Prof. Dr. Andreas Igl
TH Deggendorf

200 Tage DORA – Ausblick auf Forschung und Umsetzungsperspektiven

Deggendorfer Notiz 2025/07 | 5. August 2025

KI-generiertes Bild

Mit dem Erreichen der Marke von zweihundert Tagen seit Inkrafttreten der Digital Operational Resilience Act (DORA) am 17. Januar 2025 rückt nicht die retrospektive Analyse, sondern vielmehr die zukunftsgerichtete Betrachtung in den Mittelpunkt. Die bisherigen regulatorischen Entwicklungen haben den Grundstein für ein harmonisiertes Rahmenwerk zur IKT-Risikosteuerung im europäischen Finanzsektor gelegt. Aus wissenschaftlicher und regulatorischer Sicht eröffnet sich nun ein breites Spektrum an Fragen, die über die unmittelbare Implementierung hinausgehen und in Forschung wie Praxis gleichermaßen hohe Relevanz besitzen.

Während DORA in erster Linie auf die Schaffung verbindlicher Anforderungen abzielt, bietet es in der wissenschaftlichen Auseinandersetzung die Gelegenheit, grundlegende

Zusammenhänge zwischen Regulierung, Technologie und organisatorischer Umsetzung vertieft zu untersuchen. Offene strategische Fragestellungen reichen von der Effizienz regulatorischer Instrumente bis hin zu den längerfristigen Implikationen für Innovationsprozesse im Finanzsektor. Hieraus ergeben sich Forschungsfelder, die eine kontinuierliche Begleitung sowohl in der Analyse als auch in der methodischen Weiterentwicklung erfordern.

1. Erweiterung quantitativer Modelle zur IKT-Risikomessung

Eine der grundlegenden Herausforderungen im Rahmen von DORA bleibt die präzisere Quantifizierung von IKT-Risiken. Bisher dominieren qualitative Bewertungsansätze, deren Aussagekraft in der operativen Risikoplanung limitiert ist. Die Entwicklung standardisierter, belastbarer quantitativer Verfahren könnte nicht nur die Steuerung von Risiken verbessern, sondern auch deren Integration in Kapitaladäquanz- und Liquiditätsplanungen ermöglichen. Besonders aussichtsreich erscheint die Modellierung von Verlustverteilungen, szenariobasierten Stressauswirkungen und systemischen Abhängigkeiten. Hierbei könnten Ansätze wie der „Return on Security Investment“ (RoSI) als Entscheidungskriterium dienen, um die Balance zwischen Sicherheitsinvestitionen und Resilienznutzen fundierter zu gestalten.

2. Informationssysteme zur Steuerung von IKT-Risiken

Die regulatorischen Vorgaben verlangen von Finanzinstituten, umfassende Informationssysteme zur Erfassung und Überwachung von IKT-Inventar, Sicherheitsvorfällen, Schwachstellen und Drittanbieterabhängigkeiten zu etablieren. Aus Forschungssicht besteht ein erheblicher Bedarf, die konzeptionelle Gestaltung, Governance-Mechanismen und operative Wirksamkeit solcher Systeme zu untersuchen. Fragen der Datenintegration, Standardisierung und Interoperabilität sind dabei ebenso zentral wie die langfristige Nutzbarkeit als Basis für fortgeschrittene Risikoanalysen. Die wissenschaftliche Auseinandersetzung kann hier eine Brücke zwischen Theorien der Informationssysteme und der praktischen Resilienzsteuerung schlagen.

3. Effiziente Prüfmechanismen für kritische IKT-Drittanbieter

Die zunehmende Bedeutung externer, oftmals global agierender Technologieanbieter stellt insbesondere kleinere Kreditinstitute vor besondere Herausforderungen. Die Umsetzung tiefgehender Prüfungen großer, nicht in der EU ansässiger Dienstleister ist sowohl kosten- als auch ressourcenintensiv. Vor diesem Hintergrund eröffnen sich Forschungsfragen, die alternative Prüfmechanismen wie standardisierte Zertifizierungssysteme, gemeinschaftlich genutzte Auditplattformen oder abgestufte Aufsichtsmodelle beleuchten. Vergleichende Analysen unterschiedlicher Jurisdiktionen – etwa zwischen EU, Vereinigtem Königreich und USA – könnten praktikable Ansätze zur Effizienzsteigerung bei gleichzeitiger Einhaltung der regulatorischen Anforderungen identifizieren.

4. Szenariobasierte Stresstests für digitale Resilienz

Die verpflichtenden Resilienztests im Rahmen von DORA bedürfen einer methodischen Weiterentwicklung, um die dynamische und systemische Natur von IKT-Risiken adäquat abzubilden. Klassische Penetrationstests oder Notfallübungen erfassen oftmals nur Teilaspekte möglicher Bedrohungslagen. Zukünftige Forschungsarbeiten könnten Szenario-Frameworks entwickeln, die komplexe, mehrstufige Störungen simulieren – gegebenenfalls unter Nutzung Künstlicher Intelligenz, um adaptive Angriffsmuster oder Störfälle zu generieren. Diese Tests sollten nicht nur technische Wiederherstellungsprozesse, sondern auch organisatorische, juristische und kommunikative Reaktionen umfassen.

5. Kompetenzentwicklung an der Schnittstelle von Sicherheit, Data Literacy und KI

DORA macht deutlich, dass operative Resilienz nicht allein ein technisches, sondern in hohem Maße ein menschliches und organisatorisches Thema ist. Die Anforderungen an Fachkräfte im Bereich der IKT-Risiken verändern sich rasant, insbesondere durch den wachsenden Einfluss von Künstlicher Intelligenz auf Finanzsysteme. Forschungsarbeiten können sich der Frage widmen, wie Bildungs- und Trainingskonzepte gestaltet sein müssen, um Fähigkeiten in Cybersicherheit, Datenanalyse und KI-Kompetenz zu kombinieren. Im Fokus stehen hierbei institutionelle Strategien zur Schaffung multidisziplinärer Resilienzteams und regulatorische Impulse zur gezielten Kompetenzförderung.

6. Innovation und Compliance im digitalen Wandel ausbalancieren

Ein besonders sensibles Forschungsfeld betrifft das Spannungsfeld zwischen regulatorischer Compliance und Innovationsfähigkeit. Während DORA einerseits die operative Resilienz stärken soll, können die umfangreichen Anforderungen zugleich Einfluss auf Geschwindigkeit und Art digitaler Transformationsprozesse nehmen. Relevant wird dies insbesondere bei modularisierten Wertschöpfungsketten, plattformbasierten Geschäftsmodellen und dem Aufkommen von FinTech- und RegTech-Lösungen. Zentrale Forschungsfragen betreffen die regulatorische Balance: Schafft DORA ein innovationsförderndes Umfeld oder hemmt der regulatorische Aufwand die Anpassungs- und Experimentierfreude? Vergleichende Untersuchungen mit anderen Rechtsräumen könnten hier wertvolle Erkenntnisse liefern.

Diese sechs Bereiche sind nicht isoliert, sondern bilden eine vernetzte Forschungsagenda, die die multidimensionale Natur der operativen Resilienz widerspiegelt. Quantifizierungsmodelle hängen von hochwertigen Daten und Informationssystemen ab. Die Überwachung von Drittanbietern kreuzt sich mit Innovationsdynamiken, da die Abhängigkeit von externen Plattformen digitale Transformation sowohl ermöglicht als auch einschränkt. Szenariobasierte Stresstests erfordern Kompetenzen in Sicherheit, Daten und

KI, um effektiv gestaltet und interpretiert zu werden. Über einzelne Projekte hinaus besteht Raum für die Entwicklung integrierter Rahmenwerke, etwa eines Resilienz-Reifegradmodells, das quantitative Risikometriken, Technologie-Governance-Strukturen, Testregime und Humankapitaldimensionen einbezieht. Solche Modelle könnten als analytische Werkzeuge für akademische Forschungen und als praktische Instrumente für Regulatoren und Industrie dienen.

Obwohl DORA eine EU-Verordnung ist, reichen ihre konzeptionellen und praktischen Implikationen global. Finanzinstitute außerhalb der EU, insbesondere solche mit grenzüberschreitenden Dienstleistungen oder EU-Tochtern, unterliegen ebenfalls ihren Bestimmungen. Zudem ist das globale Finanzökosystem zunehmend vernetzt, sodass Resilienzfehler in einer Jurisdiktion international propagieren können. Forschungen, die von der Umsetzung von DORA inspiriert sind, könnten Relevanz für andere regulatorische Rahmen haben, wie die britische Politik zur operativen Resilienz, die US-Interagency Guidance on Third-Party Risk Management oder die Prinzipien des Basel Committees für operative Resilienz. In diesem Kontext bietet sich die Gelegenheit für grenzüberschreitende Forschungen, die untersuchen, wie verschiedene regulatorische Umfelder ähnliche Resilienzherausforderungen angehen. Solche vergleichenden Studien könnten internationale Standardsetzung informieren, Konvergenz in Resilienzpraktiken fördern, das Risiko regulatorischer Arbitrage reduzieren und die globale Finanzstabilität unterstützen.

Das Inkrafttreten von DORA markiert einen Wendepunkt in der Governance von IKT-Risiken im Finanzsektor. Während sein unmittelbares Ziel die regulatorische Compliance ist, liegt seine breitere Bedeutung darin, wie Institutionen digitale Resilienz verstehen, managen und investieren. Für Forscher bietet DORA ein reiches (empirisches) Setting, um das Zusammenspiel zwischen Regulation, Technologie und organisatorischem Verhalten zu untersuchen. Die skizzierten sechs Forschungsgebiete stellen einen Ausgangspunkt für eine umfassende wissenschaftliche Agenda dar, die sowohl zum akademischen Wissen als auch zu praktischen Verbesserungen der Resilienz beiträgt. Durch gezielte Arbeiten in diesen Bereichen kann DORA zu einer resilienteren, innovativen und global harmonisierten Finanzlandschaft führen.

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