Positionspapier

Digitale Souveränität und Resilienz im Bankensektor – Handlungsfähigkeit in einer vernetzten Welt sichern

- Digitale Souveränität und Cloud-Strategien
- Regulatorische Aspekte neuer Technologien
- DORA-Review
- Regulatorische Kohärenz und Entlastung

13.04.2026

Executive Summary

Das europäische Banken- und Finanzwesen steht vor komplexen Herausforderungen durch technologische Innovationen, digitale Vernetzung und zunehmende regulatorische Anforderungen. Digitale Souveränität, regulatorische Compliance, operative Resilienz und Innovationsfähigkeit sind heute eng miteinander verknüpft. Dieses Dokument beleuchtet die zentralen Handlungsfelder und gibt Orientierung für Banken, Aufsicht und Politik.

1. Digitale Souveränität und Cloud-Strategien

Banken müssen ihre Handlungs- und Entscheidungsfähigkeit in einer global vernetzten IT-Landschaft bewahren. Digitale Souveränität bedeutet keine Autarkie und auch keine ausschließliche Nutzung von Lösungen und Produkten aus der EU, sondern Entscheidungshoheit über Daten, Infrastruktur und Anwendungen einschließlich der Nutzung globaler Anbieter, sofern eine selbstbestimmte und sichere Nutzung unter Vermeidung von Lock-In-Szenarien gewährleistet werden kann. Hybride und Multi-Cloud-Strategien sowie moderne Architekturen erhöhen Resilienz und Flexibilität und bieten entsprechend große Chancen. Sie sind aber auch in der Regel mit erheblicher, zusätzlicher Komplexität und nicht zuletzt Kosten verbunden. Der Einsatz neuer Technologien wie KI erfordert eine transparente Governance sowie eine strategische Risikobewertung und eine aktive Steuerung von Abhängigkeiten.

2. Regulatorische Aspekte neuer Technologien

Neue Technologien wie KI, Automatisierung, serviceorientierte Architekturen mit Fokus auf API oder Cloud-native Entwicklungs- und Betriebsmodelle verändern Bankprozesse grundlegend. Die bestehenden, technologieneutralen Regelwerke stoßen hierbei an Auslegungsgrenzen, wenn es z.B. um die Operationalisierung der angemessenen Kontrolle im Kontext sich selbst weiterentwickelnder Systeme oder Multi-Cloud-Setup und dann noch mit containerisierten, dynamisch skalierende Workloads geht. Banken benötigen ausreichend flexible Aufsichtsspielräume, die

Bundesverband Öffentlicher Banken Deutschlands, VÖB, e.V.
Lennéstraße 11, 10785 Berlin
www.voeb.de

Präsident: Thomas Groß
Stellvertretender Präsident: Erk Westermann-Lammers
Hauptgeschäftsführerin und geschäftsführendes Vorstandsmitglied: Iris Bethge-Krauß

Registernummer im Lobbyregister: R001169

risikoorientierte, proportionale und praxisgerechte Umsetzung ermöglichen, ohne Innovation oder Wettbewerbsfähigkeit zu blockieren. Qualität, Konsistenz und Timing von Primär- und Sekundärrechtsakten sind entscheidend für Umsetzbarkeit und Planbarkeit.

3. DORA-Review: Proportionalität und Praxistauglichkeit

DORA schafft einen einheitlichen Rahmen für das Management von IKT-Risiken. Banken begrüßen das Ziel, erleben jedoch erheblichen Aufwand bei Dokumentation, Drittparteienmanagement und Meldewesen. Das Proportionalitätsprinzip ist bislang unzureichend operationalisiert. Die anstehende DORA-Review sollte praxisnahe Anpassungen ermöglichen, u. a.:

- Einführung einer mittleren Kategorie für nicht systemrelevante, aber größere Institute,
- Anerkennung bestehender Sicherheitsstandards zur Vermeidung von Doppelprüfungen,
- Optimierung von Meldeprozessen, Schwellenwerten und Nutzung des Single Entry Points.

4. Regulatorische Kohärenz und Entlastung (Querschnittsthema)

Die Vielzahl neuer und bestehender IT-bezogener Regelungen führt zu redundanten Anforderungen und erhöhtem Aufwand. Kohärenz, Harmonisierung und proportional ausgestaltete Vorgaben sind entscheidend, um operative Belastungen zu reduzieren, Innovationszyklen zu sichern und digitale Resilienz zu stärken. Differenzierung nach Systemrelevanz ermöglicht gezielte Entlastung nicht systemrelevanter Institute.

1. Digitale Souveränität und Cloud-Strategien
Handlungsfähigkeit sichern in einer global vernetzten IT-Landschaft

1.1 Digitale Souveränität: Keine Autarkie, sondern Entscheidungshoheit

Resilienz, Unabhängigkeit und digitale Souveränität sind heute zentrale Themen sowohl im politischen Diskurs als auch in der Finanzindustrie. Auslöser hierfür sind unter anderem unerwartete geopolitische Verwerfungen sowie politische Sanktionen, die Abhängigkeiten und Anfälligkeiten in globalen Wertschöpfungs- und Technologieketten z.B. durch längere Lieferzeiten und Preisschwankungen sichtbar machen. **Vor diesem Hintergrund müssen IT-seitige Abhängigkeiten neu bewertet werden – ökonomisch, technologisch und sicherheitspolitisch.**

Für Finanzinstitute stellt sich insbesondere die Frage, wie mit den veränderten Eintrittswahrscheinlichkeiten der mit strategischen digitalen Abhängigkeiten verbundenen Risiken umzugehen ist. Welche technologischen Optionen sind realistisch, wirtschaftlich tragfähig und langfristig steuerbar? Welche Abhängigkeiten lassen sich reduzieren oder diversifizieren, und welche verbleiben zwangsläufig trotz erheblicher Anstrengungen?

Eine vollständige digitale Souveränität im Sinne technologischer Autarkie ist weder erreichbar noch erstrebenswert. Erforderlich ist vielmehr eine pragmatische Sichtweise, die auf Wahlfreiheit, Flexibilität und bewusster Steuerung von Abhängigkeiten basiert. Ziel muss es sein, ein ausgewogenes Verhältnis zwischen Kontrolle und der Nutzung leistungsfähiger, wettbewerbsfähiger Angebote im nationalen, europäischen und globalen Umfeld zu finden. Der Aufbau digitaler Resilienz darf nicht als Gegengewicht zur Innovationsfähigkeit verstanden werden. Vielmehr bildet ein robustes,

technologisch modernes Fundament die Voraussetzung dafür, Innovationen sicher, skalierbar und vertrauenswürdig einzusetzen. Ohne ein angemessenes Resilienzniveau werden neue Technologien selbst zum Wettbewerbsrisiko. Gerade für Banken ist es entscheidend, neue Technologien zeitnah einzusetzen, um regulatorische Anforderungen effizient zu erfüllen, operative Risiken zu beherrschen und im internationalen Wettbewerb bestehen zu können.

Digitale Souveränität bedeutet im Bankenkontext die Fähigkeit, **digitale Ressourcen, Daten und Technologien selbstbestimmt, sicher und regelkonform zu steuern – einschließlich der Nutzung externer Anbieter, der aktiven Steuerung von Abhängigkeiten sowie der jederzeitigen Wahrung der eigenen Entscheidungs- und Handlungsfähigkeit**. Sie ist kein Ziel vollständiger technologischer Unabhängigkeit; in einer globalisierten digitalen Ökonomie wäre Autarkie weder realistisch noch wirtschaftlich sinnvoll.

Souverän handelt, wer technologische Entscheidungen eigenständig treffen kann, Alternativen kennt und Abhängigkeiten aktiv steuert. Dies schließt ausdrücklich die Nutzung globaler Technologieanbieter ein, insbesondere dort, wo Innovationsimpulse derzeit maßgeblich von Drittanbietern, häufig aus den USA, ausgehen. Digitale Souveränität bedeutet nicht Abschottung, sondern die bewusste Gestaltung unvermeidbarer Abhängigkeiten. Sie umfasst nicht nur die formale Kontrolle, sondern die tatsächliche Handlungsfähigkeit und Selbstbestimmung über geschäftskritische und differenzierende Assets, transparente Strukturen sowie realistische Wahl- und Exit-Optionen.

Die Prämisse der Entscheidungsfreiheit wirkt sich insbesondere auf Cloud-Strategien, Datenkontrolle und den Einsatz neuer digitaler Features aus – Themen, die im Folgenden näher beleuchtet werden.

1.2 Cloud-Strategien als Fundament digitaler Handlungsfähigkeit

Im Infrastrukturbereich sind viele Banken heute bereits weit fortgeschritten. Hybride und Multi-Cloud-Strategien, etwa durch die Kombination mehrerer Hyperscaler mit eigenen Rechenzentren, bilden das Rückgrat moderner Bank-IT. Der Einsatz von Container- und Kubernetes-Architekturen erhöht die Portabilität von Anwendungen und ermöglicht es, Workloads flexibel zu verlagern.
Diese Architekturansätze schaffen keine vollständige Austauschbarkeit von Cloud-Anbietern – spezifische Services, Tools und Analysefunktionen sind häufig nicht gleichwertig substituierbar.
Dies liegt daran, dass Cloud-Dienste häufig auf proprietären Technologien beruhen. Zudem wirken extraterritoriale Rechtsnormen (US CLOUD Act, FISA702) selbst bei Datenhaltung in Europa.

Dennoch stärken sie die **strategische Resilienz**, da sie Abhängigkeiten reduzieren und Exit-Optionen zumindest grundsätzlich offenhalten. Entscheidend ist dabei weniger die technische Perfektion als die Tatsache, dass die **Entscheidungshoheit über die Infrastruktur** bei den Banken verbleibt – auch wenn dies mit wachsender Komplexität und höheren Steuerungsanforderungen einhergeht.

1.3 Datenkontrolle als Kern bankenspezifischer Souveränität

Ein hohes Maß an digitaler Souveränität besteht bei Banken traditionell im Umgang mit Daten. Durch Verschlüsselung – auch in Cloud-Umgebungen –, klar definierte Zugriffskonzepte und den Verbleib der kryptographischen Schlüssel in eigener Hoheit behalten Banken jederzeit die Kontrolle über ihre Daten. Daten können gesichert, verschoben und ausgewertet werden, ohne strukturell auf einzelne Anbieter angewiesen zu sein. Diese Datenhoheit ist ein zentraler Baustein bankenspezifischer digitaler

Souveränität und bildet zugleich die Grundlage für regulatorische Compliance, Informationssicherheit und Vertrauen und damit Resilienz. Sie ist damit entscheidend für die Wettbewerbsfähigkeit.

1.4 Neue Abhängigkeiten durch innovative digitale Features und KI

Deutlich komplexer stellt sich die Lage bei darüberliegenden digitalen Funktionen dar – insbesondere bei KI-basierten Services, Automatisierungslösungen und spezialisierten Entwicklungs- und Analysewerkzeugen. In diesen Bereichen dominieren derzeit wenige, hochinnovative Anbieter zumeist aus den USA, deren Lösungen tief in bestehende Plattformen und Prozesse integriert sind.

Solche Abhängigkeiten lassen sich aktuell kaum vermeiden und sind aus Innovations- und Effizienzgesichtspunkten vielfach bewusst eingegangen worden. Sie müssen jedoch **transparent gemacht, aktiv gemanagt und strategisch bewertet** werden – auch mit Blick auf regulatorische Anforderungen, Konzentrationsrisiken und langfristige Steuerungsfähigkeit. Für den praktischen Einsatz von KI-basierten Lösungen – insbesondere in sensiblen Bereichen wie Softwareentwicklung, Testing oder produktionsnahen Prozessen – kann es sinnvoll sein, bestehende Anforderungen durch klarere, praxisnahe Mindestleitplanken zu konkretisieren. Diese sollten sich auf Basiselemente wie Nachvollziehbarkeit, Validierung, Dokumentation und Kontrollmechanismen beschränken. Ziel ist keine zusätzliche Detailregulierung, sondern eine konsistente Auslegung, die einen sicheren und verlässlichen Einsatz von KI unterstützt, ohne Innovationsspielräume unnötig einzuschränken.
Im Kontext etablierter Kontrollprinzipien stellt sich zudem die Frage, wie KI in bestehende Governance-Modelle integriert werden kann. Dies betrifft insbesondere das Vier-Augen-Prinzip. In der Praxis wird KI bereits teilweise unterstützend eingesetzt, etwa als „erstes Augenpaar“ bei Analysen, Coding oder Prüfprozessen. Eine Klarstellung der aufsichtsrechtlichen Erwartungen – insbesondere dahingehend, dass die Letztverantwortung weiterhin beim Menschen verbleibt und unter welchen Bedingungen KI unterstützend eingebunden werden kann – würde hier zusätzliche Rechtssicherheit schaffen.
Europäische Alternativen befinden sich vielfach noch im Aufbau; staatliche und europäische Fördermaßnahmen sind wichtig, können aber den bestehenden Investitionsvorsprung globaler Anbieter kurzfristig nicht ausgleichen.

1.5 Implikationen und Erwartungen aus Sicht der Banken

Digitale Souveränität entsteht nicht durch zusätzliche Regulierung, sondern durch **Rahmenbedingungen**, die eigenverantwortliche technologische Entscheidungen ermöglichen.

Wir brauchen ein **starkes und wettbewerbsfähiges IKT-Ökosystem**, um – nicht nur – den Finanzinstituten die Freiheit zu geben, die für sie geeigneten Technologien und Dienstleistungen auszuwählen. Dabei muss anerkannt werden, dass europäische Anbieter insbesondere im Bereich Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS)derzeit in der Breite und Tiefe kein vergleichbares funktionales Niveau wie bspw. die global führenden US-Cloud-Anbieter erreichen. Hier wieder die vollständige Kontrolle über alle IKT-Wertschöpfungsebenen zu erreichen, ist komplex und erfordert hohe Investitionen. Dabei geht es aber nicht nur um Investitionen, sondern vor allem um den Aufbau spezialisierten Know-hows und einer belastbare Governance. Durch die langfristige Schaffung von Plattformen, die den Austausch bewährter Verfahren unterstützen, sowie die Förderung von offenen Standards und interoperablen Lösungen kann die digitale Souveränität wirksam gestärkt

werden. Dadurch kann Europa eine Vorreiterrolle im Bereich der digitalen Souveränität einnehmen, während gleichzeitig die Wahlfreiheit und Wettbewerbsfähigkeit der Institute gefördert wird. Insbesondere können Institute – und andere Wirtschaftszweige auch - ihre Unabhängigkeit durch lokale Lösungen und Partnerschaften mit europäischen Anbietern stärken und die Compliance mit lokalen Datenschutzbestimmungen sicherstellen. Eine vollständige, in allen Dimensionen uneingeschränkte Cloud-Souveränität ist in global vernetzten IT-Ökosystemen faktisch kaum erreichbar.

Zielführender ist es, ein institutsspezifisches Ambitionsniveau digitaler Souveränität zu definieren – differenziert nach Dimensionen wie Datenhoheit, operative Steuerungsfähigkeit, architektonische Portabilität und vertragliche Transparenz. US-Souveränität wird damit zu einer strategischen Gestaltungsaufgabe und nicht zu einem absoluten Zustand. Daher gilt es als Teil dieser Rahmenbedingungen gemeinsam auf europäisch-staatlicher und wirtschaftlicher Ebene Anreize zu schaffen, die Innovationen unterstützen und in aufkommende Technologien investieren. So wären beispielsweise Super-Abschreibungen, Steuervorteile und ähnliche Maßnahme denkbar. Staatliche Förderprogramme können zudem dazu beitragen, Forschungs- und Entwicklungsinitiativen zu intensivieren sowie die Zusammenarbeit zwischen Unternehmen und Hochschulen zu fördern. Auch die Förderungen von Praxis-Kooperationen mit Universitäten und Unternehmen für zusätzliche Synergien erweitern nicht nur das technische Know-how, sondern ermöglichen die Entwicklung maßgeschneiderter Lösungen für die spezifischen Anforderungen der Finanzbranche.

Bestehende regulatorische Vorgaben sind überwiegend **technologieneutral und risikoorientiert** formuliert. Entscheidend ist jedoch, dass auch ihre Auslegung und Anwendung praxisgerecht erfolgen und aus legitimen Anforderungen an Steuerbarkeit keine impliziten Erwartungen an vollständige technologische Autarkie oder uneingeschränkte Substituierbarkeit werden. Beispielhaft seien hier mögliche rein europäische Zertifikate genannt, die die Lebenswirklichkeit nicht abbilden.

Entscheidend ist zudem eine **europäisch abgestimmte Auslegung und Aufsichtspraxis**, die Wahlfreiheit und Innovationsfähigkeit nicht durch divergierende nationale Erwartungen einschränkt. Digitale Souveränität setzt voraus, dass Banken globale Technologien verantwortungsvoll einsetzen dürfen, solange Steuerbarkeit, Transparenz und Risikomanagement sichergestellt sind.

Darüber hinaus bedarf es einer **klaren Verzahnung von Regulierung, Innovationspolitik und Standortstrategie**. Der Aufbau europäischer Alternativen sollte gezielt gefördert werden, ohne die Nutzung bestehender internationaler Lösungen zu behindern. Banken müssen in der Lage bleiben, Innovationen frühzeitig zu adaptieren, um im internationalen Wettbewerb bestehen zu können – gerade vor dem Hintergrund geopolitischer Spannungen und strategischer Abhängigkeiten.

Nicht zuletzt ist digitale Souveränität auch eine **Governance-Aufgabe der Institute selbst**. Sie erfordert klare Verantwortlichkeiten, Transparenz über Abhängigkeiten sowie realistische Exit- und Substitutionsstrategien, die regelmäßig überprüft und weiterentwickelt werden.

Unsere Petita zur Stärkung digitaler Souveränität im Bankensektor

1. **Keine implizite Autarkieerwartung aus der Regulierung**
   Gesetzgeber und Aufsicht sollten in Auslegung und Anwendung zur Vermeidung von Fehlinterpretationen in der Diskussion z.B. rund um Konzentrationsrisiken, Exit-Strategien, Multi-Vendor-Anforderungen deutlich machen, dass regulatorische Anforderungen auf die Beherrschbarkeit von Risiken abzielen – nicht **vollständige technologische Substituierbarkeit oder europäische Autarkie**
2. **Technologieneutrale und risikoorientierte Anwendung bestehender Regeln**
   Die risikoorientierte Anwendung bestehender Regelwerke sollte in der Aufsichtspraxis konsistent an tatsächlicher **Kritikalität und konkreten Risikoprofilen** ausgerichtet werden.
3. **Europäisch einheitliche Aufsichtspraxis sicherstellen**
   Divergierende nationale Auslegungen regulatorischer Anforderungen sind zu vermeiden. Banken benötigen **europaweit konsistente Erwartungen**, insbesondere bei Cloud-Nutzung, Drittparteienmanagement und Exit-Strategien.
4. **Regulierung nur bei nachgewiesenem Regelungsbedarf („Regulate when needed“)**
   Neue regulatorische Vorgaben sollten **erst dann geschaffen werden**, wenn ein konkreter, nachgewiesener Regelungs- oder Aufsichtsmangel besteht – nicht präventiv zulasten von Innovation und Wettbewerbsfähigkeit.
5. **Anerkennung von digitaler Souveränität als mehrdimensionales, risikoorientiertes Zielbild**
   Digitale Souveränität entfaltet sich in unterschiedlichen Dimensionen – etwa Datenzugriff, Governance-Strukturen, operative Steuerungsfähigkeit oder Exit-Optionen. Regulatorische Konzepte sollten anerkennen, dass Institute je nach Geschäftsmodell und Risikoprofil ein angemessenes Souveränitätsniveau definieren und umsetzen. Vollständige technologische Entkopplung ist kein regulatorisches Erfordernis; maßgeblich ist die beherrschbare und verantwortete Gestaltung von Abhängigkeiten.
6. **Förderung offener Standards und Interoperabilität statt Sonderzertifikate**
   Politische und regulatorische Initiativen sollten auf international anschlussfähige Standards, Interoperabilität und technische Portabilität setzen. Zusätzliche, nicht harmonisierte Zertifizierungsanforderungen erhöhen Komplexität und Kosten, ohne zwangsläufig einen proportionalen Sicherheitsgewinn zu erzeugen.
7. **Gezielte Innovations- und Investitionsanreize statt zusätzlicher Pflichten**
   Der Aufbau europäischer Technologiekompetenzen sollte primär über **steuerliche Anreize, Super-Abschreibungen, Förderprogramme und F&E-Kooperationen** erfolgen – nicht über regulatorische Nutzungshürden.
8. **Praxisnahe Berücksichtigung geopolitischer Realitäten**
   Regulatorische Anforderungen sollten anerkennen, dass globale Abhängigkeiten kurzfristig nicht vollständig eliminierbar sind. Banken müssen dabei Handlungsspielräume erhalten, um Risiken strategisch zu steuern und durch Diversifikation, Vertragsanpassungen oder technische Maßnahmen zu mitigieren. Eine Grundlage liefert dafür schon heute das Risikoinventar.
9. **Anerkennung institutsspezifischer Governance statt Detailvorgaben**
   Aufsicht und Gesetzgeber sollten stärker auf **interne Governance-, Risiko- und Steuerungskompetenzen** der Institute setzen und diese nutzen, statt sie durch kleinteilige Nachweispflichten zu ersetzen.
10. **Verzahnung von Regulierung, Innovationspolitik und Standortstrategie**
    Digitale Souveränität erfordert ein **kohärentes Zusammenspiel** von Finanzmarktregulierung, Digital- und Innovationspolitik sowie europäischer Standortstrategie – abgestimmt, langfristig und wettbewerbsorientiert über Behördensilos hinweg als ganzheitliche Strategie.

2. Regulatorische Aspekte neuer Technologien
Innovation ermöglichen innerhalb bestehender Regelwerke

2.1 Neue Technologien in einem bestehenden Regulierungsrahmen

Die regulatorischen Rahmenwerke im Bankenbereich sind **traditionell technologieneutral** formuliert. Sie wurden jedoch in einer Phase konzipiert, in der cloudgestützte Entwicklungs- und Betriebsmodelle, KI-basierte Entscheidungsmodelle oder hochgradig automatisierte Entwicklungsprozesse noch nicht prägend waren. In der Anwendungspraxis entstehen daraus Spannungsfelder zwischen innovationsgetriebener IT-Transformation und risikoorientierter Aufsicht. Mit horizontalen Digitalregimen wie dem AI enAct zeichnet sich zugleich ein Paradigmenwechsel hin zu technologiebezogener Regulierung ab. Funktionsbezogene Aufsicht und technologiespezifische Vorgaben überlagern sich damit zunehmend.

Für Banken bewegen sich neue Technologien nicht in einem rechtsfreien Raum, sondern müssen in bestehende aufsichtsrechtliche Rahmenwerke integriert werden – insbesondere in die Vorgaben zu Governance und interner Kontrolle (z. B. MaRisk), zum IKT-Risikomanagement (DORA), zum Auslagerungs- und Drittparteienmanagement (MaRisk AT 9, DORA Kapitel V), zur Informationssicherheit (DORA) sowie zu Datenschutz und Compliance (DSGVO, bankaufsichtliche Geheimhaltungspflichten).
In der praktischen Anwendung zeigen diese Regelwerke jedoch zunehmend Auslegungs- und Umsetzungsgrenzen, wenn hochdynamische Technologien wie Cloud-native Architekturen, KI-basierte Systeme oder modulare Plattformökosysteme eingesetzt werden. Anforderungen an vollständige Transparenz, jederzeitige Steuerbarkeit, detaillierte Vorab-Dokumentation und formale Prüfrechte lassen sich bei lernenden Systemen, global verteilten Cloud-Services oder tief integrierten Standardplattformen nur eingeschränkt erfüllen, ohne Innovation, Geschwindigkeit und Skalierbarkeit erheblich zu beeinträchtigen.

Der regulatorische Handlungsbedarf liegt daher weniger in neuen Regelungen als in einer **risikoorientierten, technologieneutralen und proportionalen Auslegung bestehender Vorgaben**, die Innovationsfähigkeit ermöglicht, ohne die Steuerbarkeit und Sicherheit der Institute zu gefährden. Dies beinhaltet auch die Anerkennung institutsspezifischer Governance- und Kontrollkonzepte sowie eine Abkehr von impliziten Anforderungen an vollständige technische Beherrschbarkeit oder Substituierbarkeit jeder einzelnen Technologiekomponente.

2.2 KI und Automatisierung: Risiko-, Kontroll- und Verantwortungsfragen

Der Einsatz von KI-basierten Systemen und weitreichender Automatisierung stellt besondere regulatorische Herausforderungen dar. Banken sind daher bereits heute schon durch die Gesetzgeber und die Aufsicht gefordert, **angemessene Governance-, Validierungs- und Überwachungsmechanismen** zu etablieren, ohne Innovationen durch übermäßige Vorsicht faktisch auszubremsen. Bestehende Vorgaben zu Modellrisiken, internen Kontrollen, Nachvollziehbarkeit von Entscheidungen und Verantwortlichkeiten sind grundsätzlich anwendbar, lassen sich jedoch nicht immer ohne Weiteres auf lernende, adaptive Systeme übertragen.

Für Banken ergibt sich daraus ein Spannungsfeld: Dieses Spannungsfeld wird in der Praxis durch etablierte Governance-Mechanismen – etwa Human-in-the-Loop-Ansätze, Modellvalidierung oder

kontinuierliches Monitoring – adressiert. Zugleich verändert der Einsatz komplexer und teilweise vortrainierter Modelle die Anforderungen an Transparenz, Verantwortungszuordnung und Kontrolltiefe. Dies erfordert eine Weiterentwicklung der Aufsichtsperspektive.

2.3 APIs, modulare IT-Landschaften und neue Abhängigkeiten

Serviceorientierte Architekturen mit Fokus auf APIs sowie modulare, Cloud-zentrische IT-Landschaften sind zentrale Enabler für Innovation, Kooperation und Skalierbarkeit. Sie ermöglichen es Banken, neue Services schnell zu integrieren, Partner anzubinden und bestehende Systeme schrittweise weiterzuentwickeln. Regulatorisch relevant sind dabei insbesondere Fragen der Auslagerung, der Drittparteiensteuerung sowie der Informationssicherheit.

Bestehende Regelungen – etwa zu Auslagerungen und IKT-Risiken – sind grundsätzlich anwendbar, erfassen jedoch die **Granularität und Dynamik** moderner API-Services und modularer IT-Landschaften nur eingeschränkt. Die Abgrenzung zwischen internen Leistungen, Fremdbezug, technischer Schnittstelle und kritischer Dienstleistung ist insbesondere in heterogenen und modularen IT-Landschaften anspruchsvoll. In der Anwendungspraxis können formale Vorgaben – etwa die Einordnung oben genannter Leistungen – zu pauschalen Einstufungen führen, die der tatsächlichen Risikostruktur heterogener und modularer IT-Landschaften nicht vollständig gerecht werden. Wie bereits unter 2.1 genannt, liegt die Herausforderung weniger im Fehlen regulatorischer Vorgaben als in deren Anwendung auf hochgradig modulare und dynamische Architekturen. Sinnvoller ist eine **Anknüpfung an das konkrete Risikoprofil der jeweiligen Funktion – etwa Kritikalität, Datenbezug, Substituierbarkeit und tatsächliche Steuerbarkeit – und nicht an die eingesetzte Technologie** selbst. So kann der Granularität heterogener und modularer IT-Landschaften Rechnung getragen und eine flexible Nutzung innovativer Architekturen ermöglicht werden. Gesetzgeber und Aufsicht sollten dies entsprechend klarstellen. Alternativ kann auch ein einheitlicher Rahmen für IKT- und Non-IKT-Leistungen zur Erhöhung von Transparenz und Steuerbarkeit eine Lösung darstellen.

2.4 Technologieneutralität braucht Auslegungsspielräume

Ein zentrales Prinzip der Finanzmarktregulierung ist die Technologieneutralität, das auch im Kontext neuer Technologien richtig und notwendig bleibt. In der praktischen Umsetzung erfordert es jedoch ausreichende Auslegungsspielräume – sowohl für Institute als auch für Aufsichtsbehörden. Diese Spielräume zeigen sich etwa bei der Anwendung bestehender Vorgaben auf modulare IT-Architekturen oder den Einsatz von Cloud- und KI-Systemen, wo die Anforderungen an Dokumentation, Verantwortlichkeiten und Steuerbarkeit nicht pauschal festgelegt werden können, sondern vom individuellen Risikoprofil des Instituts abhängen. Statt detaillierter technologiebezogener Vorgaben benötigen Banken einen **Rahmen, der risikoorientierte, proportionale und innovationsfreundliche Lösungen erlaubt**. Entscheidend ist nicht die konkrete Technologie, sondern deren Kritikalität und Einbettung in die Gesamtarchitektur. Eine zu starre oder formalistische Anwendung bestehender Regeln würde ansonsten die Einführung neuer Technologien unnötig verzögern oder verhindern**.**

2.5 Qualität und Timing regulatorischer Vorgaben (Primär- und Sekundärrecht)

Neben der inhaltlichen Ausgestaltung regulatorischer Anforderungen kommt der **Qualität und dem zeitlichen Zusammenspiel von Primär- und Sekundärrechtsakten** eine zentrale Bedeutung zu. Für

Banken ist nicht die Anzahl regulatorischer Vorgaben entscheidend, sondern ihre Verständlichkeit, Konsistenz und praktische Anwendbarkeit im jeweiligen Risikokontext.

Auf Ebene der **Primärrechtsakte** besteht der Bedarf an wenigen, dafür klaren, eindeutigen und konkreten Vorgaben, die eine zielgerichtete Umsetzung ermöglichen. Dazu gehören neben klar benannten Zielen auch konkrete Erwartungen sowie eine nachvollziehbare Beschreibung des Rahmens für delegierte Rechtsakte. Wesentlich ist zudem, dass bereits im jeweiligen Gesetz festgelegt wird, **welcher Umsetzungszeitraum den Marktteilnehmern nach Finalisierung der delegierten Rechtsakte tatsächlich zur Verfügung steht**. Konkrete Umsetzungsfristen sollten erst mit der Finalisierung konkretisierender delegierter Rechtsakte (Level 2) starten.

Die derzeit häufig praktizierte Vorgehensweise – Benennung einer Umsetzungsfrist unter Einbeziehung der Erarbeitung delegierter Rechtsakte – verkürzt die effektive Umsetzungszeit für die Institute erheblich. In der Praxis erfolgt die finale Freigabe delegierter Rechtsakte durch die Europäischen Aufsichtsbehörden und die Europäische Kommission teilweise deutlich zeitversetzt zur fachlichen Fertigstellung. Weitere Verzögerungen entstehen, wenn nachträglich Änderungen eingebracht werden. Diese zeitlichen Unsicherheiten erschweren eine strukturierte und ressourcenschonende Umsetzung erheblich.

Auf Ebene der **Sekundärrechtsakte** ist eine rechtzeitige, mandatsgetreue Finalisierung der zur Erfüllung der gesetzlichen Vorgaben zwingend notwendigen Regelungen essenziell. Das Inkrafttreten sollte konsequent an die vollständige Finalisierung und formale Freigabe des jeweiligen Rechtsaktes – etwa durch Veröffentlichung im EU-Amtsblatt – gekoppelt werden. Erst ab diesem Zeitpunkt sollte der Umsetzungszeitraum für den Markt beginnen.

Ein solcher Ansatz würde Planbarkeit, Rechtssicherheit und Umsetzungsqualität deutlich erhöhen – und damit sowohl den Instituten als auch der Aufsicht zugutekommen.

2.6 Implikationen und Erwartungen aus Sicht der Banken

Vor dem Hintergrund zunehmender geopolitischer Spannungen und globaler Technologieabhängigkeiten gehen Banken davon aus, dass neue Technologien innerhalb des bestehenden regulatorischen Rahmens genutzt werden können. Entscheidend ist, dass Risiken angemessen gesteuert werden, ohne dass Innovation oder Wettbewerbsfähigkeit durch übermäßige Formalisierung oder eine zu enge Auslegung bestehender Regeln unverhältnismäßig eingeschränkt werden.

Technologieneutralität muss dabei durch ausreichende Auslegungs- und Ermessensspielräume in der Aufsichtspraxis mit Leben gefüllt werden – orientiert am tatsächlichen Risikoprofil, der Kritikalität und der Einbettung neuer Technologien in die Gesamtarchitektur eines Instituts. **Die regulatorische Praxis darf dabei keinesfalls zur Innovationsbremse werden, sondern muss z.B. über regulatorische Sandboxes Innovationen frühzeitig begleiten. Auch andere Freiräume für die Implementierung von Innovationen sind denkbar wie Pilotprojekte unter erleichterten regulatorischen Rahmenbedingungen und die Anerkennung flexibler interner Governancestrukturen für schnelle Entscheidungen.**

Voraussetzung hierfür ist ein **grundsätzliches Vertrauen in die fachlichen und organisatorischen Kompetenzen der Institute**, neue Technologien verantwortungsvoll, risikoorientiert und regelkonform einzusetzen. Banken verfügen über etablierte Governance-, Kontroll- und Risikomanagementstrukturen sowie über tiefgehende technische Expertise, um technologische Risiken angemessen zu bewerten und zu steuern.

Ein wirksamer Regulierungsrahmen sollte diese Kompetenzen **nutzen und stärken**, statt sie durch übermäßige Detailvorgaben oder formalisierte Nachweispflichten zu ersetzen.
Ziel ist ein Rahmen, der Innovation zulässt, wirtschaftliche Handlungsfähigkeit erhält und zugleich die Steuerbarkeit und Sicherheit der Institute gewährleistet – und damit die **nachhaltige Wettbewerbsfähigkeit des europäischen Bankensektors** stärkt.

Konkret bedeutet dies: Verzicht auf übermäßige Detailvorgaben in delegierten Rechtsakten, stärkere Nutzung risikobasierter Ermessensspielräume in der Aufsichtspraxis sowie eine konsequente Anerkennung etablierter Governance-, Kontroll- und Sicherheitsstrukturen der Institute. Zudem sollten Nachweispflichten stärker auf wesentliche Risiken fokussiert und Mehrfachprüfungen systematisch vermieden werden. Nur so entsteht ein Regulierungsrahmen, der Innovation ermöglicht, wirtschaftliche Handlungsfähigkeit erhält und gleichzeitig Sicherheit und Steuerbarkeit gewährleistet.

Unsere Petita zur Stärkung von Innovation in bestehenden Regelwerken

1. **Risikoorientierte Bewertung von KI-Systemen**
   Lernende, adaptive Systeme sollen primär nach ihrem tatsächlichem Risiko und ihrer Kritikalität bewertet werden. Erklärbarkeits- und Transparenzanforderungen sind von der Aufsicht risikoorientiert zu prüfen.
2. **Fokus auf operative Steuerbarkeit statt auf technische Vollständigkeit**
   Formale Anforderungen sollten nicht pauschal verlangen, jede einzelne technische Komponente jederzeit vollständig substituierbar zu machen. Maßgeblich ist die wirksame operative Steuerbarkeit im jeweiligen Risikokontext. Für kritische oder für BCM relevante Funktionen gelten dabei entsprechend höhere Anforderungen, orientiert am jeweiligen Schutzbedarf und an den Wiederherstellungszielen.
3. **Zeitnahe Umsetzung delegierter Rechtsakte**
   Umsetzungsvorgaben sollen erst nach Finalisierung und Veröffentlichung des jeweiligen Rechtsakts beginnen, um Rechtssicherheit und realistische Planbarkeit zu gewährleisten.
4. **Vermeidung von Innovationsbremse durch Formalismus**
   Regulatorische Prüfungen sollten so ausgestaltet sein, dass sie die Einführung neuer Technologien nicht durch unverhältnismäßige formale Anforderungen erschweren.
5. **Anerkennung von institutsspezifischen Validierungs- und Monitoring-Konzepten**
   Verfügt ein Institut über etablierte und wirksame Verfahren zur Validierung und Überwachung von KI- oder Automatisierungslösungen, sollten diese im Rahmen der Aufsicht anerkannt werden. Maßgeblich sollte sein, ob die bestehenden Konzepte das jeweilige Risikoprofil angemessen abdecken – nicht, ob sie einem generischen Standardformat entsprechen. Redundante oder rein formale Parallelprüfungen ohne zusätzlichen Risikonutzen sollten vermieden werden.
6. **Transparente Abgrenzung von internen Leistungen, Fremdbezug und kritischen Funktionen**
   Anforderungen sollten die praktische Realität modularer und heterogener IT-Architekturen berücksichtigen. Maßgeblich sollte eine nachvollziehbare, konsistente und risikoorientierte Abgrenzung sein, die Institute befähigt, interne Leistungen, Fremdbezug und kritische Funktionen sachgerecht einzuordnen.
7. **Technologieneutrale Formulierung von Delegierten Rechtsakten**
   Regulatorische Anforderungen sollten technologieneutral formuliert sein. Maßgeblich ist das jeweilige Risikoprofil einer Anwendung, nicht die zugrunde liegende Technologie
8. **Fokus auf etablierte Governance-, Kontroll- und Risikomanagementstrukturen**
   Auf übermäßige Detailvorgaben sollte in (delegierten) Rechtsakten verzichtet und vielmehr auf stärkere Nutzung risikobasierter Ermessensspielräume in der Aufsichtspraxis gesetzt werden. Zudem sollten Nachweispflichten stärker auf wesentliche Risiken fokussiert und Mehrfachprüfungen systematisch vermieden werden

3. DORA-Review
Wirksamkeit durch Proportionalität und Praxistauglichkeit

3.1 Anwendbarkeit, Proportionalität und Berichtswesen

Mit dem Digital Operational Resilience Act (DORA) wird ein einheitlicher europäischer Rahmen für das Management von IKT-Risiken geschaffen, der von Banken grundsätzlich unterstützt wird. Der sehr weit gefasste Anwendungsbereich soll eine umfassende Resilienz des Finanzsystems sicherstellen, führt in der praktischen Umsetzung jedoch zu erheblichen Herausforderungen. Zwar ist das Proportionalitätsprinzip explizit im Gesetz verankert, in der konkreten Ausgestaltung der Regulatory Technical Standards (RTS) kommt es bislang nur unzureichend zur Geltung.

Aus Sicht der Banken besteht daher ein d**eutlicher Bedarf an einer stärkeren Differenzierung der DORA-Anforderungen**. Neben der vollständigen Anwendung von DORA und dem vorgesehenen vereinfachten IKT-Risikomanagementrahmen fehlt eine mittlere Ausprägung, die der Realität vieler Institute gerecht wird. Eine solche Differenzierung entlang von Systemrelevanz- oder Kritikalitätsklassen könnte insbesondere bei Dokumentationstiefe, Berichtsumfang, Testfrequenzen und Meldefristen ansetzen und das Proportionalitätsprinzip wirksam operationalisieren.

Ein **geeigneter Anknüpfungspunkt** für diese mittlere Kategorie kann die bereits etablierte aufsichtsrechtliche Risikodifferenzierung im Rahmen des Supervisory Review and Evaluation Process (SREP) sein. Auch für von der BaFin beaufsichtigte Institute wird im SREP heute bereits entlang von Größe, Komplexität, Geschäftsmodell und Risikoprofil differenziert, ohne dass diese Differenzierung formal in feste Kategorien überführt wird. DORA sollte diese Logik aufgreifen und für Institute, die nicht systemrelevant sind, aber aufgrund ihrer Bilanzsumme, operativen Bedeutung oder IKT-Abhängigkeiten einer erhöhten, jedoch nicht systemischen Aufsicht unterliegen, eine mittlere Ausprägung der Anforderungen vorsehen. Dies würde insbesondere größeren, nicht systemrelevanten Instituten – etwa Landesförderbanken oder großen regionalen Banken – **eine proportionale Umsetzung von Dokumentations-, Test- und Berichtspflichten** ermöglichen, ohne die Zielsetzung von DORA zu verwässern.

Für den mittleren Anwendungsbereich könnten reduzierte Anforderungen an Dokumentationstiefe, Prüfzyklen und vertragliche Detailvorgaben gelten. Für wesentliche, aber nicht kritische oder wichtige IKT-Drittleistungen sollten **standardisierte Nachweise** (z. B. anerkannte Zertifizierungen) ausreichen; zusätzliche institutsspezifische Prüfungen sollten **nur bei relevanten Anhaltspunkten** erfolgen, nicht anlasslos. Die Bewertung von Konzentrations- und Abhängigkeitsszenarien sollte sich stärker an der kritischen Bedeutung der Dienstleistung für die unterstützten Prozesse orientieren, statt auf die formale Vollständigkeit aller Lieferketten abzustellen. Aufsichtliche Erwartungen sollten sich am tatsächlichen Risikoprofil orientieren und an die im SREP etablierte Differenzierung nach Größe, Komplexität und Geschäftsmodell anschließen.

Eine **derzeit in Diskussion befindliche Erweiterung des Kleinbanken- oder Proportionalitätsregimes** könnte es ermöglichen, für kleinere oder weniger komplexe Institute vereinfachte Anforderungen anzuwenden. Dadurch ließe sich ein Großteil der mittleren oder nicht

kritischen IKT-Drittleistungen auf standardisierte Nachweise und risikoadäquate Prüfungen reduzieren, ohne dass eine komplexe, fein gestufte Struktur erforderlich ist.

Der **Umfang der geforderten Dokumentationen und Berichte** stellt in der Praxis einen erheblichen Aufwand dar, insbesondere bei stabilen, etablierten Prozessen – z. B. Beschreibung kryptographischer Verfahren, detaillierte Testkonzepte oder prozessuale Sollbeschreibungen. Dieser Aufwand steht häufig in keinem angemessenen Verhältnis zum zusätzlichen Erkenntnisgewinn für die tatsächliche Resilienz. Bereits nach deutschem Recht (MaRisk AT9 Abs. 7 und BT 2.1) müssen Institute ausgelagerte Aktivitäten in ihre Prüfungsplanung einbeziehen; Ersatzprüfungen (z. B. durch Big4) sind zulässig. Vor diesem Hintergrund ist es sachgerecht, Dokumentationstiefe und Prüfumfang für stabile, etablierte Prozesse **risikoorientiert und anlassbezogen** zu gestalten, ohne dass die Resilienz gefährdet wird. Fehlende Dokumentationen würden Betrieb und Störungsbehebung eher von zufälligem Handeln als von planbaren Prozessen abhängig machen.

Ergänzend sollte geprüft werden, inwieweit Dokumentation für weniger kritische oder stabile Anwendungen stärker bedarfsorientiert erstellt beziehungsweise aktualisiert werden kann. Eine teilweise Generierung „auf Abruf“ – etwa im Rahmen von Prüfungen oder konkreten Anlässen – sowie gebündelte, periodische Aktualisierungen (z. B. monatlich oder quartalsweise) könnten dazu beitragen, den laufenden Pflegeaufwand signifikant zu reduzieren, ohne die Nachvollziehbarkeit oder Prüfbarkeit wesentlich einzuschränken.

Insgesamt zeigt sich, dass die RTS sehr detaillierte Anforderungen an Dokumentation und Nachweise enthalten. Dennoch lassen sich die komplexen Abhängigkeiten moderner IKT-Systeme in der Praxis **nicht vollständig erfassen oder konsistent bewerten**. Der entstehende Aufwand entsteht daher weniger durch die Identifikation wesentlicher Risiken, sondern durch kleinteiliges Asset-, Risiko- und Nachweismanagement, das primär formalen Anforderungen dient, ohne die tatsächlichen Abhängigkeiten adäquat abzubilden.

3.2 Drittparteienrisikomanagement

Mit DORA wird das Management von IKT-Drittparteien deutlich ausgeweitet und europaweit harmonisiert. Ziel ist es, Konzentrationsrisiken zu begrenzen, Transparenz zu erhöhen und die digitale operationelle Resilienz des Finanzsystems insgesamt zu stärken. Banken unterstützen diesen Ansatz ausdrücklich. In der praktischen Umsetzung zeigt sich jedoch, dass insbesondere Anforderungen an Vertragsgestaltung, Prüfrechte und laufende Überwachung mit erheblichen operativen und wirtschaftlichen Herausforderungen verbunden sind.

Eine zentrale Herausforderung liegt in der **Ausgestaltung und Durchsetzbarkeit von Prüf- und Zugriffsrechten gegenüber IKT-Drittdienstleistern**. Insbesondere bei marktmächtigen Anbietern stoßen Institute regelmäßig an faktische Grenzen ihrer Verhandlungsmacht. Dies gilt in besonderem Maße für komplexe Lieferketten und Unterauftragsverhältnisse, in denen Transparenz und Einflussmöglichkeiten naturgemäß abnehmen. Die regulatorisch erwartete umfassende Verantwortung auch für Subdienstleister ist in der Praxis nur mit erheblichem Aufwand umsetzbar und steht nicht immer in einem angemessenen Verhältnis zum tatsächlich steuerbaren Risiko. Vor diesem Hintergrund ist die Anpassung der Kommission im Zusammenhang mit dem RTS-Sub, die **Prüfpflicht**

auf Subdienstleister zu beschränken, die kritische oder wesentliche Funktionen unterstützen, ausdrücklich zu begrüßen.

Auch die Anforderungen an eine vollständige, konsolidierte schriftliche Vertragsdokumentation stellen viele Institute vor erhebliche Herausforderungen. Einzelne Vorgaben des Art. 30 DORA erweisen sich in der Umsetzung als besonders anspruchsvoll. So verlangt Art. 30 Abs. 2 lit. i DORA die Vereinbarung von Bedingungen zur Teilnahme von IKT-Drittdienstleistern beziehungsweise deren Mitarbeitenden an **Schulungen** des Instituts, sofern der Dienstleister nicht bereits über ein adäquates Schulungs- und Sensibilisierungskonzept verfügt. Gerade bei internationalen oder standardisierten Anbietern sind solche individuellen Vereinbarungen oftmals nur eingeschränkt durchsetzbar.
Hinzu kommt, dass bislang **keine standardisierten Musterklauseln** oder aufsichtlich abgestimmten Vertragsbausteine zur Verfügung stehen. Dies führt zu einer Vielzahl individueller Vertragslösungen, erhöhtem rechtlichem und organisatorischem Abstimmungsaufwand sowie zu einer fragmentierten Umsetzungspraxis.

In der Praxis ist zudem zu beobachten, dass einzelne Anbieter regulatorische Zusatzanforderungen aus DORA in ihre Preisgestaltung einbeziehen oder gesondert bepreisen. Insbesondere bei marktprägenden oder schwer substituierbaren Services verfügen Institute häufig nur über begrenzte Verhandlungsspielräume. Hier besteht das Risiko, dass regulatorische Anforderungen zu steigenden Kosten führen, ohne dass sich die Resilienz im gleichen Maße erhöht.

Zahlreiche DORA-Anforderungen überschneiden sich inhaltlich mit etablierten Informationssicherheits- und Kontrollstandards. Bestehende Zertifizierungen wie ISO 27001, BSI-Grundschutz oder TISAX sollten daher ausdrücklich als **geeignete Nachweise für bestimmte Teilaspekte der DORA-Konformität** anerkannt werden, etwa hinsichtlich Governance, Kontrollrahmen oder kontinuierlicher Verbesserungsprozesse. Eine solche Anerkennung würde Doppelprüfungen vermeiden, die Vergleichbarkeit erhöhen und die Umsetzung effizienter gestalten.

Gleichzeitig können nicht alle DORA-spezifischen Anforderungen über bestehende Standards abgedeckt werden. Hier bedarf es einer klaren Abgrenzung, um zusätzliche Nachweise gezielt auf genuin DORA-spezifische Aspekte zu konzentrieren. Vor diesem Hintergrund erscheint eine dreistufige Anerkennungs- und Prüfarchitektur für IKT-Drittdienstleister sachgerecht:

1. **Kritische IKT-Drittdienstleister (CTPPs)**
   Für CTPPs sollte ein aufsichtlich abgestimmtes Zulassungs- oder Anerkennungsregime gelten, das über einen formalen Nachweis bestätigt, dass diese Anbieter umfassend geprüft wurden und ihre Leistungen regulatorisch akzeptiert sind. Prüfungsergebnisse sollten den beaufsichtigten Instituten zentral zur Verfügung gestellt werden, um Mehrfachprüfungen und redundante Informationsabfragen zu vermeiden.
2. **Dienstleister kritischer Dienstleistungen**
   Erbringen Dienstleister für ein Institut kritische Dienstleistungen, ohne selbst als CTPP eingestuft zu sein, sollte eine risikoorientierte Überwachung erfolgen. Hier können standardisierte DORA-Nachweise oder anerkannte Zertifizierungen als Grundlage dienen; zusätzliche institutsspezifische Prüfungen sollten nur bei konkreten Anhaltspunkten oder erhöhtem Risikoprofil erforderlich sein.

3. **Nicht-kritische beziehungsweise standardisierte Dienstleistungen**
   Für nicht-kritische, standardisierte Leistungen – etwa Office-Software oder marktübliche Cloud-Tools – sollten deutlich vereinfachte vertragliche Anforderungen und reduzierte Dokumentationspflichten gelten. Der Umfang der Nachweise sollte dem tatsächlichen Risikogehalt entsprechen.

Audits könnten dabei über zertifizierte, unabhängige Drittaudits mit regelmäßig wechselnden Prüfern in mehrjährigen Intervallen erfolgen. Prüfmethodik und -inhalte sollten in enger Abstimmung zwischen Aufsicht und Finanzwirtschaft entwickelt werden. Für marktmächtige Anbieter wäre perspektivisch auch eine stärkere Rolle zentraler oder staatlich koordinierter Prüfmechanismen denkbar, um eine effiziente und einheitliche Aufsicht sicherzustellen.

Hinsichtlich des **zentralen Informationsregisters** besteht grundsätzlich Verständnis für dessen Zielsetzung. Gleichwohl zeigt sich, dass der derzeit vorgesehene Detaillierungsgrad nicht in allen Bereichen einen proportionalen Mehrwert für die Risikosteuerung bietet. Eine stärkere Fokussierung auf tatsächlich risikorelevante Informationen würde die Datenqualität erhöhen und gleichzeitig administrativen Aufwand reduzieren. Verträge zu nicht-kritischen oder lediglich unterstützenden Funktionen sollten daher zumindest in vereinfachter Form dokumentiert werden können.

Vor dem Hintergrund einer möglichen perspektivischen Erweiterung des Registers auf IKT- und Nicht-IKT-Funktionen ist zudem wichtig, den unterschiedlichen internen Organisations- und Steuerungsmodellen der Institute Rechnung zu tragen. Ob ein Register vertragsbasiert, funktionsbasiert oder hybrid geführt wird, sollte institutsspezifisch ausgestaltet werden können. Entscheidend ist nicht die gewählte Struktur, sondern eine einheitliche Konzeption, eine konsistente Systematik und eine klare, einheitliche Begriffsverwendung.

3.3 Meldewesen

Mit DORA wird das Meldewesen für IKT-bezogene Vorfälle europaweit harmonisiert und deutlich ausgeweitet. Ziel ist es, schwerwiegende Vorfälle frühzeitig transparent zu machen und den Informationsaustausch zwischen Aufsicht und Marktteilnehmern zu verbessern. Dieses Ziel wird von Banken ausdrücklich unterstützt. In der praktischen Umsetzung zeigt sich jedoch, dass Ausgestaltung und Anwendung der Meldepflichten in ihrer derzeitigen Form operative Herausforderungen mit sich bringen und der angestrebte Mehrwert nicht in allen Fällen voll ausgeschöpft wird.

Die vorgesehenen **Schwellenwerte** für meldepflichtige Vorfälle erscheinen aus Sicht der Institute teilweise niedrig angesetzt; zudem sind einzelne Meldekriterien in der praktischen Anwendung auslegungsbedürftig.
Eine zentrale Rolle im DORA-Meldewesen spielt die Datenverfügbarkeit. Sie ist sowohl Bestandteil des Kriteriums „Datenverluste“ als auch mittelbar relevant für die Dauer von Serviceunterbrechungen und die Kritikalität betroffener Funktionen. In der Praxis führt dies dazu, dass bereits in frühen Phasen eines Vorfalls mehrere Meldekriterien parallel ausgelöst werden können, obwohl es sich häufig um interne, operativ beherrschbare Störungen ohne externe Wirkung handelt. Die fehlende klare Trennung zwischen technischer Beeinträchtigung und aufsichtsrelevanter Auswirkung begünstigt vorsorgliche

Meldungen und erhöht den Ressourcenaufwand, ohne dass der Informationsgewinn für die Aufsicht stets im gleichen Maße steigt.

Auch das Kriterium der **Kundenbetroffenheit** erweist sich als anspruchsvoll. Zu Beginn eines Vorfalls ist regelmäßig nicht belastbar abschätzbar, wie viele Kunden tatsächlich betroffen sein werden oder welche Auswirkungen sich auf Reputation und Marktverhalten ergeben. Reputationsschäden lassen sich innerhalb der vorgesehenen Fristen nur selten valide feststellen, sofern ein Cyberangriff nicht öffentlich bekannt wird. In der Folge wird das Kriterium häufig vorsorglich als erfüllt bewertet, sodass ein Vorfall – insbesondere in Kombination mit einem potenziellen Datenverlust – frühzeitig als schwerwiegend eingestuft wird, auch wenn sich diese Einschätzung später relativiert.

Zudem bilden die bestehenden Kriterien nicht sämtliche relevanten Auswirkungen differenziert ab. Auch **interne Effekte** auf kritische Prozesse, Steuerungsfunktionen oder das Institut insgesamt können erheblich sein, ohne sich unmittelbar in Kunden- oder Volumenzahlen niederzuschlagen.

Vor diesem Hintergrund erscheint eine **stärkere Differenzierung nach Art und risikobezogener Relevanz eines IKT-bezogenen** Vorfalls sachgerecht. Maßgeblich sollte nicht allein die unmittelbare Auswirkung sein, sondern auch, ob eine (absehbare) Überschreitung der institutsspezifisch definierten Wiederanlaufziele (RTO/RPO) droht. Interne Störungen, die innerhalb dieser Ziele behoben werden können und keine sicherheitsrelevante Ursache aufweisen, stellen typischerweise kein erhöhtes Resilienzrisiko dar. Eine stärker an diesen Parametern ausgerichtete Einordnung würde die institutsspezifische Risikolage und den Risikoappetit angemessen berücksichtigen. Eine ausschließlich auswirkungsbezogene Betrachtung greift demgegenüber zu kurz und kann zu einem unverhältnismäßigen Meldeaufwand führen, ohne zusätzlichen Erkenntnisgewinn zu generieren.
In der operativen Umsetzung zeigt sich zudem, dass insbesondere in der Anfangsphase eines Vorfalls häufig nicht eindeutig beurteilt werden kann, ob Meldekriterien erreicht werden. Dies führt zu erhöhtem Koordinations-, Schulungs- und Abstimmungsaufwand und begünstigt eine vorsorgliche Meldepraxis.

Herausfordernd ist zudem die **uneingeschränkte Wochenend- und Feiertagsmeldepflicht**. Anders als in früheren Regelwerken bestehen hier keine Erleichterungen. In der Praxis ist es an Wochenenden regelmäßig schwierig, alle für eine qualifizierte Meldung erforderlichen Informationen kurzfristig zusammenzuführen, da spezialisierte Fachpersonen nicht in voller Breite verfügbar sind. Dies kann zu Meldungen unter erheblichem Zeitdruck führen, während gleichzeitig Ressourcen von der eigentlichen Störungsbehebung gebunden werden. Eine differenzierte, praxisgerechte Ausgestaltung der Fristen – etwa unter stärkerer Harmonisierung mit bestehenden Fristenregimen – könnte hier zur Qualitätssicherung beitragen.

Zusätzliche Belastungen ergeben sich aus der **konkreten Ausgestaltung der Meldeprozesse und -formulare**. Die wiederholte Erfassung identischer Informationen bei Erst-, Zwischen- und Abschlussmeldungen, fehlende Vorbelegungen von Stammdaten sowie technische Hürden führen zu erhöhtem administrativem Aufwand. Dieser steht nicht immer in einem angemessenen Verhältnis zum erzielten Erkenntnisgewinn.

Positiv hervorzuheben ist hingegen, dass DORA als lex specialis perspektivisch zu einer Konsolidierung der Meldungen in einem zentralen Meldehub beitragen kann. Deutschland ist mit der gebündelten Meldung an die BaFin hierfür ein Beispiel. Der im Digitalen Omnibus vorgesehene **Single Entry Point** kann – insbesondere für Industrien, die eine solche Zentralisierung bislang nicht kennen – die Chance bieten, Meldepflichten zu bündeln, Mehrfachmeldungen zu vermeiden und konsistente Ergebnisse in Dringlichkeitsfällen zu ermöglichen.
Aus Sicht der Institute sollte ein solcher Single Entry Point jedoch frühzeitig die praktischen Erfahrungen aus der DORA-Umsetzung berücksichtigen. Die Anzahl der Meldungen ist bislang nicht signifikant gestiegen; vielfach werden bestehende Meldungen nun über DORA kanalisiert. Der **Aufwand pro Meldung** hat sich jedoch spürbar erhöht – insbesondere durch die komplexe Vorfilterung und die detaillierten Formanforderungen – ohne dass stets ein entsprechender Mehrwert entsteht.

Voraussetzung für einen wirkungsvollen Single Entry Point wäre daher, ihn konsequent als Instrument zur **Harmonisierung und Vereinfachung bestehender Anforderungen** auszugestalten. Ein echter Mehrwert entsteht nur, wenn Meldekonzepte, Vorfallkategorien, Schweregrade und Schwellenwerte inhaltlich konsistent aufeinander abgestimmt werden. Der Single Entry Point sollte nicht lediglich eine technische Aggregationsplattform darstellen, sondern mit einer **Reduktion redundanter Meldefelder**, klaren Kriterien und vereinfachten Prozessen einhergehen – insbesondere mit Blick auf mögliche künftige Melderegime etwa aus dem KI-Akt oder dem Cyber Resilience Act.

3.4 Implikationen und Erwartungen aus Sicht der Banken

DORA schafft einen einheitlichen europäischen Rahmen für das Management von IKT-Risiken und wird von Banken grundsätzlich begrüßt. Die Umsetzung zeigt jedoch, dass der sehr detaillierte Anwendungsbereich und die umfangreichen Meldepflichten in der Praxis zu erheblichem Aufwand führen – insbesondere bei Dokumentation, Drittparteienmanagement und Meldewesen. Proportionalität wird bislang nur unzureichend operationalisiert, weshalb mittelgroße Institute von den Anforderungen besonders stark betroffen sind.

Die anstehende **DORA-Review** sollte daher sicherstellen, dass Anforderungen praxisnah, proportional und handhabbar gestaltet werden. Zentrale Aspekte sind:

- Einführung einer mittleren Kategorie für Institute, die nicht systemrelevant, aber groß und komplex sind, um DORA-Anforderungen in reduziertem, proportionalem Umfang umzusetzen.
- Anerkennung bestehender Informationssicherheitsstandards als Nachweis für Teile der DORA-Konformität, um Doppelprüfungen zu vermeiden.
- Anpassung der Meldeprozesse, Schwellenwerte und Kriterien, insbesondere: Differenzierung nach Ursache, Vermeidung unnötiger Wochenendmeldungen und Nutzung des Single Entry Points als wirksames Entschlackungsinstrument.

Die DORA-Review sollte außerdem den **gesamten regulatorischen Kontext** berücksichtigen: Harmonisierung, Kohärenz und Entlastung der Banken sind entscheidend, um Innovation, Wettbewerbsfähigkeit und digitale Resilienz in einem geopolitisch sensiblen Umfeld zu stärken. Nur so können Banken ihre Handlungsfähigkeit wahren, Risiken effektiv steuern und technologische Chancen nutzen.

Unsere Petita zu einer praxisnahen DORA-Anwendung

1. **Einführung einer mittleren Anforderungskategorie**
   Institute, die nicht systemrelevant, aber groß und komplex sind, sollen DORA-Anforderungen in reduziertem, proportionalem Umfang erfüllen können (Dokumentation, Testfrequenz, Berichtspflichten).
2. **Anerkennung bestehender Informationssicherheitsstandards für die mittlere Anforderungskategorie**
   ISO 27001, BSI-Grundschutz oder TISAX sollen als Nachweis für Teile der DORA-Konformität gelten, um Doppelprüfungen zu vermeiden.
3. **Differenzierte risikoorientierte Dokumentationsanforderungen:** Reduktion der Detailtiefe für stabile, etablierte Prozesse; Fokus auf risikorelevante Informationen, nicht auf Vollständigkeit jeder Lieferkette.
4. **Zentraler Single Entry Point**
   Nutzung als Instrument zur Entschlackung, Harmonisierung und Vereinheitlichung von Meldungen; redundante Felder reduzieren, klare Kriterien definieren.
5. **Differenzierung bei Vorfallmeldungen**
   Klare ex-ante Abgrenzung zwischen internen Betriebsstörungen und externen Sicherheitsvorfällen; höhere Schwellenwerte beziehungsweise explizite Ausnahme für interne Störungen, die innerhalb der definierten RTO/RPO behoben werden können.
6. **Flexible Wochenend- und Feiertagsmeldungen:** Meldepflichten sollen an das Risikoprofil des Instituts angepasst und mit anderen Meldefristen (z. B. GDPR) harmonisiert werden.
7. **Keine pauschalen Prüf- und Auditpflichten gerade bei marktmächtigen Anbietern**
   Keine pauschalen oder anlasslosen Prüf- und Auditpflichten, sofern standardisierte, anerkannte Nachweise vorliegen und keine konkreten Risikohinweise bestehen.
8. **Standardisierte Vertragsbausteine für Drittdienstleister**
   Bereitstellung von aufsichtlich abgestimmten Mustern zur Reduktion von Rechts- und Abstimmungsaufwand.
9. **Keine Mandatsüberschreitung der 2nd Level-Rechtsakte – Leben der Proportionalität**
   Proportionale Vorgaben für Dokumentationstiefe, Testzyklen und Berichtspflichten abhängig von Größe, Komplexität, Kritikalität und SREP-Differenzierung der Institute konkret leben.
10. **dreistufige Anerkennungs- und Prüfarchitektur für IKT-Drittdienstleister**
    Kritische IKT-Drittdienstleister (CTPPs): formalen Nachweis zur Bestätigung, dass diese Anbieter umfassend geprüft wurden und ihre Leistungen regulatorisch akzeptiert sind.
    Dienstleister kritischer Dienstleistungen: standardisierte DORA-Nachweise oder anerkannte Zertifizierungen als Grundlage; zusätzliche institutsspezifische Prüfungen nur bei konkreten Anhaltspunkten oder erhöhtem Risikoprofil
    Nicht-kritische beziehungsweise standardisierte Dienstleistungen: deutlich vereinfachte vertragliche Anforderungen und reduzierte Dokumentationspflichten; der Umfang der Nachweise sollte dem tatsächlichen Risikogehalt entsprechen

4. Regulatorische Kohärenz und Entlastung

Ausblick

Die Vielzahl neuer und bestehender IT-bezogener Regulierungen – von DORA über CRA bis hin zu NIS2 und sektoralen Vorgaben – führt in der Praxis zu komplexen, teils redundanten Anforderungen für Banken. Eine konsequente Überprüfung aller einschlägigen Primär- und Sekundärrechtsakte auf Notwendigkeit, Praxistauglichkeit und aufsichtsrelevante Wirkung ist daher dringend geboten. Parallelregelungen sollten identifiziert, nicht notwendige Elemente gestrichen und verbleibende Anforderungen klar an einer Aufwand-Nutzen-Betrachtung ausgerichtet werden – idealerweise in einem gebündelten Omnibus-Ansatz.

Besondere Beachtung verdient die Differenzierung nach Systemrelevanz: Systemisch wichtige Institute unterliegen umfassenden Anforderungen, während nicht systemrelevante Häuser spürbare Entlastungen erfahren sollten. Dies stärkt die proportionale Umsetzung und reduziert den operativen Aufwand, ohne die Sicherheit des Finanzsystems zu beeinträchtigen.

Regulatorische Kohärenz ist zudem eng mit Innovationsfähigkeit und geopolitischen Herausforderungen verknüpft. Banken müssen neue Technologien – etwa KI, Cloud-Lösungen oder digitale Plattformen – einführen können, ohne dass unnötige regulatorische Komplexität Innovationszyklen blockiert. Gleichzeitig müssen sie Abhängigkeiten von internationalen Technologieanbietern managen und strategische Entscheidungen souverän treffen.
Eine effiziente, kohärente und proportionale Regulierung ist somit ein entscheidender Hebel, um digitale Resilienz, Innovationsfähigkeit und Wettbewerbsfähigkeit zu stärken. Sie ermöglicht Banken, technologische Chancen zu nutzen, operative Risiken wirksam zu steuern und unnötigen Aufwand zu vermeiden.

Gesamtfazit

Banken können nur dann erfolgreich, widerstandsfähig und innovationsfähig agieren, wenn digitale Souveränität, technologische Innovation, DORA-konformes IKT-Risikomanagement und regulatorische Kohärenz miteinander verzahnt werden. Eine isolierte Betrachtung einzelner Regelwerke greift zu kurz: Nur ein integrierter Ansatz, der Selbstverantwortung, Praxistauglichkeit und proportionalen Aufwand verbindet, schafft ein Fundament für resiliente, wettbewerbsfähige Finanzinstitute.

Die wesentlichen Handlungsfelder lassen sich zusammenfassend wie folgt darstellen:

- **Digitale Souveränität:** Entscheidungshoheit über Daten, Infrastruktur und Anwendungen, einschließlich globaler Anbieter, ist zentral für Flexibilität und Innovationsfähigkeit. Sie wird von den Banken **innerhalb ihres bestehenden Risikorahmens und Governance-Systems** umgesetzt, sodass neue Technologien wie hybride Multi-Cloud-Architekturen oder KI-Lösungen im bestehenden regulatorischen Rahmen sicher genutzt werden können.
- **Praxisnahe Regulierung neuer Technologien:** Technologieneutrale Regelwerke müssen flexibel, risikoorientiert und proportioniert interpretiert werden, um modulare, hybride und API-gestützte IT-Landschaften angemessen steuern zu können. Starre, formalistische Vorgaben blockieren Innovation und erhöhen operative Risiken.

- **DORA-Umsetzung:** Der einheitliche europäische Rahmen für IKT-Risiken wird von Banken unterstützt, muss aber praxisnah operationalisiert werden. Wesentliche Elemente sind die Einführung einer mittleren Anforderungskategorie, die Anerkennung etablierter Sicherheitsstandards, proportional ausgestaltete Dokumentations- und Meldepflichten sowie die effiziente Nutzung des Single Entry Points.
- **Drittparteienmanagement:** Risikoorientierte Prüfungen kritischer und wesentlicher Dienstleistungen, standardisierte Vertragsbausteine und die Vermeidung anlassloser Auditpflichten sind zentral, um den Aufwand zu reduzieren, die Steuerbarkeit zu erhöhen und gleichzeitig die Resilienz in komplexen Lieferketten sicherzustellen.
- **Meldewesen:** Differenzierte Schwellenwerte, klare Unterscheidung zwischen internen Betriebsstörungen und externen Sicherheitsvorfällen sowie praxisgerechte Fristen, insbesondere an Wochenenden und Feiertagen, sichern eine effiziente, risikoorientierte Meldung ohne unnötigen administrativen Aufwand.
- **Regulatorische Kohärenz und Entlastung:** Harmonisierung und Abbau redundanter Vorschriften sind entscheidend, um operative Belastungen zu verringern, Innovation zu ermöglichen und die digitale Resilienz zu stärken. Die Differenzierung nach Systemrelevanz gewährleistet proportionalen Aufwand und gezielte Entlastung nicht systemrelevanter Institute.
- **Europäische Simplifizierung und Harmonisierung:** Die aktuellen Bestrebungen der EU, regulatorische Anforderungen zu überprüfen, zu harmonisieren und zu vereinfachen – etwa im Rahmen des Digitalen Fitness Checks – bieten eine Chance, bestehende Doppelprüfungen, inkonsistente Vorgaben und überflüssige Komplexität zu reduzieren. Diese Prinzipien der Entlastung, Harmonisierung und praxisgerechten Operationalisierung lassen sich auf DORA und verwandte Vorschriften übertragen. Bankenseitig bedeutet dies, dass etablierte Standards, risikobasierte Prüfungen und proportional ausgestaltete Meldeprozesse konsequent genutzt werden können, um administrativen Aufwand zu reduzieren und gleichzeitig die regulatorische Zielsetzung zu erfüllen.

In der Summe zeigt sich: Nur durch die konsequente Verzahnung von **digitaler Souveränität, technologischer Innovationsfähigkeit, praxisnaher DORA-Anwendung und regulatorischer Kohärenz**, ergänzt um die Chancen europäischer Harmonisierung und Entlastung, können Banken Risiken wirksam steuern, Chancen neuer Technologien nutzen und gleichzeitig ihre operative Resilienz sichern. Dieses Gesamtverständnis bildet die Grundlage für ein zukunftsfähiges, resilientes und wettbewerbsstarkes europäisches Finanzsystem – gerade auch angesichts geopolitischer Unsicherheiten.

Der Bundesverband Öffentlicher Banken Deutschlands, VÖB, ist ein Spitzenverband der deutschen Kreditwirtschaft. Er vertritt die Interessen von 64 Mitgliedern, darunter die Landesbanken sowie die Förderbanken des Bundes und der Länder. Die Mitgliedsinstitute des VÖB haben eine Bilanzsumme von rund 3.200 Milliarden Euro und bilden damit etwa ein Viertel des deutschen Bankenmarktes ab. Die öffentlichen Banken nehmen ihre Verantwortung für Mittelstand, Unternehmen, die öffentliche Hand und Privatkunden wahr und sind in allen Teilen Deutschlands fest in ihren Heimatregionen verwurzelt. Mit 57 Prozent sind die ordentlichen VÖB-Mitgliedsbanken Marktführer bei der Kommunalfinanzierung und stellen zudem rund 22 Prozent aller Unternehmenskredite in Deutschland zur Verfügung. Die Förderbanken im VÖB haben im Jahr 2024 Förderdarlehen in Höhe von knapp 60 Milliarden Euro bereitgestellt. Als einziger kreditwirtschaftlicher Verband übt der VÖB die Funktion eines Arbeitgeberverbandes für seine Mitgliedsinstitute aus. Die tarifrechtlichen Aufgaben, insbesondere der Abschluss von Tarifverträgen, werden von der Tarifgemeinschaft Öffentlicher Banken wahrgenommen. Ihr gehören rund 65.000 Beschäftigte der VÖB-Mitgliedsinstitute an. Weitere Informationen unter www.voeb.de