FIRM
Frankfurt Institute for
Risk Management and Regulation

White Paper – September 2023

ROUND TABLE PAYMENTS

Risikomanagement und operative Resilienz im Zahlungsverkehr

Von Dr. Markus Ampenberger, Prof. Dr. Tobias Berg und Daniel Regending

Inhalt

A Zusammenfassung

Die Bedeutung des elektronischen Zahlungsverkehrs hat in den letzten Jahren rasant zugenommen. Gründe dafür sind technologische Innovationen, fortschreitende Digitalisierung und eine Modernisierung der Marktinfrastruktur. Für Banken stellt die Abwicklung des Konto- und Kartenzahlungsverkehrs daher eine Kernwertschöpfungskette und ein wichtiges Geschäftsfeld dar.

Aus regulatorischer Perspektive gehört der Zahlungsverkehr zur kritischen Marktinfrastruktur. Auch für die Privat- und Firmenkunden von Finanzdienstleistern stehen Stabilität, Zuverlässigkeit, Datensicherheit und Servicequalität im Zahlungsverkehr im Vordergrund. Das Marktumfeld ist dynamisch und von technologischer Entwicklung, immer anspruchsvolleren Kundenerwartungen zur „Echtzeit-Abwicklung" von Zahlungen und geopolitischen Konflikten geprägt. Daher muss sich ein aktives Risikomanagement im Zahlungsverkehr kontinuierlich anpassen. Die operative Stabilität rückt zudem in den Fokus von Regulatoren und Aufsichtsbehörden, u.a. der European Banking Authority, nationalen Aufsichtsbehörden, EZB und Deutschen Bundesbank.

Operative Resilienz bezeichnet dabei die Fähigkeit, kritische Kernfunktionen auch im Störungsfall weiterhin erbringen zu können. Für Banken in Deutschland sind dazu fünf Kernelemente besonders wichtig: organisatorische Aufstellung, interne Kontrollsysteme, stabile IT-Infrastruktur, ein funktionierendes Notfall-Management sowie die Etablierung einer adäquaten Risikostrategie und -kultur.

Zur weiteren Verbesserung der operativen Resilienz im Zahlungsverkehr gibt es für Banken sowohl interne als auch externe Handlungsfelder. Intern benötigen Banken eine klare Risiko-Strategie, ein bereichsübergreifendes Betriebsmodell, und ein regulatorischer „Radar", um gesetzliche Anforderungen und/oder verpflichtende Änderungen in der Marktinfrastruktur zu antizipieren und termingerecht umzusetzen. Dafür bedarf es qualifiziertes Personal sowie ein Risikomanagement, das auch externe Vendoren oder Partner im Zahlungsverkehr aktiv einbezieht. Extern ergeben sich ebenfalls eine Reihe möglicher Maßnahmen: Ein Austausch unter Banken und ggf. mit nationalen Sicherheitsbehörden zur Einschätzung der aktuellen Cyber-Gefährdungs- und Bedrohungslage, sowie ein Austausch mit anderen Branchen, die ebenfalls zur kritischen Infrastruktur gehören, um voneinander zu lernen. Die Festlegung von Branchenstandards zu operativer Resilienz kann Instituten helfen, besser einzuschätzen wo sie stehen und eine Diskussion zum Aufbau gemeinsamer Notfallmechanismen die operative Resilienz in der Bankenbranche möglicherweise dauerhaft verbessern.

B Kontext: Marktumfeld und Problemstellung

B.1 ZAHLUNGSVERKEHR ALS SYSTEMRELEVANTE INFRASTRUKTURFUNKTION

Der Zahlungsverkehr hat sich in den letzten zehn Jahren in Deutschland und Europa stark verändert. Im europäischen Wirtschaftsraum wurden nationale Zahlungsverkehrslösungen im Konto-Zahlungsverkehr, beispielsweise bei Überweisungen und Lastschriften, durch einen einheitlichen Euro-Zahlungsverkehr abgelöst, den SEPA-ZV. Im Karten-Zahlungsverkehr dominieren zwar oft noch nationale Debitkarten-Schemes wie zum Beispiel die Girocard (im Sprachgebrauch auch „EC-Karte") in Deutschland oder Carte Bancaire in Frankreich. Jedoch gewinnen internationale Kreditkartennetzwerke wie VISA, Mastercard oder American Express immer mehr an Bedeutung. Neue Technologien und Innovationen haben dafür gesorgt, dass Konsumenten neben klassischen Bezahlverfahren – also Bargeld, Überweisungen, Lastschriften und Kartenzahlungen – auch neue Bezahlmethoden nutzen können. Dazu zählen unter anderem mobile Payments, beispielsweise Apple Pay oder Google Pay, digitale Wallets wie Paypal oder Echtzeitüberweisungen, also Instant Payments. Durch das starke Wachstum im e-/m-Commerce ist für viele Händler die einfache, reibungslose Abwicklung von Zahlungen online – oft in Verbindung mit moderner Konsumgüterfinanzierung „Buy Now, Pay Later" – mittlerweile genauso wichtig wie die Akzeptanz von elektronischen Zahlungen an der Ladenkasse. Das Ökosystem des Zahlungsverkehrs umfasst sowohl eine Vielzahl an etablierten Marktteilnehmern – Banken, Kartennetzwerke, Karten Issuer, Merchant Acquirer und spezialisierte ZV-Dienstleister – als auch neue Anbieter von Zahlungsverkehrsprodukten wie FinTechs und BigTechs. Der Wettbewerbsdruck, aber auch Kooperationsmöglichkeiten nehmen in diesem Ökosystem kontinuierlich zu.

Das Girokonto und die grundlegende Abwicklung von Zahlungen stellen weiterhin eine Kernwertschöpfungskette im Bankengeschäft dar. Der Zahlungsverkehr ist ein technologieintensives, skalengetriebenes Geschäftsfeld mit einem sehr hohen Automatisierungs- und Digitalisierungsgrad. Das Geschäftsfeld gibt Banken die Möglichkeit, stabile Provisionserträge mit relativ geringer Kapitalunterlegung zu realisieren und stabile Kundenbeziehungen zu pflegen. Ein hoher Innovationsgrad erfordert die kontinuierliche Weiterentwicklung einer modernen ZV-Infrastruktur unter anderem durch die Einführung neuer Nachrichtenformate ISO 20022, Request-to-Pay- und Instant-Payment-Leistungen sowie perspektivisch die Etablierung eines digitalen Euro als Central Bank Digital Currency (CBDC). Bei dieser Modernisierung arbeiten viele Banken mit externen IT-Vendoren oder BPO-Partnern zusammen.

Spezialisierte Zahlungsverkehrs-Unternehmen und FinTechs mit Zahlungsverkehrsschwerpunkt haben in der zurückliegenden Dekade starkes Marktwachstum und gute Kapitalmarktbewertungen erzielt. Allerdings hat sich die Bewertung von Payment-Dienstleistern ähnlich wie in anderen Technologiebranchen nach Rekordjahren in den letzten beiden Jahren erstmals – mitunter deutlich – normalisiert. Zusätzlich beeinflussen geopolitische Konflikte – beispielsweise der Russland-Ukraine Krieg – den Zahlungsverkehr. Der internationale SWIFT-Zahlungsverkehr wird als wichtiges Sanktionsmittel eingesetzt und führt damit zu einem erhöhten Aufkommen an Sanktions- und Embargoprüfungen bei den Instituten.[1] Darüber hinaus hat die Anzahl an Cyberangriffen mit Unterstützung staatlicher Institutionen als Instrument der asymmetrischen Kriegsführung in den letzten Jahren deutlich zugenommen. Das gesteigerte Interesse der Regulatoren und Aufsichtsbehörden an der Payments-Branche unterstreicht die Bedeutung des Zahlungsverkehrs als kritische Infrastruktur für internationale Finanzmärkte und als Basis für wirtschaftliche und gesellschaftliche Aktivitäten.[2]

B.2 EIN ROBUSTES RISIKOMANAGEMENT IM ZAHLUNGSVERKEHR IST UNABDINGBAR

In dem dynamischen, immer komplexeren Marktumfeld gewinnt das Risikomanagement im Zahlungsverkehr und die operative Resilienz der ZV-Infrastruktur an Relevanz. Dies ergibt sich insbesondere aus drei Faktoren:

(i) Die Stabilität des Zahlungsverkehrs steht für die Privat- und Firmenkunden genauso wie für Finanzinstitutionen im Vordergrund. Es besteht nur eine minimale Fehlertoleranz für die korrekte, termingerechte Ausführung von Zahlungsströmen.

(ii) Der Schutz der sensiblen Konto- und Transaktionsdaten sowie Cyber-Sicherheit gewinnt vor dem Hintergrund zunehmender Digitalisierung und ebenfalls immer öfter auftretenden und raffinierteren Hacker-Angriffen an Bedeutung.

(iii) Die operative Stabilität des Zahlungsverkehrs rückt außerdem weiter in den Fokus der nationalen und internationalen

1 Vgl. zur Relevanz des Zahlungsverkehrs bei geopolitischen Konflikten u. a. die Berichterstattung in der Presse: Wirtschaftswoche 02/2022 "Swift: Die ultimative Sanktionswaffe gegen Russland", Handelsblatt 02/2022 „Neue Forderungen nach Ausschluss Russlands aus Zahlungsverkehrssystem Swift", FAZ 02/2022 „Westen schließt russische Banken von SWIFT aus".

2 Der karten- und kontogestützte Zahlungsverkehr gehört zur kritischen Infrastruktur i.S.v. § 10 Absatz 1 Satz 1 des BSI-Gesetzes und wird durch das Bundesamt für Sicherheit in der Informationstechnik überwacht.

Regulatoren, u. a. der European Banking Authority (EBA), nationalen Aufsichtsbehörden, EZB und Deutsche Bundesbank.

B.3 ÜBERBLICK ZU WESENTLICHEN RISIKEN IM ZAHLUNGSVERKEHR

Im Zahlungsverkehr gibt es unterschiedliche Risikoarten (vgl. Abbildung 1), die größtenteils von operationellen Risiken geprägt sind und die es für Banken aktiv zu steuern gilt:

(i) Finanzielle Risiken, zum Beispiel Kreditrisiken bei der Ausgabe von Kreditkarten oder im Zahlungsakzeptanzgeschäft,

(ii) Rechtliche beziehungsweise Compliance Risiken im Zusammenhang mit Finanzkriminalität (Prävention von Geldwäsche und Terrorismusfinanzierung, Einhaltung von Sanktions-/Embargoregelungen),

(iii) IT-Risiken aus Cyberangriffen, Einhaltung des Datenschutzes beziehungsweise Gewährleistung von Stabilität der ZV-Plattformen bei hoher Spitzenauslastung und

(iv) operative Risiken zum Beispiel aus der Zusammenarbeit mit externen Partnern oder einem Business Process Outsourcing sowie gegebenenfalls Fehler des eigenen Personals bei manuellen Prozessen.

Aus diesen Risiken und vor dem Hintergrund der Stabilitätsanforderungen des Zahlungsverkehrs ergibt sich ein gesteigerter Bedarf für ein aktives Risikomanagement zur Erhöhung der operativen Resilienz. Diese rückt auch zunehmend in den regulatorischen Fokus.

Abbildung 1: Relevante Risiken im Zahlungsverkehr

C Operative Resilienz im Zahlungsverkehr

C.1 BEGRIFFSDEFINITION UND WESENTLICHE KOMPONENTEN: OPERATIVE RESILIENZ

Der Begriff „operative Resilienz" wird in den Basel Committee on Banking Supervision (BCBS) Principles for Operational Resilience vom 31.03.2021 und im Digital Operational Resilience Act (DORA) vom 17.01.2023 näher definiert. Operative Resilienz bezeichnet demnach die Fähigkeit einer Bank, kritische Kernfunktionen wie Zahlungsverkehrsleistungen auch im Störungsfall erbringen zu können. Das BCBS hat dazu sieben Prinzipien formuliert. Insbesondere fokussieren diese auf folgende Aspekte:

1. die Integration operativer Resilienz in die bestehende Governance des Instituts,
2. die Integration operativer Resilienz in das bestehende Risikomanagement des Instituts,
3. die Entwicklung von Business Continuity Plänen,
4. die Ermittlung von Abhängigkeiten kritischer Geschäftsprozesse,
5. die Steuerung und Überwachung der Beziehungen zu Drittanbietern und Vendoren,
6. die kontinuierliche Verbesserung des Incident Managements sowie
7. die Sicherstellung von Cyber und Data Security

Vergleichbare Kernkomponenten finden sich auch in DORA (vgl. Abbildung 2). Diese Komponenten sind

- Risikomanagement,
- Business Continuity Management,
- Incident Reporting,
- Penetration Testing gegen simulierte (z. B. Cyber-) Attacken[3], und
- Vendorenmanagement

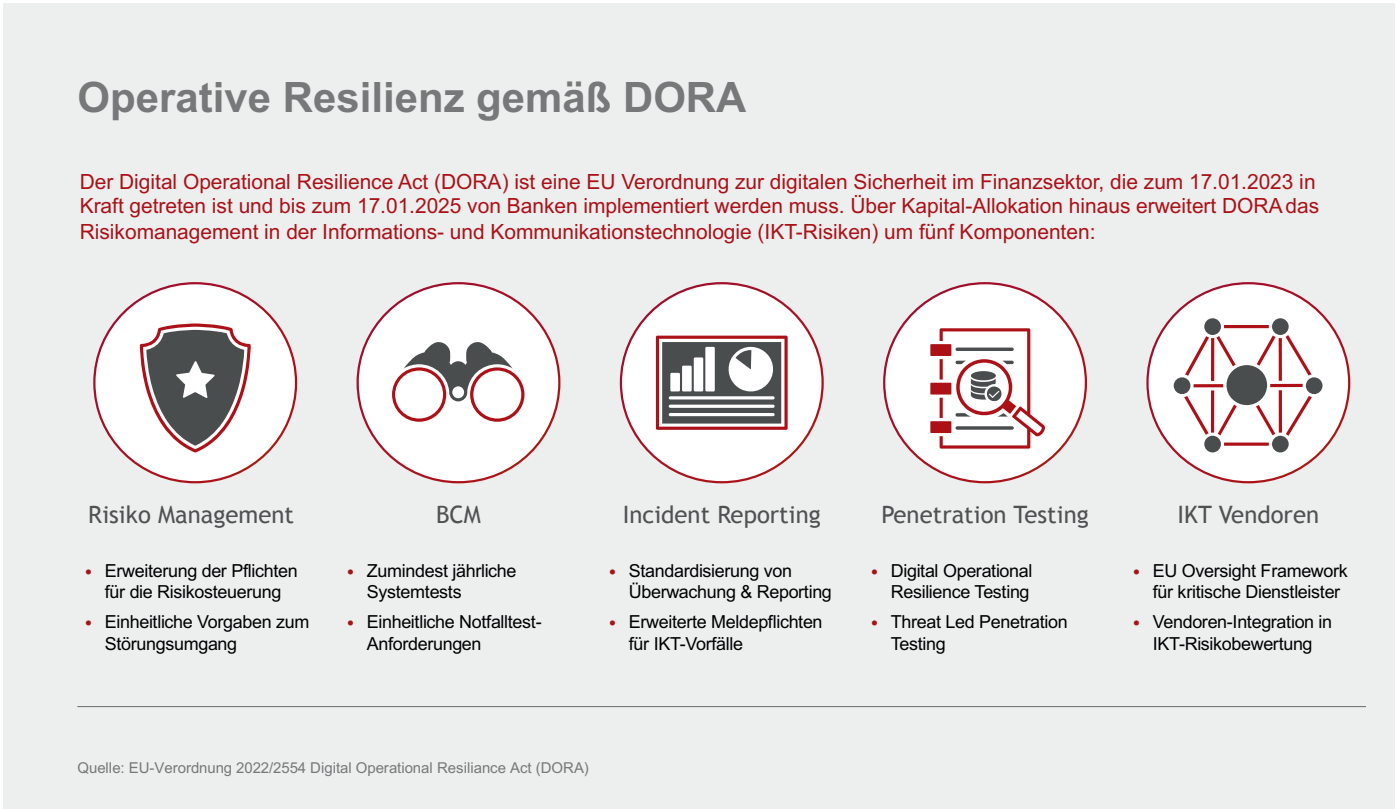

Abbildung 2: Definition von operativer Resilienz gemäß DORA

3 Ein Beispiel stellt der geplante Cyber Resilience Stress Test der EZB im Jahr 2024 dar, dessen Ergebnis in den Supervisory Review and Evaluation Process (SREP) einfließen wird. Basis ist ein Katalog an rund 500 zu beantwortenden Fragen.

C.2 GRUNDLAGE DER STUDIE

Grundlage dieses White Papers sind Erkenntnisse aus strukturierten Interviews mit mehreren Banken in Deutschland zwischen November 2022 und Februar 2023 zum Risikomanagement im Allgemeinen und zur operativen Resilienz im Speziellen für den Zahlungsverkehr. Dabei waren die aktuellen Marktherausforderungen, die Aufstellung der Institute in Bezug auf Organisation, Prozesse, internes Kontrollsystem sowie IT-Infrastruktur im Zahlungsverkehr, und mögliche bank-interne oder branchenübergreifende Optimierungsmaßnahmen im Fokus der Diskussion. Gesprächspartner waren unter anderem Leiter der Zahlungsverkehrseinheiten, Leiter des Produktmanagements im Zahlungsverkehr und Experten aus dem Risikomanagement für den Zahlungsverkehr.

C.3 AKTUELLE HERAUSFORDERUNGEN UND AUFSTELLUNG DER BANKEN

Im generellen Marktumfeld sind aktuell insbesondere regulatorische Entwicklungen im Fokus der Banken. Im Vordergrund stehen – zum Zeitpunkt der Interviews – kurzfristig die Konsolidierung der Clearing- und Settlement-Infrastruktur T2/T2S im Zahlungsverkehr und in der Wertpapierabwicklung in Europa sowie die einheitliche Einführung der ISO 20022 Datenformate im grenzüberschreitenden Zahlungsverkehr. Weitere Hauptthemen sind die Anforderungen zu Instant Payments, zum Beispiel im aktuell laufenden Gesetzgebungsverfahren der Europäischen Kommission, die aktive und passive Abwicklung von Echtzeitzahlungen für alle Zahlungsdienstleister und Banken in Europa verpflichtend zu machen. Auf der Agenda stehen weiterhin künftige Anforderungen zur IT, Cyber- und Datensicherheit, unter anderem aus der DORA-Regulierung EU 2022/2554, die ab 1. Januar 2023 gilt und bis Ende 2025 verpflichtend umzusetzen ist. Außerdem findet aktuell ein Review der EU-Richtline Payment Service Directive 2 (PSD2) 2015/2366 statt, so dass im Laufe des Jahres 2023 mit einem ersten Entwurf für eine Payment Service Directive 3 zu rechnen ist. Perspektivisch spielt auch die mögliche Einführung eines digitalen Euros eine wichtige Rolle. Darüber hinaus gilt es für die Zahlungsverkehrsspezialisten in den Banken, neue Regularien in angrenzenden, für den Zahlungsverkehr sehr relevanten Bereichen wie etwa digitale Assets oder die Anforderungen aus einer Weiterentwicklung der Geldwäscheregulierung kontinuierlich zu beobachten, zu bewerten und umzusetzen. Das gilt beispielsweise für die MiCA-Regulierung (Markets in Crypto Assets, EU-Verordnung 2019/1937).

Für viele Banken kommt dabei hinzu, dass sie im Zahlungsverkehr auf einer veralteten Infrastruktur arbeiten, die in den nächsten Jahren einer grundlegenden Modernisierung bedarf. Dabei haben die Zahlungsverkehrs-Applikationen typischerweise wichtige Schnittstellen in das Kernbanksystem oder zu angrenzenden IT-Anwendungen. Dazu gehören vor allem das Kontomodul, aber auch Systeme für das Transaktionsmonitoring zur Geldwäscheprävention oder zur Embargo- und Sanktionsprüfung. Dieser Modernisierungsdruck und die gleichzeitig massiven Veränderungen in der Zahlungsverkehrsinfrastruktur führen zu einem hohen Investitionsbedarf und der Notwendigkeit, Priorisierungsentscheidungen zwischen regulatorischen Anforderungen, Modernisierungs- oder Konsolidierungsmaßnahmen in der Legacy IT sowie Produktinnovationen zu treffen. Die Anforderungen werden in großen, komplexen Change-Projekten umgesetzt, die eine enge Zusammenarbeit zwischen Fachbereichen wie zum Beispiel dem Produktmanagement für den Zahlungsverkehr, Zahlungsverkehrs Operations und Compliance/Risikomanagement sowie der IT erfordern. Aufgrund dieser notwendigen Maßnahmen und des stetigen Kostendrucks in einem skalengetriebenen Geschäftsfeld hat das Outsourcing der Zahlungsverkehrsabwicklung von Banken an spezialisierte Dienstleister in den letzten Jahren an Bedeutung gewonnen. Damit gehen aber auch wiederum gesteigerte Anforderungen an das Risikomanagement beziehungsweise die Steuerung und Überwachung eines BPO-Providers einher.

Ein vielfach bestätigtes Problem für Banken ist dabei, ausreichend und qualifiziertes Personal mit Zahlungsverkehrs-Knowhow zu gewinnen, zu fördern und zu binden. Interviewteilnehmer beobachten einen verstärkten Wettbewerb um begrenzte Fachressourcen, auch da viele Marktteilnehmer aufgrund der massiven Modernisierung in der Marktinfrastruktur und regulatorischer Zeitvorgaben ähnliche Change-Projekte zeitgleich durchführen.

C.4 BEDEUTUNG DES RISIKOMANAGEMENTS ZU OPERATIVER RESILIENZ

Aufgrund der zuvor beschriebenen allgemeinen Risiken im Zahlungsverkehr, Marktherausforderungen und daraus abgeleiteten Veränderungsaufgaben wird das Thema „operative Resilienz“ für viele Institute immer relevanter. Das Notfallmanagement (Business Continuity Management), bei dem die Gefährdungsanalyse, Notfalltests und die Ableitung von Notfallplänen (Disaster Recovery Plan) zur möglichst schnellen Herstellung eines funktionierenden Geschäftsbetriebs nach einer Extremsituation im Fokus stehen, ist für Banken ein selbstverständliches und regulatorisch gefordertes Element des Risikomanagements. Operative Resilienz geht jedoch über das reine Notfallmanagement hinaus und hat einen stärkeren Fokus auf präventive Maßnahmen („Operational Resilience by Design“), die die Einhaltung des vorab definierten Risikoappetits möglichst sicherstellen sollen.

Operative Resilienz bezeichnet also die Fähigkeit, operative Risiken und Szenarien für den Geschäftsbetrieb frühzeitig

zu erkennen, Gefahren vorzubeugen, Maßnahmen zu entwickeln, auf Notfallsituationen zu reagieren und aus Gefährdungssituationen zu lernen. Sie betrifft die Organisations- und Geschäftsprozesse mit einem hohen Fokus auf IT- und Datensicherheit im Zahlungsverkehr. Daher bedarf ein bankinternes Programm zur Stärkung der operativen Resilienz in der Regel der Teilnahme aller am Zahlungsverkehr beteiligten Fachbereiche, um hier End-to-End Risikomanagemententscheidungen zu verbessern und gleichzeitig die Geschäftsstrategie im Blick zu behalten. Aus den geführten Interviews hat sich gezeigt, dass für die meisten Banken fünf Kernelemente wichtig sind im Kontext der operativen Resilienz: organisatorische Aufstellung, interne Kontrollsysteme, stabile IT-Infrastruktur, ein funktionierendes Notfall-Management sowie eine adäquate Risikostrategie und -kultur (vgl. Abbildung 3)

Abbildung 3: Kernelemente operativer Resilienz

Der Begriff „operative Resilienz“ spielt im aktiven Sprachgebrauch der an der Befragung teilnehmenden Institute überwiegend bisher eine untergeordnete Rolle. Der eigene Reifegrad der operativen Resilienz wird von den Interviewteilnehmern als „mittel bis hoch“ und damit als z. T. noch ausbaufähig eingeschätzt, wobei alle teilnehmenden Banken diese Selbstbeurteilung auf Basis der aktuell geltenden regulatorischen Anforderungen abgegeben haben (also vor Inkrafttreten von DORA ab 2025). Da in diesem Bereich des Risikomanagements bislang nur wenig Austausch stattfindet und damit kaum Branchentransparenz existiert, können viele Institute nicht vollständig einschätzen, wie gut oder schlecht sie im Vergleich zu Wettbewerbern aufgestellt sind (vgl. Abbildung 4).

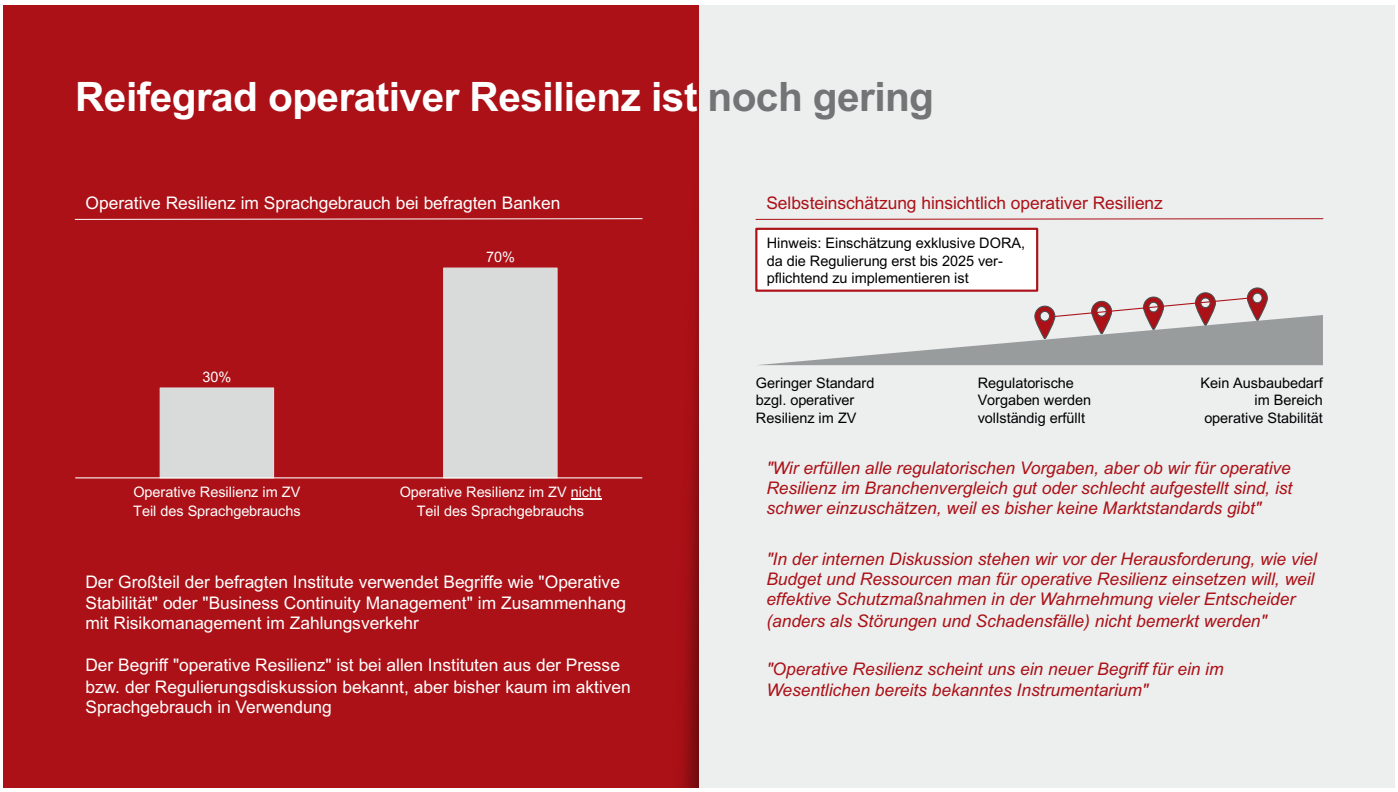

Abbildung 4: Reifegrad operativer Resilienz in deutschen Banken

Zur Steigerung der operativen Resilienz wurden verschiedene interne Maßnahmen genannt: Change-Projekte zur Implementierung regulatorischer Anforderungen oder zur Modernisierung der IT-Infrastruktur, Mitarbeiterschulungen und eine beständige Weiterentwicklung der Risiko- und Resilienz-Strategie. Diese Maßnahmen bedürfen kontinuierlicher Umsetzung und Weiterentwicklung, um dem ständigen Change-Prozess und hohen Innovationsgrad im Geschäftsfeld Zahlungsverkehr gerecht zu werden.

C.5 BETRIEBSMODELL ZUR STÄRKUNG DER OPERATIVEN RESILIENZ IM ZAHLUNGSVERKEHR

Ein erfolgreiches Betriebsmodell zur Stärkung der operativen Resilienz im Zahlungsverkehr umfasst demnach vier Kernelemente (vgl. Abbildung 5):

- Strategie,
- Organisation und Governance,
- Zahlungsverkehrs-Risikomanagement sowie
- Grundlagen und Enabler.

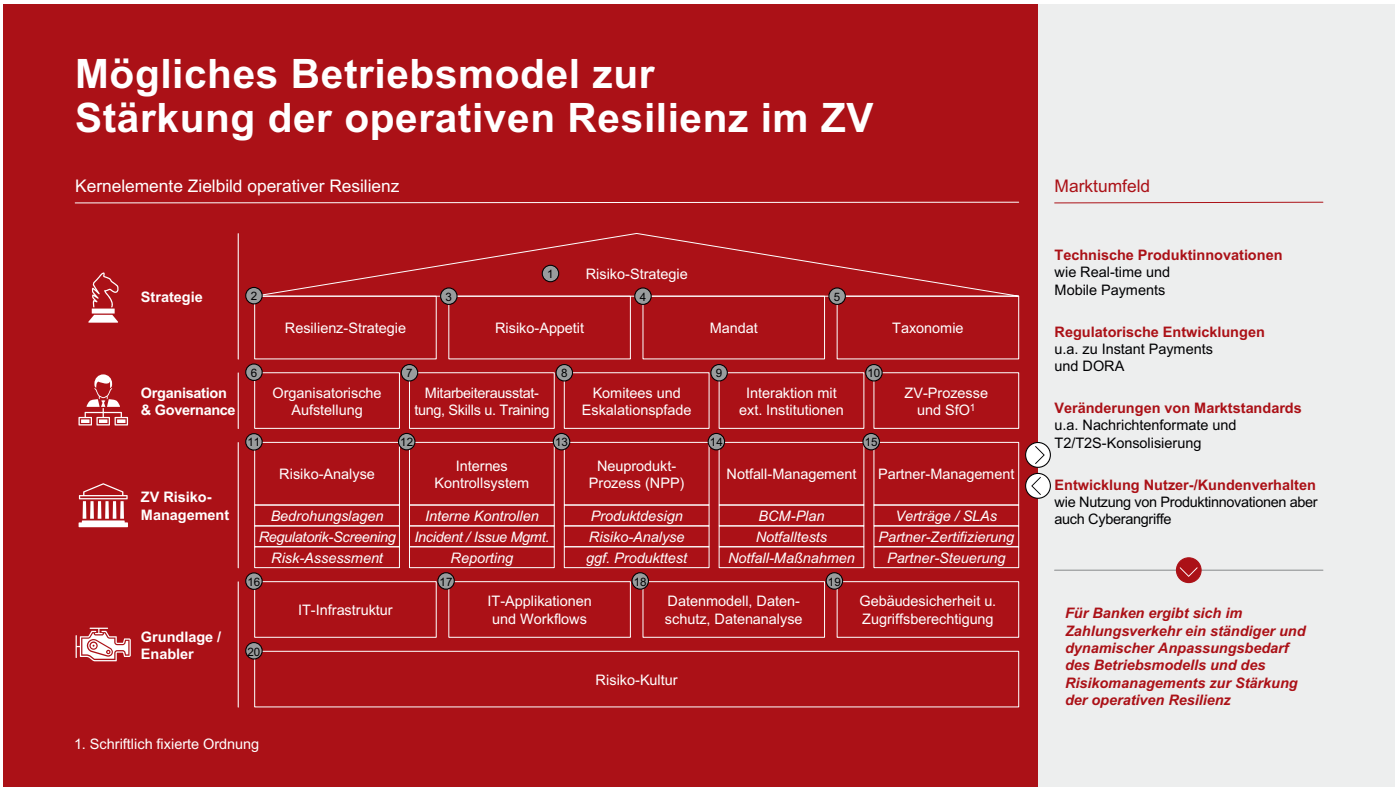

Abbildung 5: Betriebsmodell zur Stärkung der operativen Resilienz im Zahlungsverkehr

Diese Elemente sind jedoch nicht statisch, sondern müssen dynamisch weiterentwickelt werden. Wie schon zuvor im Detail ausgeführt, ist das Marktumfeld geprägt von technischen Produktinnovationen, regulatorischen Entwicklungen, stetiger Weiterentwicklung des Nutzer- und Kundenverhaltens und Veränderungen von Marktstandards. Dazu gehören zum Beispiel die Einführung von Echtzeitzahlungen, die Aktualisierung der im Zahlungsverkehr verwendeten Datenformate oder perspektivisch auch die Einführung digitaler Zentralbankwährungen. Entsprechend bedarf es einer wiederkehrenden Evaluation und Anpassung der Kernelemente des Betriebsmodells zur Stärkung der operativen Resilienz.

Übergreifend benötigt das Risikomanagement im Zahlungsverkehr eine adäquate Risiko-Strategie, die auch eine daraus abgeleitete Resilienz-Strategie enthält. Weitere wichtige Elemente der Risiko-Strategie im Zahlungsverkehr sind ein von der Bank gesetzter Risiko-Appetit, ein entsprechend klar beschriebenes Mandat zum Risikomanagement im Zahlungsverkehr sowie eine organisationsübergreifende, einheitliche Risiko-Taxonomie. Wesentliche Fragen aus Sicht operativer Resilienz sind zum Beispiel:

- Wie sind ZV-Risiken in die Risiko-Strategie der Bank integriert?
- Welche ZV-Kernprozesse müssen auch in einem Worst-Case-Szenario stabil weiter funktionieren?
- Welche Ausfallzeiten werden für ZV-Kernprozesse und IT-Systeme maximal toleriert?
- Welche Schutzmaßnahmen gegen Cyberattacken sollen etabliert werden?
- Wie viele PSD2-Meldungen[4] sind tragbar?

Die Organisation als solche spielt ebenfalls eine zentrale Rolle für die operative Resilienz des Zahlungsverkehrs. Insbesondere die Fähigkeiten und Kapazitäten der Mitarbeiter wurden von den meisten Interviewteilnehmer als zentraler Erfolgsfaktor und oft auch als aktueller Engpassfaktor genannt, gerade weil alle Institute zeitgleich regulatorische Veränderungen und Modernisierungen in der Zahlungsverkehrsinfrastruktur implementieren müssen. Weitere Aspekte sind die organisatorische Aufstellung und Verknüpfung wesentlicher betroffener Bereiche, die Umsetzung entsprechender Komitees und Eskalationspfade, die geregelte Interaktion mit externen Institutionen (wie z. B. den Auf-

4 PSD2 Meldungen sind Meldungen für schwerwiegende Betriebs- und Sicherheitsvorfälle bei Zahlungsdienstleistern. Vgl. dazu die PSD 2 Richtlinie der EU-Kommission bzw. § 54 Absatz 1 Satz 1 ZAG.

sichtsbehörden, Zentralbanken oder Betreibern der Marktinfrastruktur im Zahlungsverkehr) sowie die schriftlich fixierte Ordnung und das Prozessmanagement der ZV-relevanten Geschäftsprozesse. Relevante Fragen in diesem Zusammenhang sind beispielsweise:

- Wie sind wesentliche Produkt- und Prozessspezialisten im Zahlungsverkehr mit IT, Risikomanagement und Compliance vernetzt?
- Welche Qualifikationen werden benötigt, insbesondere um Legacy-Systeme weiter betreiben zu können?
- Zu welchem Detailgrad sind die Prozesse schon front-to-back dokumentiert und für das Risiko-Management verfügbar?

Unter Berücksichtigung der Risiko-Strategie und organisatorischen Zuständigkeiten müssen die Ziele und Anforderungen an operative Resilienz durch ein effektives Risiko-Management des Zahlungsverkehrs umgesetzt werden. Dafür bedarf es einer regelmäßigen Risikoanalyse der Prozesse im Tagesgeschäft mit Fokus auf Gefährdungs- und Bedrohungsszenarien, ein entsprechend implementiertes internes Kontrollsystem sowie gezieltes Partner-Management der externen Vendoren, BPO- oder FinTech-Partner. Weiterhin bedarf es eines funktionierenden und regelmäßig aktualisierten und getesteten Notfall-Managements im BCM-Plan sowie bereits eine Berücksichtigung von Resilienz-Aspekten im Neuprodukt-Prozess („Operational Resilience by Design"). Der letzte Aspekt ist gerade angesichts der großen Anzahl an Produktinnovationen im Zahlungsverkehr von Bedeutung. Wichtige Fragen des Risiko-Managements sind unter anderem:

- Sind die Risiken im end-to-end ZV-Prozess bekannt und werden diese regelmäßig eingeschätzt?
- Welche maximale Zeitspanne wird zur Behebung von Incidents bzw. zugrunde liegenden Issues toleriert?
- Wie wird Resilienz bereits von Anfang an im Design neuer Zahlungsverkehrsprodukte integriert?

Die Grundlage beziehungsweise die Enabler dieses Betriebsmodells sind eine stabile IT-Infrastruktur, tragfähige und moderne IT-Applikationen bzw. Workflows sowie validierte Datenmodelle und Datensicherheit, aber auch hinreichende Gebäudesicherheit, Management von Zugriffsberechtigungen und eine etablierte Risiko-Kultur in der Organisation. Im Rahmen dieser Bausteine sind vor allem folgende Fragen hilfreich:

- Wie wird operative Resilienz bereits durch die grundlegende IT-Architektur der Bank unterstützt?
- Wie stabil sind IT-Applikationen/Schnittstellen und wie gut sind sie gegenüber Cyber-Angriffen geschützt?
- Wie können neue Technologien (z.B. modulare IT-Architekturen, APIs zur einfachen Integration in Drittsysteme, oder Cloud-Infrastrukturen) sinnvoll und gleichzeitig sicher in den Zahlungsverkehr integriert werden?

D Ausblick: Was Banken jetzt tun können

Für Banken ergeben sich sowohl interne als auch externe Handlungsfelder, um die eigene Aufstellung zu verbessern.

Interne Handlungsfelder ergeben sich in folgenden Bereichen:

- Definition einer klaren Risiko-Strategie (inkl. Risiko-Appetit), um die Richtung des gesamten Risikomanagements im Zahlungsverkehr und damit auch der operativen Resilienz vorzugeben. Dies ist die Basis, um Maßnahmen zur Stärkung der operativen Resilienz inklusive des dafür erforderlichen Budgets auszuarbeiten.
- Festlegung eines adäquaten, bereichsübergreifendes Betriebsmodells inkl. bereichs- und funktionsübergreifender Zusammenarbeit. Dies muss alle Zahlungsverkehrsprodukte und alle relevanten IT-Systeme (inkl. Schnittstellen in das Kernbanksystem und relevante Umsysteme z.B. im Transaktionsmonitoring) umfassen. Bei international agierenden Instituten kommt hinzu, dass die operative Resilienz in allen Ländern gelebte Praxis sein sollte.
- Aufbau eines „regulatorischen Radars", durch das regulatorische Änderungen im Umfeld des Zahlungsverkehrs oder Änderungen in Marktstandards, die beispielsweise von Clearing- und Settlement Institutionen oder Kartennetzwerken vorgegeben sind, frühzeitig erkannt werden. Dadurch können Anforderungen an Produkte und technische Infrastruktur übersetzt und im Zuge von Change-Projekten effizient implementiert werden. Die Zahlungsverkehr-Infrastruktur hat dadurch jederzeit volle Compliance.
- Sicherstellung einer adäquaten und qualifizierten Personalausstattung inkl. einer klaren Strategie zur Rekrutierung, Schulung und Bindung von Humankapital und dem Aufbau relevanter Skills in der Organisation. Nur dadurch kann es Banken gelingen, die Durchführung von komplexen Change-Projekten im Zahlungsverkehr in time, quality und budget sicherzustellen.
- Verankerung des Risikomanagements bei Vendoren und Kooperationspartnern, v.a. da die Zusammenarbeit mit externen Software-Vendoren, BPO- oder FinTech-Partnern im ZV gängig ist. Insofern ist die Steuerung der Dienstleister besonders wichtig und wesentliche Sicherheitsstandards sollten von allen Partnern in der Wertschöpfungskette aufrechterhalten werden.

Externe Handlungsfelder bzw. Empfehlungen aus dieser Analyse ergeben sich in folgenden Bereichen:

- Austausch zur Gefährdungs- und Bedrohungslage zwischen den Banken, um sich bzgl. möglicher Risiken, Notfälle und Gefährdungsszenarien (im Hinblick auf Ursachen, beteiligte Parteien, eingesetzte „Hacker-Methoden") in der Branche abzustimmen. Dies kann nicht nur effizient sein, sondern auch den Blick auf die Gefährdungslage erweitern.
- Austausch mit deutschen Sicherheitsbehörden (wie z. B. dem Bundesnachrichtendienst oder dem Verfassungsschutz) zur Einschätzung aktueller Risiken und der Gefährdungslage, um auch (und soweit möglich) nachrichtendienstliche Erkenntnisse in die Analyse der Gefährdungslage einfließen zu lassen.
- Austausch mit anderen Branchen mit „Null-Fehler-Toleranz" oder kritischer Infrastruktur wie beispielsweise der Luftfahrtindustrie oder Energieversorgern bietet Chancen, von anderen zu Gefährdungsanalyse oder Präventionsmaßnahmen zu lernen und damit letztlich die eigene Resilienz-Strategie entsprechend zu stärken.
- Entwicklung von Branchenstandards zu operativer Resilienz im Zahlungsverkehr, um ein einheitlicheres Verständnis zu dem Begriff operative Resilienz zu schaffen und sich zu Branchenstandards bzw. „Best Practices" auszutauschen. Das würde den Instituten auch die Einschätzung erleichtern, wie sie im Marktvergleich aufgestellt sind.
- Entwicklung von Branchenlösungen für Notfallszenarien, z. B. um einen Ausfall in der ZV-Infrastruktur notfalls zu kompensieren, ggf. auch unter Einbeziehung branchenweiter Dienstleister (wie etwa SWIFT).

In jedem Fall wird das Thema operative Resilienz im Zahlungsverkehr in den nächsten Jahren weiter an Bedeutung gewinnen und ist daher für die Agenda des Bankenvorstands bzw. des Top-Managements hochrelevant. Für viele Institute bedarf es einer kritischen Überprüfung, wo sie heute stehen und wie sie das Risikomanagement im Zahlungsverkehr kontinuierlich und mit einem erhöhten Fokus auf die Stärkung der operativen Resilienz in einem herausfordernden Umfeld weiter verbessern können.

DIE AUTOREN:

Dr. Markus Ampenberger
Boston Consulting Group (BCG)

Prof. Dr. Tobias Berg
Goethe-Universität Frankfurt

Daniel Regending
Deutsche Bank