Prof. Dr. Andreas Igl
TH Deggendorf

Technologische Infrastrukturen im Fokus aufsichtlicher Bewertung

Deggendorfer Notiz 2026/04 | 6. Februar 2026

Die Notiz untersucht technologische Infrastrukturen als konstitutiven Bestandteil der Gesamtinstitutssteuerung. Im Mittelpunkt stehen das IKT-Risikomanagement nach DORA, Informationsschutz, operative Widerstandsfähigkeit sowie die Steuerung externer Technologiedienstleister. Historisch gewachsene Systemlandschaften, Dokumentationsmängel und unzureichende Governance-Verzahnung zählen zu den häufigsten Feststellungen, die gerade kleinere Regionalbanken vor erhebliche Umsetzungsherausforderungen stellen.

1. Technologische Plattformen als Steuerungsdeterminante

Die aufsichtliche Analyse im Bereich technologischer Infrastrukturen hat sich in den vergangenen Jahren deutlich verschoben. An die Stelle einer primär ordnungsmäßigkeitsorientierten Betrachtung tritt zunehmend die Bewertung von Widerstandsfähigkeit und Robustheit der technologischen Unterstützung für die Gesamtinstitutssteuerung. Technologische Systeme werden aus aufsichtlicher Perspektive nicht mehr als unterstützende Infrastruktur verstanden, sondern als konstitutiver Bestandteil der Steuerungsarchitektur eines Instituts. Ihre Leistungsfähigkeit bestimmt unmittelbar, ob Steuerungsprozesse zuverlässig funktionieren oder strukturellen Risiken ausgesetzt sind.

Die Steuerungsfähigkeit eines Instituts hängt dabei unmittelbar von der Verfügbarkeit, Integrität und Belastbarkeit der technologischen Plattformen ab. Aufsichtliche Analysen fokussieren verstärkt darauf, ob technologische Systeme die Anforderungen aus der internen Kapital- und Liquiditätsadäquanzbeurteilung operativ tragen können. Maßgeblich ist nicht allein die rechnerische Modellfähigkeit, sondern die Frage, ob Informationsverarbeitung, Risikomessung und Berichterstattung auch unter erhöhter Belastung oder eingeschränkter Systemverfügbarkeit funktionsfähig bleiben. Technologie wird damit zu einem wesentlichen Faktor für die Nachhaltigkeit der Kapital- und Liquiditätssteuerung.

Ein zentrales aufsichtliches Risiko stellen historisch gewachsene Systemlandschaften dar. Über Jahre entwickelte Architekturen mit zahlreichen Schnittstellen, Altsystemen und Sonderlösungen erhöhen die Komplexität und damit die Fehleranfälligkeit der Steuerungsprozesse. Medienbrüche, manuelle Workarounds und tabellenbasierte

Zwischenlösungen werden aus aufsichtlicher Perspektive als Indikatoren struktureller Schwächen bewertet. Sie verweisen auf eine mangelnde Integration der technologischen Infrastruktur in die Steuerungslogik und erhöhen das operationelle Risiko, insbesondere in Stress- und Krisensituationen.

Die Komplexität der technologischen Architektur beeinflusst damit direkt die Qualität und Verlässlichkeit von Steuerungsentscheidungen. Aufsichtliche Analysen untersuchen, ob die bestehende Systemlandschaft beherrschbar ist und ob technische Abhängigkeiten transparent dokumentiert und gesteuert werden. Eine unzureichende strategische Steuerung der technologischen Infrastruktur wird als Governance-Defizit gewertet, da sie regelmäßig zu inkonsistenten Prioritäten, ineffizientem Ressourceneinsatz und erhöhten Risiken führt.

Vor diesem Hintergrund gewinnt die technologische Strategie als Steuerungsinstrument an Bedeutung. Aufsichtlich wird erwartet, dass sie nachvollziehbar aus der Geschäftsstrategie abgeleitet ist und die Anforderungen der Gesamtinstitutssteuerung systematisch adressiert. Fehlt diese strategische Anbindung, werden Technologieinvestitionen häufig isoliert betrachtet und entfalten keine nachhaltige Steuerungswirkung. IKT-Risiken werden in diesem Kontext zunehmend als eigenständige Risikotreiber verstanden, deren Auswirkungen über den reinen Betrieb hinausgehen.

Mit DORA wird diese Entwicklung weiter verstärkt. Die Verordnung unterstreicht die Erwartung, dass Technologie nicht als technischer Annex, sondern als integraler Bestandteil der Gesamtinstitutssteuerung zu behandeln ist. Aufsichtliche Analysen bewerten folglich, ob Institute ihre technologische Landschaft so ausrichten, dass sie nicht nur den aktuellen Anforderungen genügt, sondern auch zukünftige Belastungen resilient bewältigen kann.

2. Dimensionen des IKT-Risikomanagements gemäß DORA

Das IKT-Risikomanagement erfährt mit DORA eine deutliche inhaltliche und methodische Schärfung. Aus aufsichtlicher Perspektive wird damit ein formalisiertes, dokumentiertes und wirksames Steuerungssystem eingefordert, das über bestehende, häufig technisch geprägte IT-Risikoprozesse hinausgeht. Maßgeblich ist, ob Institute eine konsistente Systematik zur Identifikation, Bewertung und Steuerung von IKT-Risiken etabliert haben und diese mit den Mindestanforderungen an das Risikomanagement verzahnen.

DORA differenziert IKT-Risiken in fünf klar abgegrenzte Risikobereiche, die aus aufsichtlicher Perspektive vollständig und überschneidungsfrei abzudecken sind. Der Bereich der Verfügbarkeits- und Kontinuitätsrisiken beschreibt das Risiko, dass Leistung und Verfügbarkeit von technologischen Systemen und Informationen beeinträchtigt werden. Dies umfasst insbesondere Ausfälle von Hard- oder Software, Schwächen im Systembetrieb

oder sonstige Ereignisse, die eine zeitnahe Wiederherstellung kritischer Services verhindern und damit die operative Steuerungsfähigkeit des Instituts einschränken.

Die Komponente der Sicherheitsrisiken adressiert das Risiko eines unbefugten Zugriffs auf technologische Systeme, sowohl von außen als auch von innen. Hierunter fallen insbesondere Cyberangriffe, Missbrauch von Zugriffsrechten oder unzureichende Schutzmechanismen, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen gefährden und unmittelbare Auswirkungen auf Steuerungs- und Kontrollprozesse haben können.

Das Element der Änderungsrisiken bezieht sich auf Risiken aus unzureichend gesteuerten Veränderungen in der technologischen Landschaft. Gemeint ist insbesondere die fehlende Fähigkeit, technologische Änderungen – vor allem in großen oder komplexen Veränderungsprogrammen – zeitgerecht, kontrolliert und nachvollziehbar umzusetzen. Aufsichtlich wird hierbei bewertet, ob Änderungsrisiken systematisch erfasst und in die Gesamtsteuerung integriert werden.

Der Bereich der Datenintegritätsrisiken umfasst das Risiko unvollständiger, fehlerhafter oder inkonsistenter Informationsverarbeitung über verschiedene technologische Systeme hinweg. Ursachen können schwache Kontrollen entlang des gesamten Informationslebenszyklus sein, von der Architektur und Modellierung über die Verarbeitung bis hin zur Aggregation und Ausgabe von Steuerungs- und Finanzinformationen. Aus aufsichtlicher Sicht ist dieser Risikobereich besonders kritisch, da er die Fähigkeit des Instituts beeinträchtigen kann, korrekte und zeitnahe Informationen für Risikomanagement und interne Adäquanzbeurteilungen bereitzustellen.

Die Komponente der Auslagerungsrisiken schließlich beschreibt Risiken aus der Nutzung externer Dienstleister oder konzerninterner Einheiten zur Erbringung von technologischen Leistungen. Gemeint sind negative Auswirkungen auf Leistungserbringung und Risikosteuerung, etwa durch Abhängigkeiten, unzureichende Kontrollrechte oder mangelnde Transparenz über ausgelagerte Prozesse.

Aufsichtliche Analysen bewerten vor diesem Hintergrund die Vollständigkeit der Risikoidentifikation über alle relevanten technologischen Komponenten hinweg. Erwartet wird, dass die fünf Risikokategorien nicht isoliert betrachtet, sondern in eine integrierte Gesamtrisikoinventur eingebettet werden. Die Risikobewertung muss dabei nachvollziehbar, konsistent und regelmäßig aktualisiert erfolgen. Eine rein qualitative Einstufung von IKT-Risiken wird zunehmend kritisch gesehen, insbesondere wenn sie keine Priorisierung oder Steuerungsrelevanz erkennen lässt.

Von zentraler Bedeutung sind zudem klar definierte Schnittstellen zum operationellen Risikomanagement, da viele IKT-Risiken als Treiber operationeller Verluste wirken. Aufsichtlich werden transparente Risikotoleranzen, klar festgelegte Eskalationsschwellen und

eine risikoadäquate Priorisierung von Steuerungsmaßnahmen erwartet. Wiederkehrende Feststellungen betreffen insbesondere Dokumentationsdefizite, die sowohl die interne Steuerungsfähigkeit als auch die aufsichtliche Nachvollziehbarkeit erheblich einschränken. DORA erhöht damit den Anspruch, IKT-Risiken nicht nur zu benennen, sondern systematisch, prüfbar und steuerungswirksam zu managen.

3. Informationsschutz und Geschäftskontinuität

Der Informationsschutz stellt aus aufsichtlicher Perspektive ein zentrales Kernelement der digitalen Widerstandsfähigkeit dar und bildet die Grundlage für die Verlässlichkeit technologiegestützter Steuerungsprozesse. Aufsichtliche Analysen beschränken sich dabei nicht auf die formale Existenz eines Informationsschutzmanagementsystems, sondern fokussieren auf dessen tatsächliche Wirksamkeit. Maßgeblich ist, ob technische und organisatorische Maßnahmen geeignet sind, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen nachhaltig zu schützen und ob sie im operativen Betrieb konsequent angewendet werden.

Ein wesentlicher Analyseaspekt betrifft die klare Regelung von Rollen und Verantwortlichkeiten im Informationsschutzprozess. Aufsichtlich wird bewertet, ob Zuständigkeiten für Prävention, Detektion und Reaktion eindeutig definiert, dokumentiert und institutionell verankert sind. Unklare Abgrenzungen zwischen technologischem Betrieb, Informationsschutzfunktion und Managementebene führen regelmäßig zu Feststellungen, da sie Entscheidungs- und Eskalationsprozesse verzögern und die Reaktionsfähigkeit im Ereignisfall beeinträchtigen.

Eng damit verknüpft ist die Beurteilung der Geschäftskontinuitätskonzepte. Diese werden nicht allein anhand ihrer konzeptionellen Ausgestaltung bewertet, sondern auf ihre tatsächliche Umsetzbarkeit hin überprüft. Aufsichtliche Analysen untersuchen, ob Notfallkonzepte, Wiederanlaufpläne und Krisenorganisation realistische Annahmen zugrunde legen und ob die definierten Wiederanlaufzeiten unter den gegebenen technischen und organisatorischen Rahmenbedingungen erreichbar sind. Zu optimistische oder nicht belegte Zeitvorgaben gelten als Indikator für eine unzureichende Durchdringung der Abhängigkeiten innerhalb der technologischen Landschaft.

Ein zentrales Qualitätsmerkmal wirksamer Informationsschutz- und Kontinuitätsstrukturen sind regelmäßige Tests. Aufsichtlich wird erwartet, dass Notfall- und Wiederanlaufpläne nicht nur theoretisch vorhanden sind, sondern durch strukturierte Tests validiert werden. Typische Defizite zeigen sich in unzureichend definierten Testszenarien, einer fehlenden Einbindung relevanter Organisationseinheiten oder einer zu geringen Komplexität der Übungen, die reale Störfälle nicht adäquat abbildet.

Besonders kritisch bewertet wird die Dokumentation der Testergebnisse. Unvollständige oder nicht nachvollziehbare Testprotokolle erschweren die Bewertung der Wirksamkeit

und verhindern eine systematische Ableitung von Verbesserungsmaßnahmen. Ebenso werden starke Abhängigkeiten von einzelnen Schlüsselpersonen beanstandet, da sie die Robustheit der Notfallorganisation im Krisenfall erheblich einschränken.

Mit DORA werden diese Anforderungen weiter verschärft. Die Verordnung betont explizit die Notwendigkeit eines durchgängigen Ansatzes von Prävention, Detektion und Reaktion auf IKT-bezogene Sicherheitsvorfälle. Aufsichtliche Analysen bewerten folglich, ob Informationsschutz- und Geschäftskontinuitätsstrukturen nicht nur formal bestehen, sondern integraler Bestandteil der Gesamtinstitutssteuerung sind und auch unter Stressbedingungen eine belastbare Handlungsfähigkeit gewährleisten.

4. Operative Widerstandsfähigkeit im digitalen Kontext

Die digitale operative Widerstandsfähigkeit erweitert den klassischen Fokus der Notfallvorsorge um eine ganzheitliche, zukunftsgerichtete Perspektive. Aus aufsichtlicher Perspektive geht es nicht mehr allein darum, ob Störungen grundsätzlich beherrscht werden können, sondern ob Institute in der Lage sind, digitale Beeinträchtigungen frühzeitig zu erkennen, ihre Auswirkungen zu begrenzen und die Steuerungsfähigkeit auch unter Stressbedingungen aufrechtzuerhalten. Widerstandsfähigkeit wird damit zu einem eigenständigen Qualitätsmerkmal der Gesamtinstitutssteuerung.

Ein zentraler Analyseaspekt ist die Reaktionsfähigkeit auf technologiebezogene Vorfälle. Aufsichtlich wird bewertet, ob Melde-, Entscheidungs- und Eskalationsprozesse so ausgestaltet sind, dass sie im Ereignisfall schnell und wirksam greifen. Dabei rücken nicht nur technische Reaktionsmechanismen in den Fokus, sondern auch organisatorische Abläufe, Entscheidungszuständigkeiten und Kommunikationswege. Eine rein technische Betrachtung der Widerstandsfähigkeit wird als unzureichend angesehen, da sie die Wechselwirkungen mit Governance- und Steuerungsprozessen außer Acht lässt.

Von besonderer Bedeutung sind Resilienztests und Szenarioanalysen. Aufsichtliche Analysen untersuchen, ob diese Tests realistische Stresssituationen abbilden, die sowohl technische Ausfälle als auch organisatorische Engpässe berücksichtigen. Szenarien mit begrenzter Systemverfügbarkeit, verzögerter Informationsverarbeitung oder Ausfällen kritischer Dienstleister gewinnen dabei an Bedeutung. Entscheidend ist, ob die Tests über Standardannahmen hinausgehen und die tatsächliche Belastbarkeit der Steuerungsprozesse sichtbar machen.

Die Wiederherstellungsprozesse müssen klar dokumentiert, regelmäßig überprüft und durch Tests validiert sein. Aufsichtlich wird erwartet, dass Wiederanlaufzeiten nachvollziehbar definiert und ihre Erreichbarkeit empirisch belegt ist. Unzureichend getestete Wiederherstellungspläne oder fehlende Ableitungen aus Testergebnissen werden regelmäßig als Schwachstellen identifiziert.

Im Lichte der internen Kapital- und Liquiditätsadäquanzbeurteilung gewinnt die Verknüpfung von Resilienztests mit bestehenden Szenarioanalysen erheblich an Bedeutung. Aufsichtliche Analysen bewerten, ob digitale Störszenarien in Kapital- und Liquiditätsstressszenarien integriert sind und ob deren Auswirkungen auf Risikotragfähigkeit und Liquiditätslage systematisch analysiert werden. Ergebnisse aus Resilienztests müssen sich nachvollziehbar in Steuerungsentscheidungen widerspiegeln, etwa in der Priorisierung von Investitionen, der Anpassung von Schwellenwerten oder der Weiterentwicklung von Notfallkonzepten.

Mit DORA wird digitale Widerstandsfähigkeit explizit als eigenständiges Steuerungsziel etabliert. Die aufsichtliche Analyse richtet sich folglich darauf, ob Institute Widerstandsfähigkeit nicht als isoliertes Technologiethema behandeln, sondern als integralen Bestandteil der Gesamtinstitutssteuerung verstehen und in ihre strategischen und operativen Entscheidungsprozesse einbinden.

5. Externe Technologiedienstleister und Auslagerungsbeziehungen

Die Steuerung von externen Technologiedienstleistern und Auslagerungsbeziehungen rückt mit DORA verstärkt in den Mittelpunkt der aufsichtlichen Analyse, da Abhängigkeiten von externen Dienstleistern ein zentrales IKT-Risiko für die Gesamtinstitutssteuerung darstellen. Digitale Wertschöpfungsketten sind zunehmend arbeitsteilig organisiert, wodurch die Verfügbarkeit, Integrität und Sicherheit bankinterner Prozesse maßgeblich von der Leistungsfähigkeit externer Anbieter abhängt. Aufsichtliche Analysen fokussieren daher auf die Frage, ob diese Abhängigkeiten transparent erfasst, risikoadäquat gesteuert und in die Gesamtinstitutssteuerung integriert sind.

DORA erweitert die bisherigen nationalen Auslagerungsregelungen deutlich und verschiebt den Beurteilungsmaßstab von einer primär formalen Betrachtung hin zu einer stärkeren Betonung von Steuerbarkeit und Widerstandsfähigkeit. Während bestehende Regelwerke insbesondere die ordnungsgemäße Vertragsgestaltung und Überwachung adressieren, fordert DORA eine umfassendere Sicht auf IKT-bezogene Abhängigkeiten, einschließlich intra-gruppaler Leistungen und komplexer Dienstleisterketten. Aufsichtlich wird daher bewertet, ob Institute diese erweiterten Anforderungen systematisch in ihre bestehenden Auslagerungsprozesse integriert haben.

Ein zentraler Analyseaspekt ist die Vollständigkeit des Drittdienstleisterinventars. Erwartet wird eine konsistente und aktuelle Erfassung aller IKT-relevanten Auslagerungen, einschließlich der eindeutigen Kennzeichnung von Dienstleistern für kritische oder wichtige Funktionen. Unvollständige Inventare oder uneinheitliche Klassifizierungen gelten als wesentliche Schwachstellen, da sie eine risikoorientierte Steuerung und Überwachung erheblich erschweren. Besonders kritisch werden Fälle bewertet, in denen zentrale

Steuerungs- oder Informationsprozesse ausgelagert sind, ohne dass deren Kritikalität angemessen reflektiert wird.

Die Risikoanalysen im Zusammenhang mit externen Technologiedienstleistern müssen über Einzelbetrachtungen hinausgehen und auch Konzentrationsrisiken berücksichtigen. Aufsichtliche Analysen untersuchen, ob Institute Abhängigkeiten von einzelnen Anbietern, Technologien oder Regionen identifizieren und bewerten. Eine fehlende Berücksichtigung kumulativer Risiken wird regelmäßig als Mangel festgestellt, da sie die tatsächliche Risikolage verzerrt.

Zunehmend detailliert analysiert werden auch die Vertragsinhalte. Erwartet werden klare Regelungen zu Informationsrechten, Prüfungs- und Zugriffsrechten, Meldepflichten bei Störungen sowie zu Sicherheits- und Resilienzanforderungen. Defizite im Vertragsmanagement zählen zu den häufigsten Feststellungen, insbesondere wenn Verträge historisch gewachsen sind und neue regulatorische Anforderungen nicht abbilden.

Ein besonderer aufsichtlicher Schwerpunkt liegt auf Ausstiegsstrategien. Aufsichtlich wird bewertet, ob Institute realistische und umsetzbare Ausstiegs- und Substitutionsszenarien definiert haben, die auch unter Stressbedingungen tragfähig sind. Fehlende oder rein theoretische Ausstiegskonzepte werden kritisch beurteilt, da sie die Handlungsfähigkeit im Krisenfall erheblich einschränken.

Schließlich wird die Überwachung der Dienstleister risikoorientiert bewertet. Erwartet wird ein systematischer Überwachungsansatz, der Art, Umfang und Kritikalität der Auslagerung berücksichtigt. DORA verschärft in diesem Kontext die Erwartungen an Transparenz und Steuerbarkeit und macht deutlich, dass die Verantwortung für ausgelagerte IKT-Leistungen uneingeschränkt beim Institut verbleibt.

6. Systemarchitekturen und technologische Landschaften

Die Systemarchitekturen und technologischen Landschaften besitzen aus aufsichtlicher Perspektive eine hohe Relevanz für die Qualität und Verlässlichkeit der Gesamtinstitutssteuerung. Die Architektur bestimmt maßgeblich, ob Steuerungsprozesse transparent, konsistent und beherrschbar ausgestaltet sind. Aufsichtliche Analysen untersuchen daher verstärkt, inwieweit Komplexität, historische Entwicklung und technische Schnittstellen die Steuerungsfähigkeit und die Informationsqualität beeinflussen.

Ein zentraler Analyseaspekt ist die Transparenz der Systemlandschaft. Aufsichtlich werden aktuelle und vollständige Architekturübersichten erwartet, die zentrale Anwendungen, Informationsflüsse und Abhängigkeiten nachvollziehbar darstellen. Fehlende oder veraltete Dokumentationen werden kritisch bewertet, da sie eine fundierte Risikoanalyse erschweren und die Steuerbarkeit komplexer Strukturen infrage stellen. Besonders im

Fokus stehen Schnittstellen, da sie ein zentrales Fehlerrisiko darstellen und häufig Ursache für Informationsinkonsistenzen und manuelle Korrekturen sind.

Altsysteme erhöhen aus aufsichtlicher Perspektive die operationellen Risiken, insbesondere wenn sie nur eingeschränkt wartbar sind oder nicht mehr vollständig in moderne Sicherheits- und Steuerungskonzepte integriert werden können. Gleichzeitig werden Redundanzen in der Systemlandschaft als Effizienz- und Risikotreiber bewertet, da sie Komplexität erhöhen und die Fehleranfälligkeit von Steuerungsprozessen verstärken. Aufsichtlich wird daher analysiert, ob die bestehende Architektur bewusst gesteuert oder lediglich historisch fortgeschrieben wird.

Ein weiterer Schwerpunkt liegt auf der Nachvollziehbarkeit von Informationsflüssen. Erwartet wird, dass Informationsherkunft, Verarbeitungsschritte und Zielsysteme klar dokumentiert sind und konsistent genutzt werden. Systemabhängigkeiten müssen in die Risikoanalysen einbezogen werden, da Ausfälle oder Fehlfunktionen einzelner Komponenten regelmäßig kaskadierende Effekte auf Steuerungs- und Berichtssysteme haben.

Veränderungen der Systemarchitektur sind kontrolliert und strukturiert umzusetzen. Aufsichtlich wird bewertet, ob Anpassungen systematisch geplant, risikoseitig bewertet und in die Gesamtsteuerung eingebettet werden. Mit DORA steigen die Anforderungen an die Beherrschbarkeit komplexer technologischer Strukturen, da Institute ihre Architektur nicht nur funktional, sondern auch resilienzorientiert weiterentwickeln müssen.

7. Feststellungsmuster und Optimierungsansätze

Die Auswertung aktueller Analysen zeigt bei Finanzunternehmen erhebliche Reifegradunterschiede in der Ausgestaltung von Technologie-Governance, Risikomanagement und operativer Umsetzung. Während konzeptionelle Grundlagen vielfach vorhanden sind, offenbaren aufsichtliche Analysen regelmäßig eine Lücke zwischen formaler Konzeption und tatsächlicher Wirksamkeit. Strategien, Richtlinien und Prozesse existieren, entfalten jedoch nicht in allen Fällen eine hinreichende Steuerungswirkung im laufenden Betrieb.

Ein zentrales Feststellungsfeld betrifft die Governance-Strukturen. Diese sind häufig nicht durchgängig wirksam, da Zuständigkeiten zwar definiert, Entscheidungs- und Eskalationswege jedoch nicht konsistent gelebt werden. In der Folge werden IKT-Risiken teilweise unterschätzt oder nicht risikoadäquat priorisiert. Aufsichtliche Analysen zeigen, dass IKT-Risiken zwar benannt, jedoch nicht systematisch in Steuerungsentscheidungen integriert werden, wodurch ihre tatsächliche Bedeutung für die Gesamtinstitutssteuerung unterschätzt bleibt.

Ein wiederkehrendes Schwachstellenfeld ist die Dokumentationsqualität. Unvollständige, veraltete oder inkonsistente Dokumentationen erschweren sowohl die interne Steuerung als auch die aufsichtliche Nachvollziehbarkeit. Dies betrifft insbesondere

Architekturübersichten, Risikoanalysen, Notfall- und Wiederanlaufkonzepte sowie Auslagerungsunterlagen. Defizite in der Dokumentation wirken dabei häufig als Katalysator weiterer Schwächen, da sie Transparenz und Verantwortlichkeit beeinträchtigen.

Aufsichtliche Analysen machen zudem Defizite in der Verzahnung von Technologie und Gesamtinstitutssteuerung sichtbar. Technologie wird nicht in allen Instituten als integraler Bestandteil der Steuerungsarchitektur verstanden, sondern weiterhin als technische Unterstützungsfunktion behandelt. Dies führt zu einer unzureichenden Einbindung technologischer Aspekte in strategische Planungs-, Risiko- und Entscheidungsprozesse. Insbesondere die Anbindung an die interne Kapital- und Liquiditätsadäquanzbeurteilung bleibt vielfach oberflächlich.

Verstärkt werden diese Defizite durch Ressourcenengpässe, die insbesondere kleinere und mittlere Regionalbanken betreffen. Begrenzte personelle und fachliche Kapazitäten erschweren die Umsetzung komplexer regulatorischer Anforderungen und führen zu einer starken Abhängigkeit von Schlüsselpersonen. Aufsichtsseitig wird dies kritisch bewertet, da es die Nachhaltigkeit der Steuerungs- und Kontrollstrukturen infrage stellt.

Mit DORA erhöht sich der Umsetzungsdruck deutlich. Die Verordnung macht klar, dass bestehende Defizite in der Technologie-Governance nicht mehr durch punktuelle Maßnahmen kompensiert werden können. Aufsichtlich wird eine strukturierte Weiterentwicklung der Technologie-Governance erwartet, die auf Integration, Konsistenz und Wirksamkeit ausgerichtet ist. Zentrale Optimierungsansätze liegen in der engeren Verzahnung von Organisationsstrukturen, technologischer Infrastruktur und Informationsmanagement sowie in der konsequenten Verankerung digitaler Widerstandsfähigkeit als Steuerungsziel der Gesamtinstitution.

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