

Operative Resilienz ist eine Führungsaufgabe

Warum bereichsübergreifende Governance zum Erfolgsfaktor wird:
Von der Umsetzung zur Wirksamkeit

Ein internationaler Flughafen zählt zu den komplexesten Organisationsstrukturen überhaupt. Täglich greifen zahlreiche Bereiche mit unterschiedlichen Aufgaben und Verantwortlichkeiten ineinander, um einen sicheren und stabilen Betrieb zu gewährleisten. Dabei sind Verantwortlichkeiten, Kommunikationswege und Aufgaben klar und geregelt.

Ein ähnlicher Grundsatz gilt für Finanzinstitute. Auch hier entsteht operative Resilienz nicht durch einzelne Maßnahmen oder isolierte Funktionen, sondern durch bereichsübergreifende Zusammenarbeit unter einer „Leitzentrale“.

Bereits kleine Störungen an den organisatorischen Schnittstellen können Auswirkungen auf den gesamten Betriebsablauf haben. Umgekehrt entsteht Stabilität dort, wo Prozesse ineinandergreifen, Informationen rechtzeitig verfügbar sind und Entscheidungen auf einer gemeinsamen Grundlage getroffen werden.

Die Umsetzung des Digital Operational Resilience Act (DORA) hat diese Zusammenhänge in dem vergangenen Jahr besonders deutlich werden lassen. Im Mittelpunkt standen zunächst regulatorische Anforderungen, neue Prozesse und organisatorische Anpassungen.

Mit etwas Abstand zur Einführungsphase zeigt sich jedoch eine weitergehende Erkenntnis: Die nachhaltige Wirkung regulatorischer Anforderungen entsteht nicht allein durch deren Umsetzung, sondern durch ihre Verankerung in der täglichen Unternehmenssteuerung.

Die entscheidende Frage lautet daher nicht nur: „Haben wir die Anforderung umgesetzt?“ Sondern vielmehr: „Sind wir als Institut in der Lage, Risiken ganzheitlich zu steu-

ern, um auch unter herausfordernden Bedingungen handlungsfähig zu bleiben?“

Operationale Resilienz ist damit nicht ausschließlich eine regulatorische Anforderung. Sie ist ein wesentlicher Bestandteil wirksamer Unternehmenssteuerung und lässt Themen, welche Schnittstellen zueinander haben, zusammenwachsen.

1. Operative Resilienz entsteht im Zusammenspiel

Operative Resilienz wird häufig zunächst einzelnen Themenfeldern oder Fachbereichen zugeordnet – z. B. der Informationssicherheit, dem IKT-Risikomanagement oder dem Notfallmanagement.

Diese Betrachtung greift jedoch zu kurz. Die Fähigkeit eines Instituts, auch unter außergewöhnlichen oder belastenden Rahmenbedingungen stabil und handlungsfähig zu bleiben, ist keine isolierte Aufgabe einzelner Bereiche. Sie ist vielmehr Ausdruck einer ganzheitlichen Steuerungsfähigkeit der Organisation.

Mit Einführung von DORA ist dieses Verständnis stärker in den Mittelpunkt gerückt. Die Verordnung fordert nicht nur belastbare Prozesse und Kontrollen, sondern stärkt vor allem den Anspruch an eine bereichsübergreifende und wirksame Unternehmenssteuerung. Der Fokus verschiebt sich damit von der isolierten Erfüllung einzelner **Anforderungen hin zur gesamtheitlichen Steuerung der Risiken im Risikomanagement der Bank.**

Managementimpulse

- ▶ Verstehen wir operative Resilienz als gemeinsame Aufgabe der gesamten Organisation?
- ▶ Werden wesentliche Risiken aus unterschiedlichen Perspektiven betrachtet und zusammengeführt?
- ▶ Verfügen wir über eine gemeinsame Grundlage für strategische Entscheidungen?

2. Schnittstellen entscheiden über Resilienz

Die Leistungsfähigkeit komplexer Organisationen entscheidet sich häufig nicht innerhalb einzelner Bereiche, sondern am Zusammenspiel.

Dies kann nur zuverlässig funktionieren, wenn Informationen und Ergebnisse zwischen den beteiligten Bereichen rechtzeitig verfügbar sind, Verantwortlichkeiten klar geregelt sind und Entscheidungen auf einer gemeinsamen Grundlage getroffen werden. Gerade an diesen Schnittstellen zeigt sich, ob das Gesamtsystem funktioniert.

DORA beinhaltet klare Regelungen für eine resiliente Organisation. Sie entsteht jedoch nicht von selbst. Sie ist das Ergebnis des abgestimmten Zusammenwirkens verschiedener Steuerungs- und Kontrollfunktionen.

Informationssicherheit/IKT-Risikokontrolle, Datenschutz, BCM, Compliance oder Auslagerungsmanagement erfüllen jeweils einen eigenständigen Auftrag und bringen ihre spezifische Expertise und ihren Blick auf Risiken mit ein.

Sehen wir die Umsetzung der DORA-Verordnung als Chance – so entsteht ein Mehrwert nicht durch die isolierte Betrachtung der einzelner Themenfelder, sondern durch die Fähigkeit, unterschiedliche Perspektiven zusammenzuführen und ein gemeinsames Verständnis von Risiken, Auswirkungen und Handlungsbedarfen zu entwickeln.

Die praktische Umsetzung regulatorischer Anforderungen hat gezeigt, dass Herausforderungen häufig nicht innerhalb einzelner Verantwortungsbereiche entstehen, sondern dort, wo Übergaben stattfinden und eine wirksame Verzahnung sicherzustellen ist.

Beispiele hierfür sind:

- ▶ Unterschiedliche Risikobewertungen
- ▶ Fehlende gemeinsame Informationsgrundlage
- ▶ Unklare Verantwortlichkeit bei bereichsübergreifenden Themen
- ▶ Verzögerung bei Entscheidungen

Die Qualität einer Institution bemisst sich nicht allein an der Leistungsfähigkeit ihrer einzelnen Funktionen. Entscheidend ist vielmehr, wie gut diese miteinander vernetzt sind und gemeinsam zur Steuerungsfähigkeit des Instituts beitragen.

Managementimpulse

- ▶ Wo liegen in Ihrem Institut die entscheidenden Schnittstellen – und wie stellen Sie sicher, dass dort Informationen und Verantwortlichkeiten wirksam ineinandergreifen?
- ▶ Sind Verantwortlichkeiten und Entscheidungswege über Bereichsgrenzen hinweg wirksam ausgestaltet?

3. Aus Ereignissen lernen: Governance zeigt sich im Ernstfall

Auch komplexe Systeme wie ein Flughafen entwickeln sich kontinuierlich weiter: Ereignisse werden analysiert, Abläufe überprüft und Verbesserungen umgesetzt. Hier ist es von essenzieller Bedeutung, Verbesserungen über das Gesamtsystem umzusetzen, um keine Lücken im Zusammenspiel zu schaffen. Genau dieser Gedanke ist auch für die operative Resilienz von Finanzinstituten entscheidend: Zum Beispiel der Umgang mit IKT-Vorfällen verdeutlicht dies besonders.

Die strukturierte Erfassung und Dokumentation eines Vorfalls ist eine wichtige Grundlage. Sie schafft Transparenz und ermöglicht Nachvollziehbarkeit.

Der eigentliche Mehrwert entsteht jedoch erst dann, wenn die gewonnenen Erkenntnisse genutzt werden:

- ▶ Welche Ursachen lagen zugrunde?
- ▶ Welche Prozesse haben funktioniert?
- ▶ Wo bestanden Schwachstellen?
- ▶ Welche Maßnahmen verbessern die Widerstandsfähigkeit nachhaltig?

Ein Vorfall sollte daher nicht ausschließlich als abgeschlossenes Ereignis betrachtet werden, sondern als Möglichkeit zur Weiterentwicklung der Organisation. Dabei spielt wiederum die Zusammenarbeit verschiedener Funktionen eine zentrale Rolle. Erst durch die gemeinsame Betrachtung von technischen, organisatorischen und regulatorischen Aspekten entsteht ein ganzheitliches Bild.

Dokumentation schafft Transparenz. Erst die gemeinsame Auswertung schafft Resilienz.

Managementimpulse

- ▶ Nutzen Sie die Erkenntnisse aus Vorfällen und Risiken systematisch zur Weiterentwicklung Ihrer Organisation?
- ▶ Sehen Sie die Erkenntnisse als Chance zur Verbesserung Ihrer Resilienz?

4. Governance als Führungsaufgabe

Operative Resilienz ist kein isoliertes Fachthema und keine rein regulatorische Verpflichtung. Sie ist ein wesentlicher Bestandteil einer zukunftsfähigen Unternehmenssteuerung.

Die Rolle des Leitungsorgans besteht dabei nicht darin, sämtliche operativen Details zu steuern. Vielmehr gilt es, eine Organisationsstruktur zu schaffen, in der Verantwortung klar verankert ist, Risiken transparent bewertet werden und fundierte Entscheidungen auf einer Grundlage getroffen werden können.

Wie bei dem komplexen System des Flughafens entsteht Stabilität nicht durch die Optimierung einzelner Einheiten, sondern durch das abgestimmte Zusammenspiel aller Beteiligten.

Die Umsetzung regulatorischer Anforderungen entfaltet daher ihren nachhaltigen Wert erst dann, wenn sie nicht nur formal erfüllt, sondern in die tägliche Steuerung der Organisation integriert wird.

Eine wirksame Governance zeigt sich nicht in der Anzahl vorhandener Regelwerke oder Kontrollen. Sie zeigt sich darin, ob eine Organisation auch unter veränderten Rahmenbedingungen handlungsfähig bleibt und Entscheidungen auf einer belastbaren Grundlage treffen kann.

Managementimpulse

- ▶ Haben wir ein gemeinsames Verständnis darüber, welche Faktoren unsere operative Resilienz maßgeblich beeinflussen?
- ▶ Sind unsere Governance-Funktionen so miteinander verzahnt, dass Risiken ganzheitlich betrachtet werden?
- ▶ Nutzen wir regulatorische Anforderungen als Impuls zur Weiterentwicklung unserer Unternehmenssteuerung?

Fazit – von der Regulierung zur gelebten Resilienz

Die Umsetzung von DORA hat viele Institute dazu veranlasst, bestehende Strukturen, Prozesse und Verantwortlichkeiten kritisch zu hinterfragen und weiterzuentwickeln.

Die wichtigste Erkenntnis geht dabei jedoch über einzelne regulatorische Anforderungen hinaus:

Operative Resilienz entsteht nicht allein durch Regelwerke, Prozesse oder Kontrollen. Sie entsteht dort, wo Verantwortung übernommen wird, Informationen wirksam zusammengeführt werden und unterschiedliche Bereiche gemeinsam zur Stabilität der Organisation beitragen.

Vielleicht liegt genau darin die wichtigste Erkenntnis aus der Umsetzung von DORA: Der Blick muss sich vom einzelnen Prozess und der einzelnen Anforderung hin zur ganzheitlichen Steuerung des Gesamtsystems verändern.

Stabilität entsteht nicht durch die isolierte Optimierung einzelner Bereiche, sondern durch das abgestimmte Zusammenspiel aller Beteiligten. Regulatorik schafft den Rahmen. Wirksame Unternehmenssteuerung schafft Resilienz. ■



Katja Schlüter

Beauftragte Informationssicherheit & Datenschutz,
E-Mail: katja.schlueter@dz-cp.de



Marc-Timo Brandenburger

Beauftragter Informationssicherheit & Datenschutz,
E-Mail: marc-timo.brandenburger@dz-cp.de