FIRM
Frankfurter Institut für
Risikomanagement und Regulierung

Resilienz trotz Cyber- und Drittparteienrisiken

Autoren

Dr. Henning Dankenbring
Dina Friedrichs
Elvira Niedermeier

Die fortschreitende Digitalisierung des Finanzsektors hat die Abhängigkeit von Informations- und Kommunikationstechnologien (IKT) sowie von spezialisierten IKT-Drittanbietern erheblich verstärkt. Gleichzeitig nehmen Cyberangriffe, operationelle Störungen und Konzentrationsrisiken zu. Die digitale operationelle Resilienz ist damit zu einem zentralen Stabilitätsfaktor für Institute und den europäischen Finanzmarkt geworden. Mit dem Digital Operational Resilience Act (DORA) wurde erstmals ein einheitlicher europäischer Rahmen zur Steuerung von IKT-, Cyber- und IKT-Drittparteienrisiken geschaffen. Parallel dazu verschärft die europäische Bankenaufsicht ihre Erwartungen an Governance, Risikosteuerung und Wirksamkeit interner Kontrollen. Digitale Resilienz wird nicht länger als rein technisches Thema betrachtet, sondern als integraler Bestandteil der Gesamtbanksteuerung. Der IT Risk Questionnaire (ITRQ) der Europäischen Zentralbank (EZB) fungiert dabei als Frühwarninstrument und Ausgangspunkt für gezielte aufsichtliche Prüfungen.

DORA und die neuen aufsichtsrechtlichen Erwartungen

Seit Januar 2025 gilt DORA verbindlich für Finanzunternehmen. Die Verordnung schafft einen einheitlichen Rahmen zur Stärkung der digitalen operationellen Resilienz und konkretisiert die Anforderungen an die Governance, das IKT-Risikomanagement, das Management von IKT-Drittparteien sowie an Resilienztests und das Management von IKT-bezogenen Vorfällen.

Die Regelungen stehen im Einklang mit den Aufsichtsprioritäten der EZB für 2026 bis 2028, die den Aufbau robuster und belastbarer Rahmenwerke für das operationelle Risikomanagement als priorisierte Schwachstelle adressieren. Im Fokus stehen insbesondere Cyberrisiken und IKT-Drittparteienrisiken, einschließlich der Steuerung von Konzentrations- und Abhängigkeitsrisiken. Die im Rahmen von DORA eingeführte direkte Beaufsichtigung kritischer IKT-Drittanbieter auf EU-Ebene stärkt zwar die Kontrolle systemischer Risiken, entbindet Institute jedoch nicht von ihrer Verantwortung für ausgelagerte Aktivitäten. Maßgeblich ist daher nicht das Vorhandensein von Konzepten, sondern der Nachweis wirksamer Governance, klarer Zuständigkeiten und einer belastbaren Risikosteuerung im operativen Betrieb.

IT Risk Questionnaire der EZB als Aufsichtsinstrument

Der IT Risk Questionnaire (ITRQ) ist ein jährliches, standardisiertes Erhebungsinstrument der EZB im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozess oder kurz SREP (Supervisory Review and Evaluation Process). Er dient der einheitlichen Beurteilung von IKT-Risiken sowie der Wirksamkeit zugehöriger Governance-, Steuerungs- und Kontrollmechanismen signifikanter Institute und bildet eine Grundlage für aufsichtliche Maßnahmen. Aktuelle SREP-Ergebnisse zeigen, dass insbesondere das Management operationeller IKT-Risiken weiterhin herausfordernd ist und durch DORA zusätzliche Komplexität gewinnt.

Gespräche mit europäischen Banken zeigen, dass sie den Reifegrad ihres IKT-Risikomanagements insbesondere in denjenigen Bereichen als gering einschätzen, in denen DORA die Erwartungen erhöht hat. Dies betrifft vor allem das Management von IKT-Drittparteien sowie das IKT-Geschäftsfortführungsmanagement. Trotz eines hohen Anteils an IKT- und Cloud-Auslagerungen sehen Banken insbesondere bei der laufenden Überwachung sowie beim Ausstieg aus vertraglichen Vereinbarungen mit IKT-Dienstleistern erheblichen Verbesserungsbedarf. Auch der Einbezug von Dienstleistern in die Planung und Durchführung von IKT-Geschäftsfortführungstests wird als wesentliche Schwachstelle wahrgenommen. Darüber hinaus können unvollständige Inventare von Prozessen, IKT-Assets und IKT-Dienstleistern und ein Ungleichgewicht bei der Ressourcenverteilung zwischen den drei Verteidigungslinien die wirksame Steuerung von Resilienz- und Konzentrationsrisiken beeinträchtigen. Insgesamt zeigen die Ergebnisse, dass der ITRQ im Kontext von DORA gezielt als Instrument zur Überprüfung der Weiterentwicklung digitaler operativer Resilienz eingesetzt wird.

Erste Erkenntnisse aus DORA-Prüfungen

DORA-Prüfungen begannen zunächst mit Themenschwerpunkten bei kleineren und mittleren Instituten durch nationale Aufsichtsbehörden und wurden Mitte 2025 auf größere sowie direkt von der EZB beaufsichtigte Banken ausgeweitet. DORA verlagert den Prüfungsfokus dabei klar auf die digitale operationelle Resilienz. Prüfungen erfolgen granularer, stärker wirksamkeitsorientiert und institutsindividuell, was zu vertieften Testanforderungen und differenzierteren Feststellungen führt.

Die bisherigen Prüfungsergebnisse zeigen wiederkehrende Schwachstellen. Häufig fehlt es an einer klar definierten und durch das Leitungsorgan getragenen Strategie für die digitale operationelle Resilienz mit messbaren Zielen und Risikotoleranzen. Kritische oder wichtige Funktionen sind nicht immer vollständig identifiziert oder konsistent mit Prozess- und Asset-Inventaren verknüpft, und Sicherheitsmaßnahmen werden teilweise nicht ausreichend risikobasiert umgesetzt oder regelmäßig überprüft. Auch im IKT-Drittparteienrisikomanagement bestehen Defizite, insbesondere bei der Berücksichtigung institutsspezifischer Anforderungen in Risikobewertungen, Verträgen und der laufenden Überwachung. Zudem sind Ausstiegsstrategien sowie die Einbindung von IKT-Drittanbietern in Resilienz- und Geschäftsfortführungstests häufig noch nicht ausreichend ausgereift.

Vor diesem Hintergrund hat die EZB im Rahmen ihrer Aufsichtsprioritäten für den Zeitraum 2026 bis 2028 gezielte Vor-Ort-Prüfungskampagnen zu Cyber- und Drittparteienrisiken sowie vertiefte Prüfungen von Cloud-Auslagerungen angekündigt.

Handlungsempfehlungen und nächste Schritte

Institute sollten bestehende Lücken in der DORA-Compliance systematisch identifizieren und über priorisierte Maßnahmenpläne schließen. Voraussetzung hierfür ist eine konsistente Governance mit klaren Verantwortlichkeiten, angemessener Ressourcenausstattung in den Überwachungs- und Kontrollfunktionen und eine aktive Einbindung des Leitungsorgans in die Steuerung von IKT- und Drittparteienrisiken. Aktuelle, konsistente und risikoorientierte Inventare von Geschäftsprozessen, IKT-Assets und Drittparteien sowie eine belastbare Methodik zur Identifikation kritischer oder wichtiger Funktionen bilden dabei die zentrale Grundlage.

Ein durchgängiges, risikobasiertes Drittparteienrisikomanagement sollte institutsspezifische Anforderungen konsequent vertraglich verankern und aktiv überwachen. Konzentrations-, Substitutions- und Ausstiegsrisiken sind systematisch zu adressieren und regelmäßig zu testen. Sicherheits- und Resilienzmaßnahmen sind wirksam umzusetzen, zu überprüfen und nachzuhalten, wobei IKT-Dienstleister konsequent end-to-end einzubeziehen sind. Nachhaltige digitale Resilienz erfordert integrierte Steuerung, regelmäßige Tests, belastbare Datenqualität und die enge Verzahnung von IKT- und operationellem Risikomanagement.

Fazit

Die bisherigen Erfahrungen mit DORA, dem IT Risk Questionnaire sowie den ersten eigenständigen DORA-Prüfungen machen deutlich, dass sich die Aufsichtspraxis nachhaltig verändert hat.

Digitale Resilienz wird nicht mehr isoliert als IT- oder Compliance-Thema betrachtet, sondern als zentraler Bestandteil der Gesamtbanksteuerung, der Governance, Prozesse, Technologie und Drittparteien gleichermaßen umfasst. Entscheidend ist nicht die formale Erfüllung regulatorischer Anforderungen, sondern der belastbare Nachweis ihrer Wirksamkeit im operativen Betrieb. Für Institute bedeutet dies, dass DORA nicht als zeitlich begrenztes Umsetzungsprojekt verstanden werden darf. Erwartet wird ein dauerhafter, integrierter Steuerungsansatz. Der IT Risk Questionnaire ist dabei ein zentrales Aufsichtsinstrument, da identifizierte Schwächen in der Selbsteinschätzung zunehmend zu vertieften Prüfungen führen können.

Institute, die ihre Governance früh stärken und operationelle Resilienz ganzheitlich verankern, verbessern ihre aufsichtliche Position und ihre langfristige Widerstandsfähigkeit.

Autoren

Dr. Henning Dankenbring
Mitglied des Beirats FIRM
KPMG ECB Office

Dina Friedrichs
Senior Manager
KPMG ECB Office

Elvira Niedermeier
Senior Manager
KPMG ECB Office

Scannen für Online-Version
https://firm.fm/?p=10856