



Regulatorische Anforderungen an digitale Steuerungsinfrastrukturen im Bankensektor: Ein Überblick

Deggendorfer Notiz 2026/02 | 1. Februar 2026

Die Notiz analysiert regulatorische Anforderungen an digitale Steuerungsinfrastrukturen im Bankensektor. Im Fokus stehen das Zusammenwirken von DORA, KWG und MaRisk sowie die Wechselwirkungen zwischen Governance-Strukturen, technologischer Infrastruktur und Informationsqualität. Aufsichtliche Analysen verlangen eine ganzheitliche Integration dieser Dimensionen in die Kapital- und Liquiditätsadäquanzbeurteilung. IKT-Risiken und Informationsqualitätsrisiken sind dabei als Risikoart zu steuern.

1. Zentrale Rolle digitaler Steuerungsinfrastrukturen für die Institutssteuerung

Digitale Steuerungsinfrastrukturen, Organisationsstrukturen und der Umgang mit Steuerungsinformationen haben sich zu unverzichtbaren Fundamenten der Stabilität und Handlungsfähigkeit von Finanzinstituten entwickelt. Die aufsichtliche Betrachtung erfasst diese Elemente längst nicht mehr als nachgelagerte Unterstützungsfunktionen, sondern als konstitutive Bestandteile der strategischen Ausrichtung und Risikoarchitektur. Der analytische Schwerpunkt verlagert sich dabei von der punktuellen Überprüfung einzelner Prozessschritte hin zu einer ganzheitlichen Einschätzung der Frage, inwieweit ein Institut seine strategischen Zielsetzungen auch unter widrigen Rahmenbedingungen operativ umsetzen kann.

Die fortschreitende Technologisierung bankfachlicher Abläufe hat diese Entwicklung erheblich vorangetrieben. Wachsende Abhängigkeiten von informations- und kommunikationstechnologischen Infrastrukturen, heterogene Systemarchitekturen sowie ein steigender Grad an Prozessautomation bewirken, dass organisatorische oder technologische Schwachstellen nicht mehr isoliert wirken. Vielmehr entfalten sie unmittelbare Konsequenzen für die Risikoerfassung, die Einhaltung definierter Schwellenwerte und die Qualität von Managemententscheidungen. Aufsichtliche Analysen konzentrieren sich daher verstärkt auf die institutseigene Kompetenz, Gefährdungspotenziale frühzeitig zu erkennen, konsistent zu bewerten und wirksam zu adressieren – selbst wenn Informationsquellen, technische Plattformen oder externe Partner temporär beeinträchtigt sind.



In dieser Perspektive werden Organisationsdesign, technologische Infrastruktur und Informationsmanagement als integraler Bestandteil der Gesamtsteuerung begriffen. Ausschlaggebend ist nicht die bloße Existenz formaler Regelungen oder installierter Systeme, sondern deren tatsächliche Leistungsfähigkeit, verlässliche Steuerungsimpulse zu generieren und operativ durchzusetzen. Aus aufsichtlicher Sicht ist insbesondere relevant, ob Governance-Strukturen eindeutige Verantwortlichkeiten etablieren, ob technische Architekturen die fachlichen Steuerungslogiken abbilden und ob der Informationshaushalt konsistente, tragfähige Grundlagen für Entscheidungsprozesse bereitstellt. Defizite in einem dieser Bereiche entfalten typischerweise systemweite Wirkung und können die Funktionsfähigkeit des gesamten Steuerungskreislaufs gefährden.

Vor diesem Hintergrund werden technologische Plattformen und Steuerungsinformationen zunehmend als produktive Ressourcen verstanden, deren Ausfall oder Fehlfunktion unmittelbare Konsequenzen für die Kapitaladäquanzbeurteilung, die Liquiditätssteuerung und interne Kontrollmechanismen nach sich zieht. Szenarien eingeschränkter Informationsverfügbarkeit oder verminderter Systemstabilität sind daher nicht mehr ausschließlich als betriebliche Risiken zu klassifizieren, sondern als potenzielle Bedrohung der Kapital- und Liquiditätssteuerung insgesamt. Die aufsichtliche Analyse richtet sich folgerichtig darauf, ob Institute auch unter Belastungs- und Krisenbedingungen ihre Handlungsfähigkeit bewahren und steuerungsrelevante Entscheidungen auf fundierter Basis treffen können.

2. Zusammenwirken regulatorischer Anforderungen

Die aufsichtliche Gesamtperspektive auf Organisationsstrukturen, technologische Infrastrukturen und Informationsmanagement wird maßgeblich durch das Ineinandergreifen von DORA, den Regelungen des Kreditwesengesetzes sowie den Mindestanforderungen an das Risikomanagement geprägt. Diese Normenkreise bilden keinen additiven Katalog isolierter Vorgaben, sondern einen kohärenten Regelungsrahmen, der Governance-, Risiko- und Steuerungserwartungen systematisch miteinander verknüpft. Aus aufsichtlicher Perspektive steht dabei weniger die formale Abarbeitung einzelner Normvorgaben im Vordergrund, sondern die Frage, ob das Institut diese Regelwerke in eine schlüssige Gesamtarchitektur der Institutssteuerung überführt.

Die gesetzlichen Governance-Vorgaben des Kreditwesengesetzes fungieren hierbei als übergeordnetes Prinzipiengerüst, das eine ordnungsgemäße Organisationsstruktur, angemessene interne Kontrollverfahren sowie ein wirksames Risikomanagement fordert. Diese Grundsätze werden durch die Mindestanforderungen an das Risikomanagement operativ konkretisiert. Insbesondere die Regelungen zur Aufbau- und Ablauforganisation präzisieren die Erwartungen an klare Kompetenzabgrenzungen, funktionale Trennungen und nachvollziehbare Entscheidungswege. Die Vorgaben zu Risikomanagementprozessen stellen sicher, dass Risiken systematisch identifiziert, bewertet, gesteuert und



überwacht werden. Ergänzend rücken die Anforderungen an Daten- und Modellgrundlagen die Qualität der Steuerungsinformationen in den Fokus und verknüpfen diese unmittelbar mit der Verlässlichkeit interner Modelle und daraus abgeleiteter Steuerungsimpulse.

Mit der DORA-Verordnung erfährt dieser Rahmen eine substanzielle Erweiterung. Aus aufsichtlicher Perspektive ist DORA nicht als isoliertes IT-Regelwerk zu verstehen, sondern als querschnittliche Präzisierung bestehender Governance-Anforderungen unter den Bedingungen zunehmender Digitalisierung. Die Verordnung konkretisiert insbesondere die Erwartungen an digitale operationelle Widerstandsfähigkeit, an das Management von IKT-Risiken sowie an die Steuerung von Abhängigkeiten gegenüber Drittanbietern. Damit schließt DORA bestehende Regelungslücken, die sich aus der wachsenden Bedeutung digitaler Prozesse für die Gesamtinstitutssteuerung ergeben, ohne die bestehenden nationalen Vorgaben zu ersetzen.

Aufsichtlich relevant ist folglich die Integrationstiefe der verschiedenen Regelwerke. Institute geraten zunehmend in den Fokus, bei denen DORA-Anforderungen isoliert in technischen Projekten adressiert werden, während organisatorische, risikosteuernde und informationsbezogene Implikationen unzureichend berücksichtigt bleiben. Solche parallelen, nicht abgestimmten Regelungskreise widersprechen dem aufsichtsrechtlichen Leitbild einer ganzheitlichen Steuerung. Erwartet wird vielmehr, dass DORA-Vorgaben systematisch in die bestehenden Governance-Strukturen eingebettet werden und dadurch ein konsistenter Steuerungsrahmen entsteht, der Organisationsdesign, technologische Infrastruktur und Informationsmanagement gleichermaßen umfasst.

In dieser Logik fungiert DORA als Katalysator für eine integrierte Sicht auf Steuerungs- und Überwachungsprozesse. Die aufsichtliche Analyse bewertet daher nicht isoliert die Einhaltung einzelner Artikel, sondern die Fähigkeit des Instituts, regulatorische Anforderungen zu einem belastbaren Gesamtsystem zu verdichten, das sowohl den Anforderungen der nationalen Aufsicht als auch den europäischen Leitlinien Rechnung trägt.

3. Wechselwirkungen zwischen Governance-Strukturen, technologischer Risikosteuerung und Informationsqualität

Organisationsstrukturen fungieren aus Sicht der Gesamtinstitutssteuerung als zentraler Steuerungsanker, da sie Verantwortlichkeiten, Entscheidungswege und Eskalationsmechanismen verbindlich festlegen. Nur wenn Rollen eindeutig zugeordnet und Entscheidungsprozesse konsistent ausgestaltet sind, können Steuerungsimpulse wirksam gesetzt und überwacht werden. Aufsichtliche Analysen richten sich daher verstärkt auf die Frage, ob organisatorische Regelungen nicht nur formal dokumentiert, sondern auch operativ gelebt werden. Diskrepanzen zwischen festgelegten Zuständigkeiten und tatsächlich



praktizierten Abläufen wirken sich unmittelbar auf die Qualität der Risikosteuerung aus und erschweren eine konsistente Gesamtinstitutssicht.

Die technologische Infrastruktur bildet in diesem Gefüge das operative Rückgrat der Gesamtinstitutssteuerung. Sie übersetzt organisatorische Vorgaben in ausführbare Prozesse, ermöglicht die technische Umsetzung von Risikomessung und stellt die Infrastruktur für Berichterstattungs- und Entscheidungsprozesse bereit. Dabei gewinnt die Durchgängigkeit der Systemlandschaft zunehmend an Bedeutung. Medienbrüche, manuelle Umgehungslösungen oder historisch gewachsene Insellösungen werden aus aufsichtlicher Sicht kritisch hinterfragt, da sie die Nachvollziehbarkeit von Steuerungsentscheidungen beeinträchtigen und die Abhängigkeit von Schlüsselpersonen erhöhen. Die technologische Infrastruktur ist damit nicht lediglich Ausführungsorgan, sondern ein eigenständiger Einflussfaktor auf die Steuerungsfähigkeit des Instituts.

Als verbindendes Element zwischen Organisationsstrukturen und technologischer Infrastruktur kommt dem Informationsmanagement eine Schlüsselrolle zu. Informationen stellen die Grundlage für Risikomessung, -steuerung und -überwachung dar und determinieren maßgeblich die Qualität der darauf aufbauenden Entscheidungen. Aufsichtsseitig wird zunehmend analysiert, ob Informationen entlang der gesamten Wertschöpfungskette konsistent definiert, qualitätsgesichert verarbeitet und adressatengerecht genutzt werden. Unklare Informationsverantwortlichkeiten, inkonsistente Datenhaushalte oder divergierende Informationsstände zwischen Fach- und Steuerungssystemen gelten als Indikatoren für strukturelle Schwächen im Steuerungsrahmen.

Die enge Wechselwirkung zwischen Organisationsstrukturen, technologischer Infrastruktur und Informationsmanagement wird damit zu einem zentralen Analysegegenstand. Organisationsstrukturen definieren die Spielregeln, technologische Infrastruktur setzt diese technisch um, und Informationsmanagement stellt sicher, dass die resultierenden Informationen belastbar sind. Aus aufsichtlicher Sicht ist entscheidend, ob diese Komponenten durchgängig aufeinander abgestimmt sind oder lediglich nebeneinander bestehende Einzelkonzepte darstellen. Typische Feststellungen betreffen Inkonsistenzen zwischen organisatorischen Vorgaben, IT-seitigen Prozessabbildungen und den tatsächlich genutzten Steuerungsinformationen. Solche Inkongruenzen führen nicht nur zu Effizienzverlusten, sondern gefährden die Verlässlichkeit von Steuerungs- und Überwachungsprozessen insgesamt und rücken damit in den Fokus der aufsichtlichen Bewertung.

4. Paradigmenwechsel durch technologische Abhängigkeitsstrukturen

Der aufsichtliche Analysefokus unterliegt im Zuge zunehmender technologischer Abhängigkeitsstrukturen einem deutlichen Paradigmenwechsel. An die Stelle einer primär retrospektiven Ordnungsmäßigkeitsprüfung tritt zunehmend eine zukunftsgerichtete Beurteilung der Widerstandsfähigkeit des Instituts. Aufsichtsliche Analysen zielen damit



weniger auf die Frage ab, ob bestehende Regelungen formal eingehalten wurden, sondern darauf, ob Organisationsstrukturen, technologische Infrastruktur und Steuerungsprozesse auch unter veränderten Rahmenbedingungen tragfähig ausgestaltet sind.

Im Mittelpunkt steht dabei die Analyse struktureller Abhängigkeiten. Hierzu zählen insbesondere die Bindung zentraler Steuerungsprozesse an einzelne IT-Systeme, die Nutzung externer Dienstleister sowie die Ausgestaltung der Systemlandschaft insgesamt. Konzentrationsrisiken, etwa durch hochgradig integrierte Kernbanksysteme oder eine starke Fokussierung auf wenige Auslagerungspartner, werden aus aufsichtlicher Sicht zunehmend kritisch bewertet. Entscheidend ist, ob das Institut diese Abhängigkeiten transparent identifiziert, angemessen steuert und in seine Risiko- und Notfallkonzepte integriert.

Ein weiterer Schwerpunkt liegt auf der Fähigkeit, auch bei IKT-Störungen steuerungsfähig zu bleiben. Aufsichtliche Analysen hinterfragen daher, ob Risikomessung, Liquiditätssteuerung und Berichterstattung im Störfall weiterhin in ausreichender Qualität möglich sind oder ob Steuerungsprozesse faktisch zum Erliegen kommen. Dabei rückt weniger die vollständige Vermeidung von Störungen als vielmehr der Umgang mit ihnen in den Fokus.

Die DORA-Verordnung verstärkt diesen Ansatz, indem sie klassische IT-Prüfungsansätze systematisch erweitert. Durch die explizite Verankerung von Anforderungen an Prävention, Detektion, Reaktion und Wiederherstellung wird digitale Widerstandsfähigkeit als kontinuierlicher Steuerungsprozess verstanden. Aufsichtliche Analysen bewerten folglich nicht isolierte Einzelmaßnahmen, sondern die Fähigkeit des Instituts, digitale Risiken vorausschauend zu adressieren und deren Auswirkungen auf die Gesamtinstitutssteuerung nachhaltig zu begrenzen.

5. Integration in die interne Kapital- und Liquiditätsadäquanzbeurteilung

Die Integration von Organisationsstrukturen, technologischer Infrastruktur und Informationsmanagement in die Gesamtinstitutssteuerung erfolgt konsequent entlang der Vorgaben zur internen Kapital- und Liquiditätsadäquanzbeurteilung sowie entsprechender aufsichtlicher Leitlinien. Beide Steuerungskreise verlangen eine ganzheitliche Betrachtung aller wesentlichen Risiken, die die Kapital- und Liquiditätsausstattung eines Instituts beeinflussen können. Vor diesem Hintergrund werden IKT-Risiken und Informationsqualitätsrisiken nicht mehr als reine operationelle Begleiterscheinungen verstanden, sondern als potenziell steuerungsrelevante Risikotreiber, die unmittelbar auf die Risikotragfähigkeit und die Liquiditätssteuerung wirken.

Aus aufsichtlicher Sicht wird zunehmend erwartet, dass diese Risiken systematisch in die Risikoinventur integriert sind. Maßgeblich ist dabei nicht allein die formale Zuordnung zur Risikokategorie der operationellen Risiken, sondern die inhaltliche Durchdringung ihrer Wirkungszusammenhänge. Technologie- und informationsbezogene Schwächen sollen



sich nachvollziehbar in Szenario- und Stresstests widerspiegeln, etwa durch Annahmen zu eingeschränkter Informationsverfügbarkeit, verzögerter Risikomessung oder eingeschränkter Zahlungsfähigkeit bei Systemausfällen. Entscheidend ist, ob diese Annahmen konsistent in die Kapital- und Liquiditätsplanung einfließen und in den Steuerungskennzahlen abgebildet werden.

Besondere Aufmerksamkeit gilt der Frage, ob die eingesetzten Systeme und Informationshaushalte die methodischen Anforderungen der internen Modelle tatsächlich tragen. Sowohl in der Kapitaladäquanzbeurteilung als auch in der Liquiditätssteuerung wird vorausgesetzt, dass Modelle auf belastbaren, konsistenten und aktuellen Informationen basieren. Aufsichtliche Analysen adressieren daher verstärkt, ob Informationsqualitätsdefizite, manuelle Korrekturen oder systemische Brüche die Aussagekraft der Modelle beeinträchtigen. Schwächen im technologischen oder Informationsumfeld werden dabei zunehmend als eigenständige Risikoart bewertet, die nicht lediglich durch Modellannahmen kompensiert werden dürfen, sondern aktiv zu steuern sind.

Darüber hinaus wird erwartet, dass sich IKT-Risiken und Informationsqualitätsrisiken nachvollziehbar in Steuerungsentscheidungen widerspiegeln. Dies betrifft insbesondere die Festlegung von Schwellenwerten, die Priorisierung von Investitionen in Systeme und Informationsqualität sowie die Ableitung von Maßnahmen bei identifizierten Defiziten. Eine rein technische Behandlung dieser Themen außerhalb der Steuerungsgremien wird aus aufsichtsrechtlicher Sicht als unzureichend angesehen.



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](#)