, IKT-Drittparteienverträge, Pentestberichte, IT-Notfalltests), die die Durchführung von Prozessen, Regelungen und Verfahren dokumentieren |
| 3 | 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) | Nachvollzug von Prozessabläufen der organisatorischen Vorkehrungen zur Einhaltung der DORA-Anforderungen einschließlich Qualitätssicherungsmaßnahmen |
| 4 | Einsichtnahme am System (z.B. um die Kritikalitätseinstufung der IKT-Assets im Asset-Inventar | Nachvollzug von Tätigkeiten zur Einhaltung der DORA-Anforderungen (insb. in Bezug auf die |

| Nr. | Angemessenheitsprüfung (ToD) | Wirksamkeitsprüfung (ToE) |
|---|---|---|
| | oder Authentifizierungsmechanismen im Active Directory nachzuvollziehen) | Festlegung der kritischen oder wichtigen Funktionen des Finanzunternehmens und der daraus abgeleiteten Maßnahmen) |
| **5** | Einsichtnahme in Berichte der zweiten und dritten Verteidigungslinie (z.B. zentrales Auslagerungsmanagement, Bericht zur Überprüfung des IKT-Risikomanagementrahmens und Berichte der Internen Revision) | Einsichtnahme in den Bericht zur Überprüfung des IKT-Risikomanagementrahmens der Kontrollfunktion |
| **6** | | 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) |
| **7** | | Einsichtnahme in die Prüfungsdokumentation der Internen Revision |

Abbildung 1: Einführung von Evidenzen für Implementierungsprüfungen

Zur Einführung von Evidenzen für Implementierungsprüfungen

Die Erweiterung des Evidenzrahmens um Evidenzen der Implementierung für die Teststufe ToI ermöglicht eine direkte Anlehnung an das ToX-3LoD-System und verschafft einer Organisation eine vollständige, widerspruchsfreie und sich gegenseitig ausschließende Menge an Evidenzen.

Bezogen auf Ihre Evidenzen aus dem Entwurf wären die Anteile Risikoanalysen und IT-Notfalltests des Eintrags ToE-2 Evidenzen der Teststufe ToI.

Zusammenführung beider Erweiterungen

Die Einhaltung einer strikten Abgrenzung der Prüfungshandlungen und Evidenzen zu ToD, ToI und ToE ist genauso wichtig für die Gesamtfunktion des ToX-3LoD-Systems wie die Abgrenzung der Aufgaben der drei Verteidigungslinien.

Eine Vermischung führt zu Unsauberkeiten, Widersprüchen und Erschwernissen durch falsche Zuordnung von Prüfungshandlungen und Evidenzen sowie fortfolgend zu Fehlern in die Kontrollen der Verteidigungslinien hinein.

Die unbedingte Einhaltung der beschriebenen Zuordnung und Reihenfolge verdeutlicht Abbildung 2. Die Abbildung enthält zur Vollständigkeit auch die vierte Verteidigungslinie. Diese befindet sich außerhalb der Organisation und wird für die Zwecke unserer Ausführungen nicht beachtet. Mit dieser eindeutigen Trennung der Prüfungshandlungen in ToD, ToI und ToE können Planung, Durchführung und Rechenschaft eines Managementsystems (ISMS nach ISO/IEC 27001, DSMS nach ISO/IEC 27701, IKT-Risikorahmen nach DORA, BCM nach ISO/IEC 3301 etc.) besser erreicht werden, da jede Verteidigungslinie zu jedem Umsetzungsstand und Zeitpunkt die volle Transparenz über ihre Aufgaben, Prozesse und Lieferobjekte hat.

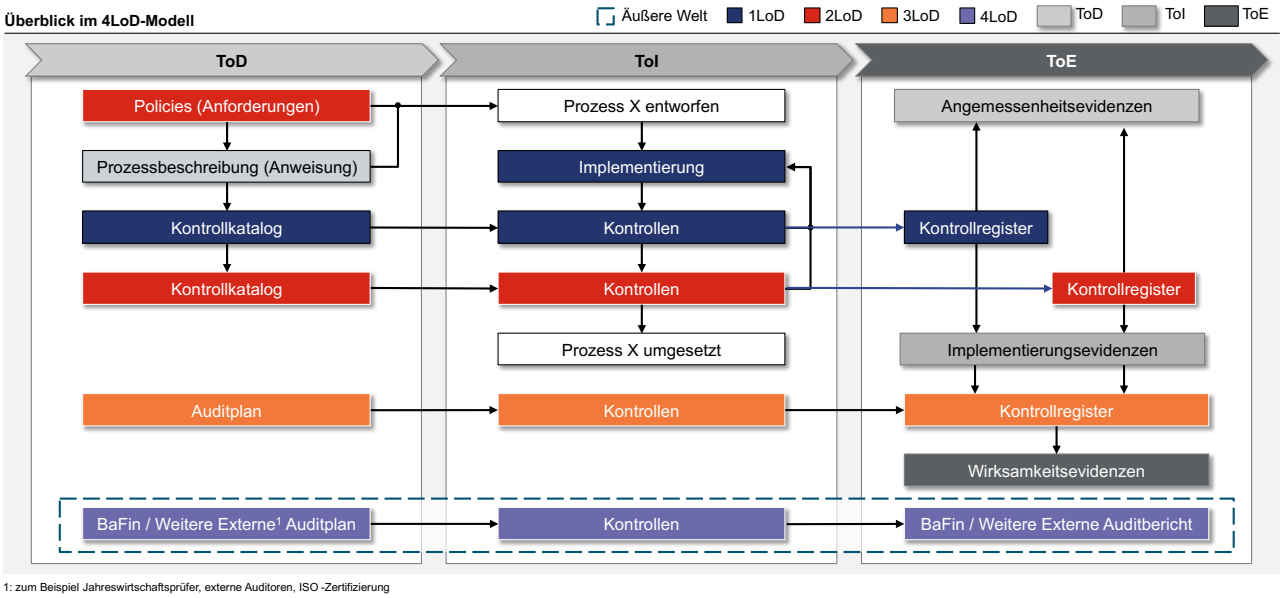


Abbildung 2: Entwurf, Implementierung und Effektivität im ToX-4LoD-System

Unserer Auffassung nach würden diese zwei Erweiterungen die Anwendbarkeit Ihres Prüfungsstandards wertstiftend verbessern. Dem IDW als viel beachtetem Leitmedium der Prüfungslandschaft kommt eine entscheidende Rolle bei der Prüfungskette zu. Eine von Beginn an korrekt verstandene Prüfungsnomenklatur- und -klassifikation der Prüfungshandlungen und damit verbundener Evidenzen kommt eine erfolgskritische Rolle zu. Eine Erweiterung Ihres Prüfstandards erfordert auch Anpassungen an diversen Textziffern in Ihrem Entwurf. Wir stehen Ihnen für diese Arbeiten gerne zur Verfügung und regen die Vorstellung unserer Erfahrungen in einem persönlichen Gespräch an, um weitergehende Informationen bereitstellen zu können.

Ihr Verständnis voraussetzend, wird unser Sekretariat einen circa einstündigen Termin anfragen.

Mit freundlichen Grüßen

Dr. Waldemar Grudzien

Paul Friedrich