Prof. Dr. Andreas Igl
TH Deggendorf

Strukturelle Governance-Anforderungen im digitalen Bankgeschäft

Deggendorfer Notiz 2026/03 | 3. Februar 2026

Die Notiz beleuchtet strukturelle Governance-Anforderungen an Banken im digitalen Zeitalter. Im Mittelpunkt stehen Aufbau- und Ablauforganisation, Kontrolllinienmodell sowie das IKT-Risikomanagement unter DORA, KWG und MaRisk. Aufsichtlich relevant ist nicht die formale Regelungsexistenz, sondern deren operative Wirksamkeit. Typische Defizite bei Regionalbanken umfassen fragmentierte Strukturen, unklare Zuständigkeiten und Personenabhängigkeiten, die eine konsistente Gesamtinstitutssteuerung gefährden.

1. Grundanforderungen an Strukturen und Prozesse

Die Strukturierung von Aufbau- und Ablauforganisation bildet aus aufsichtlicher Perspektive den wesentlichen Bezugspunkt für die Beurteilung der Ordnungsmäßigkeit und Leistungsfähigkeit der Gesamtinstitutssteuerung. Ausschlaggebend ist, ob die organisatorischen Festlegungen geeignet sind, die Anforderungen aus strategischer Ausrichtung, Risikoprofil und fortschreitender Digitalisierung konsistent abzubilden. Der Beurteilungsmaßstab ergibt sich primär aus den gesetzlichen Governance-Vorgaben sowie den Mindestanforderungen an das Risikomanagement, die eine klare, transparente und wirksame Organisation verlangen, deren Ausgestaltung sich an Größe, Komplexität und Risikolage des Instituts orientiert.

Zentral für die aufsichtliche Analyse ist dabei nicht die formale Existenz organisatorischer Festlegungen, sondern deren Aktualität, Nachvollziehbarkeit und praktische Wirksamkeit. Organisatorische Vorgaben müssen schriftlich fixiert, eindeutig formuliert und regelmäßig überprüft werden. Fehlende Aktualisierungen, historisch gewachsene Sonderregelungen oder widersprüchliche Zuständigkeitsbeschreibungen werden regelmäßig als Governance-Mängel festgestellt. Besonders kritisch bewertet wird, wenn organisatorische Strukturen nicht erkennbar aus der strategischen Ausrichtung und der technologischen Strategie abgeleitet sind und damit keine konsistente Steuerungslogik erkennen lassen.

Mit Inkrafttreten von DORA erfährt dieser Beurteilungsmaßstab eine inhaltliche Konkretisierung. DORA fordert explizit eine klare organisatorische Verankerung der Verantwortung für IKT-Risiken und deren Steuerung. Für die Aufbauorganisation bedeutet dies, dass

bestehende Organisationsrichtlinien, Geschäftsverteilungspläne und Kompetenzregelungen systematisch auf DORA-Konformität zu überprüfen sind. Aufsichtlich wird erwartet, dass DORA-Anforderungen nicht isoliert in IT-nahen Dokumenten adressiert werden, sondern integraler Bestandteil der Gesamtorganisation sind. Parallele Regelungskreise oder isolierte Zuständigkeiten gelten als Indikatoren für eine unzureichende Governance-Reife.

Besondere aufsichtliche Aufmerksamkeit gilt den Schnittstellen zwischen Fachbereichen und technologischer Infrastruktur. Die Aufbauorganisation muss klar regeln, wer fachlich verantwortet, wer technisch umsetzt und wer überwacht. Unklare Abgrenzungen zwischen Linienfunktionen, zentralen Steuerungseinheiten und IT führen regelmäßig zu ineffizienten Entscheidungsprozessen und erhöhen das Risiko inkonsistenter Steuerungsimpulse. Aus aufsichtlicher Sicht ist daher entscheidend, ob die Organisation eine durchgängige Verantwortlichkeitskette vom strategischen Ziel bis zur operativen Umsetzung sicherstellt.

Auch die Ablauforganisation wird verstärkt unter Resilienzgesichtspunkten bewertet. Prozesse müssen nicht nur im Normalbetrieb funktionieren, sondern auch unter Stressbedingungen tragfähig bleiben. Aufsichtliche Analysen untersuchen, ob Entscheidungs- und Eskalationsprozesse bei IKT-Störungen, Informationsproblemen oder Ausfällen externer Dienstleister handlungsfähig ausgestaltet sind. Abläufe, die stark auf manuelle Eingriffe oder informelle Abstimmungen angewiesen sind, werden kritisch hinterfragt, da sie in Krisensituationen erfahrungsgemäß an ihre Grenzen stoßen.

Insgesamt wird eine konsistente Verzahnung von Organisation und technologischer Strategie erwartet. Historisch gewachsene Strukturen, die den heutigen digitalen Abhängigkeiten nicht mehr gerecht werden, stehen dabei besonders im Fokus. Die Aufbau- und Ablauforganisation wird somit zum Prüfstein dafür, ob Institute in der Lage sind, die steigenden Anforderungen an digitale Widerstandsfähigkeit und IKT-Risikosteuerung nachhaltig und steuerungswirksam in ihre Gesamtinstitutssteuerung zu integrieren.

2. Zuständigkeitsabgrenzungen und Kontrolllinienmodell

Die eindeutige Festlegung von Rollen und Verantwortlichkeiten stellt einen zentralen aufsichtlichen Schwerpunkt im Rahmen der Gesamtinstitutssteuerung dar. Aus aufsichtlicher Perspektive ist entscheidend, ob das Institut das Kontrolllinienmodell konsistent und durchgängig auch auf IKT-Risiken und Informationsqualitätsrisiken anwendet. Dabei geht es nicht allein um eine formale Zuordnung von Funktionen, sondern um die tatsächliche Wirksamkeit der Rollenverteilung im Zusammenspiel von Steuerung, Kontrolle und Überwachung.

Besondere Aufmerksamkeit gilt der Rolle des Vorstands, dem nach den gesetzlichen Governance-Vorgaben und explizit nach DORA eine nicht delegierbare

Gesamtverantwortung für die digitale operationelle Widerstandsfähigkeit zukommt. Aufsichtliche Analysen untersuchen, ob diese Verantwortung durch strukturierte Informations-, Berichts- und Eskalationsprozesse unterlegt ist oder ob in der Praxis eine faktische Delegation an die IT-Leitung stattfindet. Letzteres wird kritisch bewertet, da es regelmäßig zu einer Verkürzung der Governance-Kette und zu einer unzureichenden strategischen Einbindung von IKT-Risiken führt.

Die erste Kontrolllinie umfasst typischerweise den operativen IT-Betrieb sowie die Fachbereiche, die IT-gestützte Prozesse nutzen. Aufsichtlich wird hier eine klare Zuordnung der Verantwortung für den sicheren Betrieb von Systemen, die Informationsverarbeitung und die Einhaltung definierter Kontrollmechanismen erwartet. Unklare Zuständigkeiten oder informelle Abstimmungen zwischen Fachbereich und IT gelten als Risikofaktoren, insbesondere wenn zentrale Steuerungsprozesse betroffen sind.

Die zweite Kontrolllinie – bestehend aus Funktionen wie Risikocontrolling und Informationssicherheit – muss fachlich unabhängig ausgestaltet sein und über ausreichende Ressourcen verfügen. Aufsichtsseitig wird analysiert, ob diese Funktionen in der Lage sind, technologie- und informationsbezogene Risiken eigenständig zu bewerten, zu überwachen und gegenüber dem Vorstand transparent zu berichten. Häufige Feststellungen betreffen eine unzureichende personelle Ausstattung oder eine zu starke Nähe zum operativen IT-Bereich, wodurch die Kontrollfunktion faktisch geschwächt wird. Insbesondere die Abgrenzung zwischen IT-Leitung, IKT-Kontrollfunktion und Risikocontrolling erweist sich bei Regionalbanken regelmäßig als unscharf und unzureichend dokumentiert.

Auch die Interne Revision als dritte Kontrolllinie rückt stärker in den Fokus. Aufsichtlich wird erwartet, dass sie über ausreichende IT- und Informationskompetenz verfügt, um die Angemessenheit und Wirksamkeit der Steuerungs- und Kontrollprozesse sachgerecht beurteilen zu können. Eine rein formale Prüfung von Richtlinien ohne tiefgehendes Verständnis der Systemlandschaft wird zunehmend als nicht ausreichend angesehen. Defizite in der fachlichen Qualifikation der Revision führen regelmäßig zu Einschränkungen in der Prüfungsqualität und werden entsprechend adressiert.

Ein weiterer Schwerpunkt liegt auf der Regelung von Verantwortlichkeiten bei Auslagerungen und für Drittdienstleister. Auch bei der Nutzung externer IKT-Drittdienstleister verbleibt die Gesamtverantwortung beim Institut. Aufsichtlich wird daher bewertet, ob Rollen, Entscheidungsbefugnisse und Eskalationswege auch über Organisationsgrenzen hinweg klar definiert sind und ob die zweite Kontrolllinie Zugriff auf relevante Informationen erhält. Fehlende Transparenz in den Berichtswegen oder unklare Eskalationsmechanismen gelten als wesentliche Governance-Mängel.

Insgesamt wird eine konsistente Umsetzung der Rollen- und Verantwortlichkeitsmodelle über alle Organisationseinheiten hinweg erwartet. Typische Schwachstellen bei

Regionalbanken zeigen sich weniger in der konzeptionellen Ausgestaltung als in der praktischen Anwendung: Verantwortlichkeiten sind zwar beschrieben, werden jedoch nicht gelebt oder widersprechen sich zwischen verschiedenen Dokumenten. Die aufsichtliche Bewertung fokussiert daher zunehmend darauf, ob Governance-Strukturen nicht nur formal existieren, sondern tatsächlich die Steuerungs- und Überwachungsfähigkeit im Bereich Organisationsstrukturen, technologische Infrastruktur und Informationsmanagement nachhaltig unterstützen.

3. Institutionalisierung des technologiebezogenen Risikomanagements

Die organisatorische Verankerung des IKT-Risikomanagements ist aus aufsichtlicher Perspektive ein wesentlicher Bestandteil eines wirksamen Risikomanagementsystems. Maßgeblich ist, ob IKT-Risiken als integraler Bestandteil der Gesamtinstitutssteuerung verstanden und entsprechend in bestehende Steuerungs- und Überwachungsprozesse eingebettet sind. Eine isolierte Betrachtung von IKT-Risiken, losgelöst von anderen wesentlichen Risikoarten, wird zunehmend als nicht ausreichend beurteilt, da digitale Abhängigkeiten regelmäßig Wechselwirkungen mit operationellen, strategischen und finanziellen Risiken aufweisen.

Aufsichtliche Analysen legen besonderes Augenmerk auf die eindeutige Festlegung organisatorischer Zuständigkeiten. Erwartet wird, dass Verantwortlichkeiten für Identifikation, Bewertung, Steuerung und Überwachung von IKT-Risiken klar geregelt und dokumentiert sind. Unklare Rollenzuweisungen oder überlappende Zuständigkeiten zwischen IT, Informationssicherheit und Risikocontrolling erschweren eine konsistente Steuerung und werden als Governance-Schwäche bewertet. DORA verstärkt diese Anforderungen, indem sie explizit klare Zuständigkeiten sowie funktionierende Eskalationswege fordert, die auch in Stress- und Krisensituationen praktikabel sind.

Ein zentraler Analyseaspekt betrifft die Integration von IKT-Risiken in die Risikoinventur. IKT-Risiken sind regelmäßig zu identifizieren, zu bewerten und in ihrer Wesentlichkeit zu priorisieren. Häufige Feststellungen betreffen eine fehlende oder unzureichende Priorisierung, wodurch Steuerungsimpulse verwässert und Ressourcen nicht risikoadäquat eingesetzt werden. Ebenso aufsichtlich relevant sind die Schnittstellen zum operationellen Risikomanagement, da IKT-Risiken vielfach als Treiber operationeller Verlustereignisse wirken.

Darüber hinaus wird die Qualität der Risikoberichterstattung bewertet. Berichte müssen adressatengerecht ausgestaltet sein und es dem Vorstand ermöglichen, Risiken zu verstehen, Entscheidungen abzuleiten und Maßnahmen zu priorisieren. Aufsichtsseitig wird analysiert, ob Steuerungsimpulse aus dem IKT-Risikomanagement nachvollziehbar dokumentiert und in Entscheidungen überführt werden oder ob Berichte lediglich beschreibenden Charakter haben.

Wiederkehrende Schwachstellen zeigen sich in Dokumentationsdefiziten und fehlender Durchgängigkeit zwischen Konzeption und Umsetzung. Unvollständige oder inkonsistente Dokumentationen erschweren die aufsichtliche Nachvollziehbarkeit und lassen Zweifel an der tatsächlichen Wirksamkeit des IKT-Risikomanagements aufkommen. DORA fungiert hierbei als Verstärker, indem sie organisatorische Konsistenz nicht nur fordert, sondern explizit prüfbar macht und damit die Anforderungen an Struktur und Nachvollziehbarkeit deutlich erhöht.

4. Steuerungskreisläufe und Monitoring-Mechanismen

Die Qualität der Steuerungskreisläufe und Monitoring-Mechanismen stellt aus aufsichtlicher Perspektive ein zentrales Indiz für den Reifegrad des Governance-Systems dar. Bewertet wird, ob diese Prozesse nicht nur formal beschrieben, sondern tatsächlich wirksam ausgestaltet sind und einen kontinuierlichen Steuerungskreislauf ermöglichen. Im Fokus steht dabei insbesondere die Einbindung von IKT-Risiken und Informationsqualitätsrisiken in die bestehenden Steuerungsgremien der Bank sowie die Konsistenz zwischen Organisationsrichtlinien, strategischer Ausrichtung und technologischer Strategie.

Aufsichtlich wird erwartet, dass IKT-Risiken und Informationsrisiken regelmäßig und strukturiert auf Vorstandsebene adressiert und mit dem Aufsichtsrat erörtert werden. Eine rein anlassbezogene oder reaktive Berichterstattung wird als unzureichend angesehen, da sie keine vorausschauende Steuerung erlaubt. Entscheidend ist, ob die Berichte eine ausreichende Verdichtung der Informationen aufweisen, um Risiken angemessen beurteilen zu können, ohne dabei wesentliche Details zu verlieren. Zu stark aggregierte Darstellungen erschweren aus aufsichtlicher Sicht eine sachgerechte Bewertung der Risikolage und führen häufig zu Feststellungen.

Ein weiterer Analyseaspekt betrifft die Qualität der Entscheidungsgrundlagen. Steuerungsentscheidungen müssen auf belastbaren, aktuellen und konsistenten Informationen beruhen. Aufsichtliche Analysen untersuchen, ob die zugrunde liegenden Informationen verlässlich sind und ob Annahmen, Bewertungen und Handlungsoptionen nachvollziehbar dokumentiert wurden. Unklare oder widersprüchliche Entscheidungszuständigkeiten innerhalb der Gremien führen regelmäßig zu Governance-Mängeln, da sie eine eindeutige Verantwortung für getroffene Maßnahmen vermissen lassen.

Die Eskalation von Risiken ist ein weiteres zentrales Element wirksamer Steuerungsprozesse. Aufsichtlich wird bewertet, ob definierte Schwellenwerte, Meldewege und Eskalationsmechanismen existieren und tatsächlich angewendet werden. Verzögerte oder informelle Eskalationen werden kritisch gesehen, insbesondere wenn sie dazu führen, dass wesentliche Risiken nicht zeitnah auf der richtigen Entscheidungsebene behandelt werden. Steuerungskreisläufe und Monitoring-Mechanismen müssen daher klar dokumentiert, nachvollziehbar und für alle beteiligten Funktionen verbindlich sein.

Mit DORA werden diese Anforderungen weiter verschärft. Die Verordnung verlangt eine kontinuierliche Überwachung der IKT-Risiken sowie eine regelmäßige Überprüfung der zugrunde liegenden organisatorischen Regelungen. Aus aufsichtlicher Perspektive ist dabei besonders relevant, ob die Steuerungsprozesse auch in Stress- und Krisensituationen greifen und handlungsfähig bleiben. Eine rein formale Gremienstruktur ohne belastbare Entscheidungs- und Nachverfolgungsmechanismen wird als nicht ausreichend bewertet.

Schließlich analysieren aufsichtliche Bewertungen die Nachverfolgung von Maßnahmen, die aus Steuerungsentscheidungen resultieren. Erwartet wird, dass beschlossene Maßnahmen klar zugeordnet, terminiert und hinsichtlich ihrer Wirksamkeit überprüft werden. Defizite in diesem Bereich lassen Zweifel an der Nachhaltigkeit der Steuerung aufkommen und werden regelmäßig als Hinweis auf strukturelle Schwächen im Governance-System gewertet.

5. Identifizierte Defizite und Entwicklungsperspektiven

Abschließend rücken typische organisationsbezogene Schwachstellen verstärkt in den aufsichtlichen Fokus. Diese resultieren häufig aus historisch gewachsenen Strukturen, begrenzten personellen Ressourcen und einer hohen Abhängigkeit von einzelnen Schlüsselpersonen. Aufsichtlich wird regelmäßig festgestellt, dass Governance-Modelle zwar konzeptionell beschrieben sind, jedoch nicht durchgängig umgesetzt werden und damit ihre steuerungswirksame Funktion verlieren.

Ein zentrales Defizit liegt in fragmentierten Governance-Strukturen, bei denen organisatorische Regelungen nur teilweise konkretisiert oder nicht konsistent aufeinander abgestimmt sind. Neue regulatorische Anforderungen, insbesondere aus DORA, werden vielfach verzögert integriert oder isoliert in bestehenden Regelwerken ergänzt, ohne die Gesamtorganisation systematisch weiterzuentwickeln. Dies führt zu parallelen Strukturen, unklaren Zuständigkeiten und einer eingeschränkten Steuerungsfähigkeit.

Weit verbreitet sind zudem Zuständigkeitskonflikte zwischen Fachbereichen, IT, Informationssicherheitsfunktion, IKT-Kontrollfunktion und Risikocontrolling. Fehlende Klarheit über Verantwortlichkeiten bewirkt, dass Steuerungsimpulse auf operativer Ebene versanden oder nur unzureichend umgesetzt werden. In diesem Zusammenhang werden unvollständige oder veraltete Dokumentationen regelmäßig als Feststellung adressiert, da sie sowohl die interne Steuerung als auch die aufsichtliche Nachvollziehbarkeit erheblich beeinträchtigen.

Kritisch bewertet wird ferner die ausgeprägte Personenabhängigkeit in zentralen Steuerungs- und Kontrollfunktionen. Wenn Wissen, Entscheidungsbefugnisse oder Prozesse nicht ausreichend institutionalisiert sind, entstehen erhebliche operationelle und steuerungsrelevante Risiken. Diese werden durch Ressourcenengpässe zusätzlich verstärkt,

da Kontroll- und Überwachungsfunktionen ihre Aufgaben nur eingeschränkt wahrnehmen können.

Aus aufsichtlicher Perspektive liegen wesentliche Entwicklungsperspektiven in der klaren Strukturierung und Weiterentwicklung der Organisationsmodelle. Erforderlich ist eine stärkere Verzahnung von Organisationsstrukturen, technologischer Infrastruktur und Informationsmanagement, die über formale Anpassungen hinausgeht und die tatsächlichen Steuerungsprozesse adressiert. Erwartet wird eine proaktive Governance-Weiterentwicklung, bei der DORA nicht isoliert umgesetzt, sondern als integraler Bestandteil der Gesamtinstitutssteuerung verstanden wird. Der durch DORA deutlich erhöhte Handlungsdruck macht deutlich, dass organisatorische Schwächen nicht länger als Randthema betrachtet werden können, sondern unmittelbar die aufsichtsrechtliche Beurteilung der Steuerungs- und Überwachungsfähigkeit prägen.

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