Prof. Dr. Andreas Igl
TH Deggendorf

Betriebserlaubnis für den IKT-Risikomanagementrahmen: Die Validierungspflicht nach DORA in Methodik und Praxis

Deggendorfer Notiz 2026/07 | 23. April 2026

Die Notiz analysiert die regulatorischen Anforderungen an die Überprüfung des IKT-Risikomanagementrahmens nach DORA und deren prüfungspraktische Umsetzung. Im Mittelpunkt steht Art. 6 Abs. 5 DORA, der eine mindestjährliche Validierung durch die IKT-Kontrollfunktion sowie die Vorlage eines strukturierten Berichts gegenüber dem Leitungsorgan und auf Anforderungen gegenüber der Aufsicht verbindlich normiert. Eine Analogie zur technischen Hauptuntersuchung verdeutlicht die Prüflogik: Von der Vollständigkeitsprüfung zur substanziellen Funktionsprüfung. Frühe Prüfungserfahrungen offenbaren typische Defizite in Berichtsfristen, Leitungsorganbefassung und Ressourcenausstattung der IKT-Kontrollfunktion – besonders ausgeprägt im genossenschaftlichen Sektor und bei Sparkassen.

1. Eine neue Prüfpflicht entsteht: Die aufsichtliche Einordnung nach DORA

Mit dem Digital Operational Resilience Act (DORA) – der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates – hat der europäische Gesetzgeber einen regulatorischen Rahmen geschaffen, der die digitale operationale Resilienz von Finanzunternehmen erstmals kohärent und sektorübergreifend normiert. Im Mittelpunkt dieser Regulierungsarchitektur steht der IKT-Risikomanagementrahmen, dem eine konstitutive Funktion zukommt: Er bildet das konzeptionelle Fundament für das systematische Management aller IKT-bezogenen Risiken eines Finanzunternehmens und schafft die strukturelle Voraussetzung für ein hohes Maß an digitaler operationaler Widerstandsfähigkeit.

Art. 6 Abs. 1 DORA normiert in diesem Zusammenhang eine weitreichende Verpflichtung. Kreditinstitute und andere vom Anwendungsbereich der Verordnung erfasste Finanzunternehmen sind gehalten, über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen zu verfügen, der vollständig in das institutsweite Gesamtrisikomanagement integriert ist. Die Anforderung beschränkt sich dabei nicht auf die formale Existenz eines solchen Rahmens; verlangt wird vielmehr, dass er das Unternehmen in die Lage versetzt, IKT-Risiken schnell, effizient und umfassend zu adressieren. Die Formulierung des Verordnungstextes lässt keinen Zweifel daran, dass der Gesetzgeber einen

substanziellen, operativ wirksamen Steuerungsmechanismus vor Augen hat – und nicht ein bloßes Dokument zur regulatorischen Pflichterfüllung.

Der inhaltliche Mindestumfang des Rahmens wird durch Art. 6 Abs. 2 DORA präzisiert. Danach sind Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools verbindlich einzubeziehen, sofern diese für den angemessenen Schutz aller Informations- und IKT-Assets erforderlich sind. Dieser Schutzauftrag erstreckt sich ausdrücklich auf Computer-Software, Hardware und Server ebenso wie auf physische Komponenten und Infrastrukturen – darunter Räumlichkeiten, Rechenzentren und ausgewiesene sensible Bereiche. Die Verordnung verfolgt damit einen ganzheitlichen Schutzansatz, der die traditionelle Trennung zwischen physischer Sicherheit und IT-Sicherheit überwindet und eine integrierte Betrachtung des gesamten IKT-Schutzbedarfs einfordert.

Besondere regulatorische Bedeutung erlangt die Regelung zur Überprüfungs- und Dokumentationspflicht in Art. 6 Abs. 5 DORA. Der IKT-Risikomanagementrahmen unterliegt einer mindestjährlichen Überprüfungspflicht; darüber hinaus ist eine Revision anlassbezogen durchzuführen – namentlich nach dem Auftreten schwerwiegender IKT-bezogener Vorfälle sowie nach aufsichtsrechtlichen Anweisungen oder nach Feststellungen aus einschlägigen Tests der digitalen operationalen Resilienz oder aus Auditverfahren. Der Rahmen ist auf Grundlage der bei Umsetzung und Überwachung gewonnenen Erkenntnisse kontinuierlich zu verbessern. Diese Anforderung konstituiert ein dynamisches Regelungskonzept: Der IKT-Risikomanagementrahmen ist kein einmalig erstelltes Dokument, sondern ein lebendes Instrument, das sich an veränderte operative Realitäten und neue Erkenntnisse aus der Praxis anzupassen hat.

Ein zentrales Merkmal des DORA-Regelungskonzepts liegt in der aufsichtlichen Einbindung des Überprüfungsprozesses. Art. 6 Abs. 5 Satz 3 DORA sieht vor, dass der zuständigen Behörde auf deren Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens vorzulegen ist. Diese Berichtspflicht gegenüber der Aufsicht verleiht dem Überprüfungsprozess eine Dimension, die weit über interne Qualitätssicherungsmaßnahmen hinausgeht: Die Ergebnisse der Überprüfung werden zum Gegenstand einer potenziellen aufsichtlichen Würdigung und können Gegenstand nachgelagerter Eingriffsbefugnisse werden. Damit rückt die Qualität des Überprüfungsprozesses selbst in den Fokus der regulatorischen Anforderungen.

Der IKT-Risikomanagementrahmen ist, wie die Verordnung im Gesamtkontext verdeutlicht, weder als isoliertes Regelwerk zu verstehen noch auf seine normative Funktion als Mindestanforderungserfüllung zu reduzieren. Er steht in einem systematischen Zusammenhang mit einer Vielzahl nachgelagerter DORA-Anforderungen: mit den Regeln zur Meldung schwerwiegender IKT-Vorfälle nach Art. 17 ff. DORA, mit den Anforderungen an das Testen der digitalen operationalen Resilienz nach Art. 24 ff. DORA sowie mit dem IKT-Drittparteienrisikomanagement nach Art. 28 ff. DORA. Der Rahmen liefert für diese

Bereiche die konzeptionelle Grundlage und die strategische Ausrichtung; Defizite im Rahmen wirken damit unmittelbar auf die Qualität aller nachgelagerten Prozesse durch.

Ergänzend zur Verordnung selbst hat die Europäische Aufsichtsbehördenarchitektur – bestehend aus EBA, ESMA und EIOPA als gemeinsame Ausschussstruktur – einen umfangreichen Bestand an Level-2-Texten entwickelt, der die Anforderungen der Verordnung operationalisiert. Hervorzuheben sind insbesondere die Delegierten Verordnungen zu den technischen Regulierungsstandards (RTS) sowie die Durchführungsverordnungen zu den technischen Durchführungsstandards (ITS), die Detailregelungen zu Inhalt, Struktur und Ausgestaltung des IKT-Risikomanagementrahmens sowie der zugehörigen Berichtspflichten enthalten. Für die praktische Handhabung des Rahmens sind darüber hinaus die von den europäischen Aufsichtsbehörden veröffentlichten Leitlinien relevant, die zwar formal keine verbindliche Rechtsqualität besitzen, jedoch im Rahmen des aufsichtlichen Comply-or-Explain-Mechanismus faktisch eine erhebliche normative Bindungswirkung entfalten.

Aus prüfungspraktischer Perspektive ist die regulatorische Neuerung durch DORA von erheblicher Relevanz. Mit der Einführung der Überprüfungspflicht nach Art. 6 Abs. 5 DORA entsteht für Finanzunternehmen eine Prüfaufgabe, die in ihrer Ausgestaltung spezifische methodische Anforderungen stellt und sich von klassischen Compliance-Prüfungen in wesentlichen Aspekten unterscheidet. Zu prüfen ist nicht nur, ob ein IKT-Risikomanagementrahmen formal existiert, sondern ob er substanziell wirksam ist, ob er die normativen Mindestanforderungen vollständig erfüllt, ob er in das Gesamtrisikomanagement integriert ist und ob er die dynamischen Anforderungen an eine kontinuierliche Verbesserung erfüllt. Diese mehrdimensionale Prüfaufgabe erfordert eine strukturierte Vorgehensweise, die sowohl den normativen Anforderungsrahmen als auch die operative Realität des jeweiligen Instituts systematisch in den Blick nimmt.

Die nachfolgenden Abschnitte widmen sich der Frage, wie eine solche Überprüfung methodisch konzipiert und praktisch durchgeführt werden kann. Dabei werden sowohl die institutionellen Grundlagen – insbesondere die Rolle der IKT-Kontrollfunktion – als auch die methodischen Instrumente und die Anforderungen an die Berichterstattung in den Mittelpunkt gestellt. Angesichts der frühen Prüfungserfahrungen mit dem DORA-Regime verbleiben zudem offene Fragen, die einer kritischen Würdigung bedürfen.

2. Bekanntes neu gedacht: Die Hauptuntersuchung als Spiegel interner IKT-Prüflogik

Regulatorische Anforderungen gewinnen an praktischer Überzeugungskraft, wenn sie sich in anschaulichen Analogien erschließen lassen. Die Überprüfungspflicht nach Art. 6 Abs. 5 DORA und die damit verbundene Berichterstattung an das Leitungsorgan lassen

sich in ihrer strukturellen Logik treffend mit der technischen Hauptuntersuchung eines Kraftfahrzeugs vergleichen – einem Verfahren, das in seinem Aufbau eine bemerkenswerte Parallele zur IKT-Prüfpraxis aufweist.

Ein Kraftfahrzeug benötigt für den Betrieb im öffentlichen Straßenverkehr eine Betriebserlaubnis, die in regelmäßigen Abständen durch eine fachkundige Prüforganisation erneuert wird. Der Prüfer kombiniert dabei Vollständigkeitsprüfungen – sind alle sicherheitsrelevanten Komponenten vorhanden? – mit Funktionsprüfungen, die überprüfen, ob Bremsen, Lichtanlage und elektronische Systeme ordnungsgemäß arbeiten. Über eine eindeutige Fahrzeugidentifikationsnummer steht dem Prüfer ein lückenloses Inventar aller verbauten Teile zur Verfügung, darunter zahlreiche Komponenten von Drittherstellern, sodass fehlerhaft arbeitende, wartungsbedürftige oder rückrufbetroffene Teile unmittelbar identifiziert werden können. Das Ergebnis dieser Untersuchung mündet in einem kompakten Prüfbericht, der Kernkennzahlen enthält, festgestellte Mängel dokumentiert und konkrete Handlungsempfehlungen formuliert. Dieser Bericht begründet die Betriebserlaubnis für einen definierten Zeitraum und ist dauerhaft mitzuführen.

Die Übertragung dieser Prüflogik auf den IKT-Risikomanagementrahmen ist unmittelbar evident. Die Mitglieder des Leitungsorgans tragen die Gesamtverantwortung dafür, dass der IKT-Risikomanagementrahmen des Instituts seine regulatorische „Betriebserlaubnis" besitzt – das heißt, in seiner Gesamtheit funktionsfähig, wirksam und normkonform ausgestaltet ist. Die Rolle der fachkundigen Prüfinstanz übernimmt die IKT-Kontrollfunktion, die über die methodische Qualifikation und die erforderlichen Ressourcen verfügt, um diese Aufgabe sachgerecht wahrzunehmen. Dabei stützt sie sich auf Vorinformationen aus allen relevanten Teilbereichen des IKT-Risikomanagements – aus dem IKT-Drittparteienmanagement, dem Notfallmanagement, dem Testprogramm zur digitalen operationellen Resilienz sowie aus internen und externen Prüfungen. Die Zusammenführung dieser Informationsquellen ermöglicht nicht nur eine Vollständigkeitskontrolle der einzelnen Rahmenkomponenten, sondern auch eine Beurteilung ihrer wechselseitigen Verzahnung und ihrer Funktionsfähigkeit im Zusammenspiel – eine Dimension, die für die Wirksamkeit des Gesamtrahmens entscheidend ist.

Gemäß Art. 6 Abs. 5 DORA erfolgt die Überprüfung im jährlichen Rhythmus oder anlassbezogen, insbesondere nach dem Auftreten schwerwiegender IKT-Vorfälle. In einem solchen Fall kann eine gezielte Überprüfung der betroffenen Teilbereiche ausreichen, ohne dass eine vollständige Rahmenrevision erforderlich wäre. Mit dem abschließenden Validierungsbericht erhalten die Mitglieder des Leitungsorgans einen strukturierten, nachvollziehbaren Überblick über den Funktionszustand des IKT-Risikomanagementrahmens – vergleichbar mit dem Prüfprotokoll der Hauptuntersuchung, das den aktuellen Betriebszustand dokumentiert, identifizierte Schwachstellen benennt und konkrete Ansätze zur Weiterentwicklung aufzeigt.

Die Analogie lässt sich an einem entscheidenden Punkt konsequent zu Ende denken. So wie ein Fahrzeugführer nach bestandener Hauptuntersuchung jederzeit damit rechnen muss, im Rahmen einer allgemeinen Verkehrskontrolle von der Polizei angehalten zu werden – ob zufällig oder anlassbezogen –, steht auch das Finanzinstitut unter dem jederzeitigen Vorlagevorbehalt der Aufsicht. Die BaFin kann den Validierungsbericht gemäß Art. 6 Abs. 5 DORA ohne Vorankündigung und unabhängig vom regulären Überprüfungszyklus anfordern. Ebenso wie der Fahrzeugführer in diesem Moment einen gültigen, vollständigen und mitgeführten Prüfnachweis vorzuweisen hat, muss das Institut einen Bericht vorlegen können, der zu jedem Zeitpunkt aktuell, nachvollziehbar und prüfungsfest ist. Ein veralteter, lückenhafter oder inhaltlich nicht belastbarer Bericht verfehlt diese Anforderung in gleicher Weise, wie ein abgelaufener Hauptuntersuchungsnachweis die Betriebserlaubnis des Fahrzeugs in Frage stellt – mit entsprechenden aufsichtlichen Konsequenzen.

3. Die IKT-Kontrollfunktion in Aktion: Mandat, Methodik und Prüfdurchführung

Was DORA von der IKT-Kontrollfunktion verlangt, geht weit über das hinaus, was in vielen Instituten bislang als Aufgabenprofil dieser Funktion verstanden wird. Der Kern der Neuerung liegt in einer qualitativen Verschiebung des Prüfauftrags: Während klassische Compliance-orientierte Kontrollansätze primär auf Vollständigkeit ausgerichtet sind – ist das erforderliche Dokument vorhanden, wurde die vorgeschriebene Maßnahme umgesetzt, existiert eine entsprechende Richtlinie? –, fordert DORA mit der Überprüfung des IKT-Risikomanagementrahmens eine genuine Funktionsprüfung. Die entscheidende Frage lautet nicht länger allein, ob eine Komponente des Rahmens vorhanden ist, sondern ob sie wirksam funktioniert, ob sie mit den übrigen Teilbereichen des Rahmens verzahnt ist und ob sie im Zusammenspiel der Gesamtarchitektur die intendierte Schutzwirkung entfaltet.

Diese Unterscheidung ist für das Anforderungsprofil der IKT-Kontrollfunktion von grundlegender Bedeutung. Eine Funktionsprüfung setzt voraus, dass die prüfende Instanz über vollständige Transparenz hinsichtlich aller im IKT-Risikomanagementrahmen verbauten Komponenten verfügt – vergleichbar mit dem Zugriff des TÜV-Prüfers auf die Fahrzeugdatenbank, in der sämtliche eingebauten Teile lückenlos dokumentiert sind. Ohne ein belastbares, aktuell gehaltenes Inventar aller relevanten IKT-Assets, Verfahren, Richtlinien, Protokolle und Tools ist eine substanzielle Funktionsbewertung methodisch nicht möglich. Die Transparenz über die Rahmenkomponenten ist damit keine nachgeordnete Dokumentationsanforderung, sondern die unabdingbare Grundlage jeder ernsthaften Prüfung.

Darüber hinaus muss die IKT-Kontrollfunktion – wiederum in Analogie zum Fahrzeugprüfer, der auf Rückrufinformationen der Hersteller zugreift – in der Lage sein, externe

Erkenntnisse über bekannte Schwachstellen, Sicherheitslücken oder Funktionsdefizite einzelner IKT-Komponenten in ihre Bewertung einzubeziehen. Hersteller und Anbieter von IKT-Produkten und -Dienstleistungen kommunizieren regelmäßig sicherheitsrelevante Informationen, die für die Beurteilung des Schutzstatus des Instituts unmittelbar relevant sind. Eine IKT-Kontrollfunktion, die diesen Informationsfluss nicht systematisch verarbeitet, operiert an einem wesentlichen Teil der Realität vorbei.

Methodisch stützt sich die Überprüfung des IKT-Risikomanagementrahmens auf eine Vielzahl von Vorprodukten, die aus dem laufenden Betrieb des Risikomanagements hervorgehen. Interne und externe Prüfberichte, Ergebnisse aus dem TLPT-Programm und anderen Tests der digitalen operationellen Resilienz, Berichte aus dem IKT-Drittparteienmanagement, Notfallübungen sowie Vorfallsanalysen liefern der IKT-Kontrollfunktion das Datenmaterial, auf dessen Grundlage eine fundierte Gesamtbewertung erst möglich wird. Die Kunst der Prüfdurchführung besteht darin, diese heterogenen Informationsquellen systematisch zusammenzuführen, zu gewichten und zu einer konsistenten Aussage über den Funktionszustand des Rahmens zu verdichten – nicht als mechanische Aggregation von Einzelbefunden, sondern als analytische Syntheseleistung, die Wechselwirkungen und systemische Muster erkennt.

Ein weiterer, in der bisherigen Praxis häufig unterschätzter Aufgabenbereich der IKT-Kontrollfunktion betrifft die Verantwortung für den kontinuierlichen Verbesserungsprozess. Art. 6 Abs. 5 DORA macht explizit deutlich, dass der IKT-Risikomanagementrahmen auf Grundlage der bei Umsetzung und Überwachung gewonnenen Erkenntnisse fortlaufend zu verbessern ist. Die IKT-Kontrollfunktion trägt nicht nur die Verantwortung für die Feststellung von Verbesserungsbedarfen, sondern auch für deren systematische Nachverfolgung und Dokumentation. Maßnahmen müssen terminiert, verantwortet und auf ihre Umsetzung hin überprüft werden; der Verbesserungskreislauf muss als geschlossener Regelkreis gestaltet und nachgewiesen werden können.

Betrachtet man dieses Aufgabenspektrum in seiner Gesamtheit, wird deutlich, dass die regulatorischen Anforderungen von DORA an die IKT-Kontrollfunktion ein Tätigkeitsprofil konstituieren, das in den bisherigen Arbeitsvolumina dieser Funktion bei den meisten Instituten nicht vollständig abgebildet ist. Insbesondere in der genossenschaftlichen Finanzgruppe und im Sparkassensektor zeigt sich, dass die IKT-Kontrollfunktionen häufig auf ein Aufgabenportfolio ausgerichtet sind, das primär auf Dokumentation und formale Compliance ausgerichtet ist – nicht jedoch auf die methodisch anspruchsvolle Kombination aus Inventartransparenz, Funktionsbewertung, externer Informationsverarbeitung, Vorproduktintegration und KVP-Verantwortung, die DORA einfordert. Die Anpassung der Ressourcenausstattung, der Qualifikationsprofile und der internen Prozesse an diese erweiterten Anforderungen stellt für viele Institute eine der zentralen operativen

Herausforderungen der DORA-Implementierung dar – und ist zugleich eine Frage, die in der aufsichtlichen Bewertung der Rahmenwirksamkeit zunehmend an Gewicht gewinnen wird.

4. Ergebnisse sichtbar machen: Aufbau und Wirkung eines überzeugenden Prüfberichts

Der Validierungsbericht ist das zentrale Kommunikationsinstrument der Überprüfung des IKT-Risikomanagementrahmens. Er ist nicht nur das Ergebnis der Prüftätigkeit der IKT-Kontrollfunktion, sondern zugleich das Dokument, das gegenüber dem Leitungsorgan und gegenüber der Aufsicht die Funktionsfähigkeit des Rahmens nachweist. Seine inhaltliche und formale Ausgestaltung ist regulatorisch präzise normiert: Art. 27 der Delegierten Verordnung (EU) 2024/1774 – dem RTS zum IKT-Risikomanagement – legt Format, Inhalte und Struktur des Berichts verbindlich fest und schafft damit einen Mindeststandard, der von jedem betroffenen Institut zwingend einzuhalten ist.

Bereits auf der Ebene der Formanforderungen setzt der RTS eine klare Vorgabe: Gemäß Art. 27 Abs. 1 RTS ist der Bericht in einem durchsuchbaren elektronischen Format vorzulegen. Diese auf den ersten Blick technisch wirkende Anforderung hat eine unmittelbare praktische Konsequenz: Der Bericht muss so aufgebaut sein, dass einzelne Inhalte von der Aufsicht gezielt abgerufen und ausgewertet werden können. Ein unstrukturiertes, schwer navigierbares Dokument erfüllt diese Anforderung nicht – auch dann nicht, wenn es inhaltlich alle erforderlichen Angaben enthält.

Inhaltlich geht Art. 27 Abs. 2 RTS weit über eine formale Vollständigkeitsprüfung hinaus. Der Bericht hat umfassende Informationen zu enthalten, die eine substanzielle Funktionsbewertung des gesamten IKT-Risikomanagements ermöglichen. Konkret sind im Bericht unter anderem Angaben zur Identifikation des Finanzunternehmens, eine Beschreibung des Prüfgegenstands und des Prüfzeitraums, die angewandte Methodik der Überprüfung sowie eine Bewertung der Wirksamkeit der einzelnen Komponenten des IKT-Risikomanagementrahmens aufzunehmen. Darüber hinaus müssen identifizierte Schwachstellen und Verbesserungspotenziale konkret benannt und mit Maßnahmenempfehlungen hinterlegt werden. Der Bericht schließt mit einer Gesamtbewertung des Funktionszustands des Rahmens, die dem Leitungsorgan eine fundierte Entscheidungsgrundlage liefert.

Aus dieser normativen Anforderungsstruktur ergeben sich zwei gleichwertige Funktionsdimensionen des Validierungsberichts. Aus Sicht des Instituts dient er der institutseigenen Qualitätssicherung: Er macht den tatsächlichen Funktionszustand des IKT-Risikomanagementrahmens transparent, identifiziert Handlungsbedarfe und schafft die Grundlage für den regulatorisch geforderten kontinuierlichen Verbesserungsprozess. Aus

aufsichtlicher Perspektive stellt er eine regelmäßige, nachvollziehbare Überblicksdokumentation dar, die der BaFin eine belastbare Beurteilung des Resilienzstatus des Instituts ermöglicht – ohne dass eine vollständige Vor-Ort-Prüfung erforderlich wäre.

Für die Praxis bedeutet dies, dass die Qualität des Validierungsberichts nicht allein nach seinem formalen Umfang zu bemessen ist. Entscheidend ist seine analytische Tiefe: Ein überzeugender Bericht verbindet die Darstellung der Prüfmethodik mit einer differenzierten Wirksamkeitsbewertung, benennt Schwachstellen präzise und ohne Verharmlosung und formuliert Maßnahmen so konkret, dass ihre Nachverfolgung im Rahmen des KVP möglich ist. Ein Dokument, das sich auf die Feststellung beschränkt, alle Komponenten seien vorhanden, verfehlt den regulatorischen Anspruch des Art. 27 RTS ebenso wie die inhaltlichen Erwartungen eines kritisch prüfenden Leitungsorgans. Der Bericht muss Antworten auf die Frage liefern, wie gut der Rahmen funktioniert – nicht nur, ob er existiert.

Die Doppelfunktion des Berichts – als internes Steuerungsinstrument und als aufsichtliches Nachweisdokument – prägt auch die Anforderungen an seine sprachliche und argumentative Gestaltung. Er muss so formuliert sein, dass er für die Mitglieder des Leitungsorgans ohne tiefgreifende technische Vorkenntnis verständlich ist, zugleich aber die methodische Substanz aufweist, die eine aufsichtliche Plausibilitätsprüfung erfordert. Diese Kombination aus Verständlichkeit und fachlicher Belastbarkeit ist keine triviale Leistung – sie erfordert eine bewusste inhaltliche Strukturierung und ein klares Verständnis der jeweiligen Adressatenperspektive.

5. Noch in Bewegung: Offene Fragen, Diskussionen und frühe Prüfungserfahrungen

Mit dem Ablauf des ersten DORA-Anwendungsjahres am 17. Januar 2026 sind die ersten Prüfungserfahrungen mit dem Validierungsbericht zum IKT-Risikomanagementrahmen verfügbar – und sie offenbaren ein Bild, das zwischen regulatorischem Anspruch und institutioneller Praxisrealität noch erhebliche Spannungsfelder aufweist. Die nachfolgenden Feststellungen und Diskussionspunkte spiegeln den aktuellen Stand der frühen Umsetzungspraxis wider und benennen Handlungsbedarfe, die für die weitere Entwicklung des Prüfregimes von besonderer Bedeutung sind.

Feststellung 1: Verspätete Berichterstattung als strukturelles Umsetzungsproblem

Die erste und in der Breite bedeutsamste Feststellung aus frühen Prüfungserfahrungen betrifft die zeitliche Dimension der Berichterstattung. Zahlreiche Institute haben den Validierungsbericht erst nach dem 17. Januar 2026 fertiggestellt – einem Datum, das den Ablauf des ersten vollständigen DORA-Anwendungsjahres markiert. In der aufsichtlichen Einordnung ist eine solche Verzögerung in der Regel als Mangel im Bereich F2 zu

klassifizieren, der zwar noch keine unmittelbaren Eingriffsbefugnisse auslöst, aber dokumentationspflichtig ist und bei Wiederholung an aufsichtlicher Relevanz gewinnt.

Die Analogie zur Hauptuntersuchung trägt auch hier: Wie ein Fahrzeug nach Ablauf der regulären Prüffrist noch eine gewisse Karenzzeit genießt, bevor die Betriebserlaubnis als erloschen gilt, verfügt auch der IKT-Risikomanagementrahmen über eine implizite Toleranzspanne. Gleichwohl darf diese Karenzzeit nicht zur Regel werden. Entscheidend ist dabei ein Verständnis, das in der Praxis keineswegs selbstverständlich ist: Als fertiggestellt gilt der Validierungsbericht nicht bereits mit seiner Erstellung durch die IKT-Kontrollfunktion. Fertiggestellt im regulatorischen Sinne ist er erst mit seiner förmlichen Behandlung im Leitungsorgan – mindestens auf Ebene des Gesamtvorstands. Solange dieses Gremium den Bericht nicht zur Kenntnis genommen und die Kenntnisnahme nachvollziehbar dokumentiert hat, existiert regulatorisch kein abgeschlossener Validierungsbericht. Dieser Unterschied zwischen technischer Erstellung und institutioneller Vollendung des Berichts wird in der Praxis häufig unterschätzt.

Feststellung 2: Unklarheiten beim Überprüfungsturnus

Eine zweite, weit verbreitete Unklarheit betrifft die Frage, auf welchen Bezugszeitraum der jährliche Überprüfungsturnus zu beziehen ist. Viele Institute orientieren sich am Geschäftsjahr und planen die Fertigstellung des Validierungsberichts für das erste Quartal des Folgejahres. Dies ist formal möglich, birgt aber ein strukturelles Risiko: Wird der Bericht für das Geschäftsjahr 1. Januar bis 31. Dezember erst in den Monaten Februar oder März des Folgejahres dem Vorstand vorgelegt, ist die regulatorische Karenzzeit bereits erheblich beansprucht – und im Wiederholungsfall potentiell überschritten.

Methodisch vorzugswürdig ist ein Überprüfungsturnus, der die Fertigstellung des Berichts – einschließlich seiner Behandlung im Vorstand – spätestens im Dezember eines jeden Jahres vorsieht. Dies ermöglicht, in direkter Analogie zur Hauptuntersuchung, eine nahtlose Anschlussbetriebserlaubnis: Der im Dezember abgenommene Bericht begründet die Resilienz-Betriebserlaubnis für das folgende Jahr und stellt sicher, dass das Institut zu keinem Zeitpunkt ohne gültige, aktuelle Validierung operiert. Eine solche Taktung setzt freilich voraus, dass die IKT-Kontrollfunktion ihre Überprüfungshandlungen bereits im dritten Quartal des laufenden Jahres beginnt – was wiederum eine frühzeitige Kapazitätsplanung und einen strukturierten Prüfkalender erfordert.

Herausforderung: Anlassbezogene Überprüfung nach schwerwiegenden IKT-Vorfällen

Eine besondere konzeptionelle Herausforderung stellt die anlassbezogene Überprüfung nach schwerwiegenden IKT-Vorfällen dar. In der Diskussion wird häufig von einem „vereinfachten Bericht" oder „Kurzbericht" gesprochen – eine Bezeichnung, die methodisch irreführend ist und zu falschen Schlüssen über den erforderlichen Prüfumfang verleiten

kann. Der Begriff suggeriert, dass in einem solchen Fall weniger strenge Anforderungen gelten, was regulatorisch nicht zutreffend ist.

Zutreffend ist hingegen, dass die anlassbezogene Überprüfung eine andere Struktur aufweist als die reguläre Jahresvalidierung – aber keine geringere methodische Sorgfalt erfordert. Der sachgerechte Ansatz folgt dem Prinzip einer risikoorientierten Modularisierung: In einem ersten Schritt ist zu analysieren, welche Teilbereiche des IKT-Risikomanagementrahmens durch den eingetretenen Vorfall betroffen waren oder potenziell beeinträchtigt worden sein könnten. Auf dieser Grundlage werden gezielt die relevanten Module einer vollwertigen Funktionsprüfung unterzogen, während nicht betroffene Teilbereiche ausgeklammert bleiben. Das Ergebnis ist kein Bericht minderen Formats, sondern ein auf die wesentlichen Aspekte des konkreten Anlasses konzentrierter Bericht mit vollständiger methodischer Substanz.

Die Analogie zur Fahrzeuguntersuchung verdeutlicht die Logik dieses Ansatzes: Wenn ein Fahrzeughalter neue Reifen oder Felgen einträgt, führt der Prüfer keine vollständige Neuuntersuchung des Fahrzeugs durch, insbesondere keine Abgasmessung oder Überprüfung der Beleuchtungsanlage. Er konzentriert sich auf die durch die Änderung betroffenen Komponenten und prüft diese mit der gleichen fachlichen Sorgfalt wie im Rahmen der regulären Hauptuntersuchung. Genau diese schlaue Modularisierung ermöglicht Effizienz ohne Qualitätsverlust – und ist das methodische Leitprinzip für die anlassbezogene Teilvalidierung des IKT-Risikomanagementrahmens.

Handlungsempfehlungen für LSI-Institute im genossenschaftlichen Sektor und bei Sparkassen

Aus den dargestellten Feststellungen und Herausforderungen lassen sich konkrete Handlungsempfehlungen ableiten, die insbesondere für Less Significant Institutions (LSI) im genossenschaftlichen Sektor und im Sparkassenbereich von unmittelbarer praktischer Relevanz sind.

Vorrangig ist die formale Kenntnisnahme durch das vollständige Leitungsorgan sicherzustellen. Der Validierungsbericht sollte nicht allein durch das zuständige Vorstandsmitglied gezeichnet werden, sondern durch den Gesamtvorstand und – als Leitungsorgan im Sinne von Art. 4 Abs. 1 Nr. 7 DORA – auch durch den Aufsichtsrat förmlich zur Kenntnis genommen werden. Diese Kenntnisnahme ist nachvollziehbar zu dokumentieren; die bloße Weiterleitung des Berichts ohne dokumentierten Beschluss genügt den regulatorischen Anforderungen nicht.

Eng damit verbunden ist die Notwendigkeit, den jährlichen Validierungszyklus als institutionalisierten Standardprozess in der schriftlich fixierten Ordnung zu verankern. Die erstmalige Erstellung des Berichts darf nicht als Einzelereignis begriffen werden, sondern als Startpunkt eines dauerhaften Regelkreises. Methodik, Zeitplan, Verantwortlichkeiten und

Eskalationswege sind formal zu dokumentieren, sodass der jährliche Überprüfungsprozess ohne erneuten konzeptionellen Abstimmungsaufwand reproduzierbar ist.

Gleichzeitig muss die ressourcenseitige Absicherung der IKT-Kontrollfunktion dauerhaft gewährleistet sein. Eine vollwertige Funktionsprüfung des IKT-Risikomanagementrahmens ist – wie in Kapitel 3 dargelegt – ressourcenintensiv und verlangt personelle sowie zeitliche Kapazitäten, die in vielen Instituten bislang nicht in ausreichendem Umfang eingeplant sind. Ohne eine angemessene Ausstattung der IKT-Kontrollfunktion bleibt die regulatorische Anforderung einer substanziellen Funktionsprüfung strukturell unerfüllbar.

Darüber hinaus sollte die von der IKT-Kontrollfunktion entwickelte Validierungsmethodik formal dokumentiert, kritisch reflektiert und im Sinne eines kontinuierlichen Verbesserungsprozesses fortlaufend weiterentwickelt werden. Erkenntnisse aus internen und externen Prüfungen, aus aufsichtsrechtlichen Verlautbarungen sowie aus dem kollegialen Austausch im Sektor sind systematisch in die Methodenweiterentwicklung einzuspeisen. Eine Methodik, die sich nicht selbst hinterfragt, verliert über die Zeit an Relevanz und Trennschärfe.

Schließlich empfiehlt sich die Entwicklung eines eigenständigen, schlanken Verfahrens für die anlassbezogene Teilvalidierung. Für den Fall schwerwiegender IKT-Vorfälle oder wesentlicher Änderungen im Rahmen sollte ein klar definierter Prozess existieren, der ohne den zeitlichen Aufwand einer vollständigen Jahresüberprüfung auskommt, aber dennoch die wesentlichen Nachweispflichten gegenüber der Aufsicht nach Art. 6 Abs. 5 DORA erfüllt. Die oben beschriebene risikoorientierte Modularisierung bietet hierfür den methodischen Rahmen – sie muss jedoch vorab konzipiert und dokumentiert sein, damit sie im Anlassfall ohne Zeitverlust angewendet werden kann.

Prof. Dr. Andreas Igl
BDO-Stiftungsprofessor an der TH Deggendorf
Lehrbeauftragter an der Hochschule der Deutschen Bundesbank

andreas.igl@th-deg.de
(Mobil): 0151 2301 8610
(LinkedIn): Link