# Digital Operational Resilience

## Neue Impulse für das operative Risikomanagement

QA Financial (expleo) accourt PAYMENTS SPECIALISTS ReedSmith

# Inhaltsverzeichnis

# Einleitung

**Digital Operational Resilience (DOR) ist die Fähigkeit eines Unternehmens, sich schnell von spontanen Serverausfällen zu erholen und Unterbrechungen im Customer Service weitestgehend zu vermeiden. Möglich wird das, indem ein starkes Bewusstsein für potenzielle Schwachstellen aufgebaut wird. Darüber hinaus ist es nötig, eine proaktive Strategie zu implementieren, um Risiken zu reduzieren.**

Eine gefestigte Compliance-Kultur ist angesichts zunehmender Regularien seitens des Gesetzgebers Grundvoraussetzung für ein erfolgreiches Unternehmen. Allerdings reicht es nicht mehr aus, sich ausschließlich auf das operative Tagesgeschäft zu konzentrieren. Um nicht ins Hintertreffen zu geraten, müssen bereits im Vorfeld Vorkehrungen getroffen werden. Dazu gehört es, die digitalen Prozesse auf zukünftige Anforderungen und betriebliche Veränderungen hin zu optimieren.

## Aufbau einer Compliance-Kultur

Der Digital Operational Resilience Act (DORA) wird voraussichtlich 2024 innerhalb der EU in Kraft treten. Weitere internationale Vorschriften und Regularien werden vermutlich folgen. Unternehmen, die diese harten Bestimmungen nicht ernst nehmen, indem sie rechtzeitig ihre DOR-Strategien überarbeiten, drohen empfindliche Bußgelder.

Der vorliegende Bericht wurde gemeinsam mit QA Financial in Auftrag gegeben und in Zusammenarbeit mit unseren bewährten Partnern Reed Smith LLP und Accourt Payment Specialists entwickelt. Er umfasst tiefgehende Erkenntnisse aus Marktanalysen und persönlichen Interviews, die das Konzept der DOR als grundlegenden Geschäftsfaktor untermauern. Der Bericht befasst sich mit dem aktuellen Stand und dem Verständnis von DOR in Unternehmen und den zukünftigen Auswirkungen von DORA auf den Banken-, Finanzdienstleistungs- und Versicherungssektor in der EU und in Großbritannien.

## Die wichtigsten Erkenntnisse:

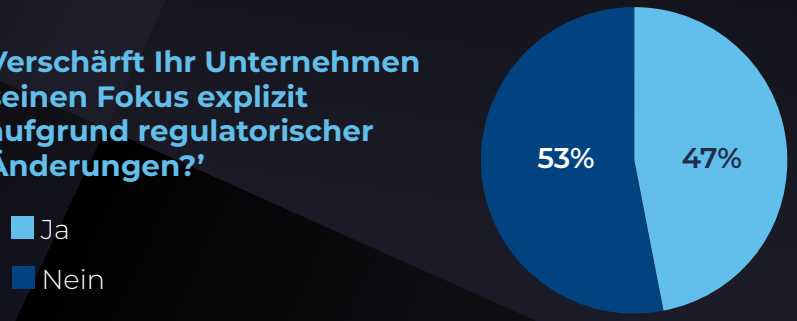
**20%** aller befragten Unternehmen nehmen Software-Qualität als Risikofaktor wahr

**20%** kennen den Digital Operational Resilience Act (DORA)

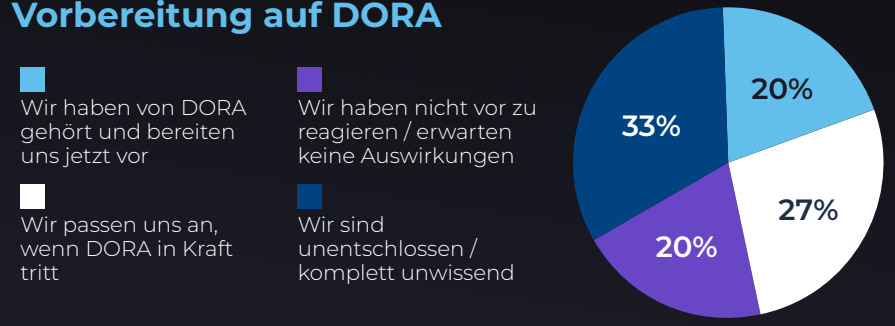
**25%** wissen um die Bedeutung von Digital Operational Resilience

**1%** Der Digital Operational Resilience Act wird vermutlich Geldstrafen in Höhe von 1% des durchschnittlichen Tagesumsatzes als Folge von Softwareproblemen nach sich ziehen

**Verschärft Ihr Unternehmen seinen Fokus explizit aufgrund regulatorischer Änderungen?'**




**Vorbereitung auf DORA**




**50%** fokussieren sich verstärkt auf Digital Resilience, angetrieben durch die geschäftliche Nachfrage nach permanenten Zugriffsmöglichkeiten auf Systeme und Lösungen sowie aufgrund zunehmender Regulierungsvorschriften

**100%** der Unternehmen mit technologisch versierten Vorstandsmitgliedern konzentrieren sich verstärkt auf das Thema DOR

**Banken haben klare Verantwortlichkeiten im Zusammenhang mit DOR definiert**

**Der Wandel von unternehmensbezogenen Bedürfnissen bis hin zur 24-Stunden-Erreichbarkeit für Mitarbeiter und Kunden ist das Hauptanliegen im Zusammenhang mit DOR**

# Methodik

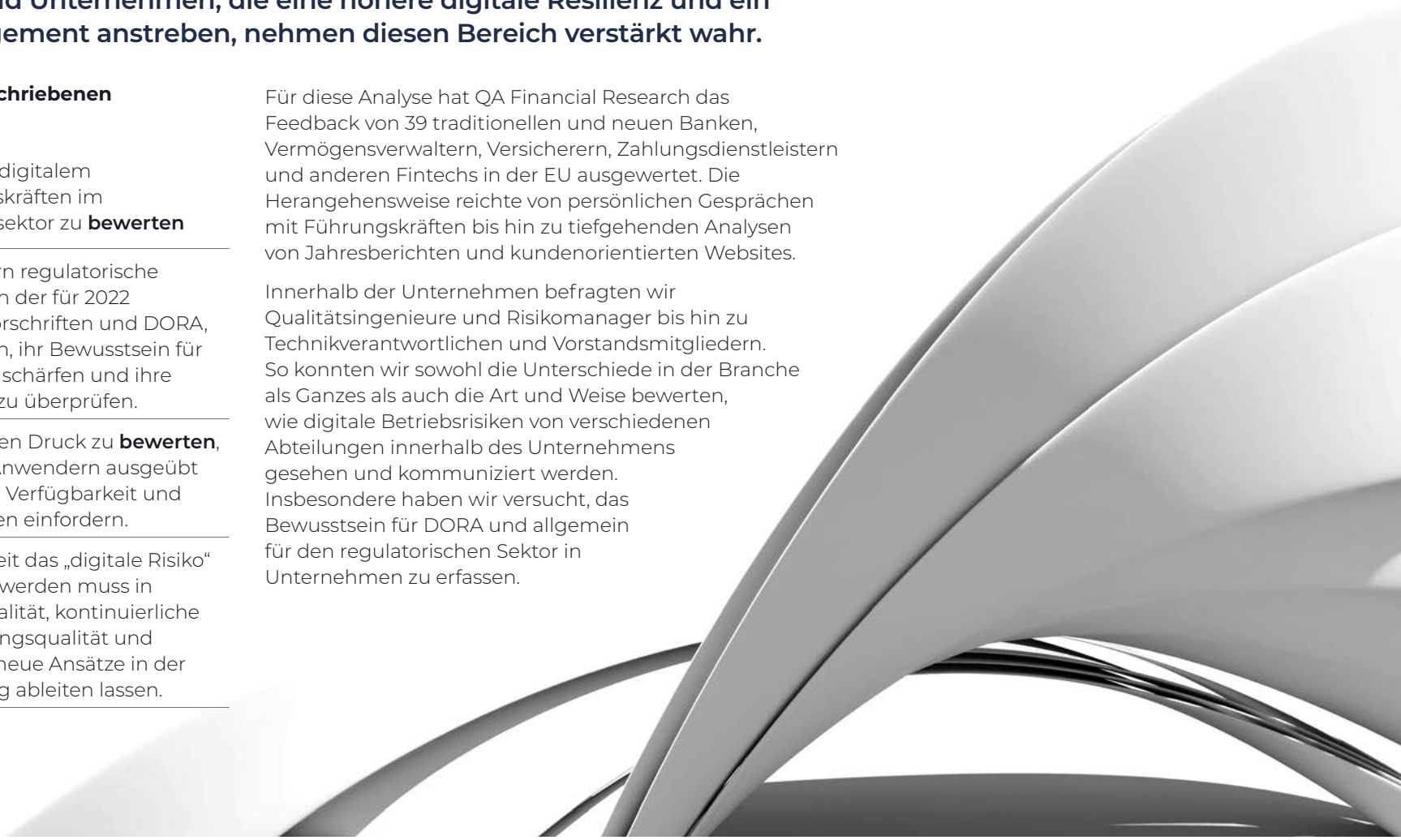
## Das digitale betriebliche Risiko ist ein Teilbereich des allgemeinen betrieblichen Risikos. Regulierungsbehörden und Unternehmen, die eine höhere digitale Resilienz und ein verbessertes Risikomanagement anstreben, nehmen diesen Bereich verstärkt wahr.

**Das Ziel der in diesem Papier beschriebenen Untersuchung besteht darin:**

- Das Bewusstsein von „digitalem Risiko“ unter Führungskräften im Finanzdienstleistungssektor zu **bewerten**
- **Festzustellen**, inwiefern regulatorische Faktoren, einschließlich der für 2022 beschlossenen FCA-Vorschriften und DORA, Unternehmen zwingen, ihr Bewusstsein für das „digitale Risiko“ zu schärfen und ihre Governance-Prozesse zu überprüfen.
- Den unternehmerischen Druck zu **bewerten**, der von Kunden und Anwendern ausgeübt wird, die eine ständige Verfügbarkeit und Aktualität von Systemen einfordern.
- Zu **evaluieren**, inwieweit das „digitale Risiko“ stärker berücksichtigt werden muss in Bezug auf Softwarequalität, kontinuierliche Testverfahren, Kodierungsqualität und inwieweit sich daraus neue Ansätze in der Unternehmensführung ableiten lassen.

Für diese Analyse hat QA Financial Research das Feedback von 39 traditionellen und neuen Banken, Vermögensverwaltern, Versicherern, Zahlungsdienstleistern und anderen Fintechs in der EU ausgewertet. Die Herangehensweise reichte von persönlichen Gesprächen mit Führungskräften bis hin zu tiefgehenden Analysen von Jahresberichten und kundenorientierten Websites.

Innerhalb der Unternehmen befragten wir Qualitätsingenieure und Risikomanager bis hin zu Technikverantwortlichen und Vorstandsmitgliedern. So konnten wir sowohl die Unterschiede in der Branche als Ganzes als auch die Art und Weise bewerten, wie digitale Betriebsrisiken von verschiedenen Abteilungen innerhalb des Unternehmens gesehen und kommuniziert werden. Insbesondere haben wir versucht, das Bewusstsein für DORA und allgemein für den regulatorischen Sektor in Unternehmen zu erfassen.



# Analysierte Finanzunternehmen

**Unsere Untersuchung umfasste die Analyse von Geschäftsberichten, Websites und etwa 20 persönlicher Gespräche mit Führungskräften der unten aufgeführten Unternehmen. Dieser Bericht vertritt nicht direkte Kommentare oder Beobachtungen der besagten Unternehmen.**

- Admiral Group
- Adyen
- Aegon
- Allianz
- Arbuthnot Latham
- Atom Bank
- Axa
- Bank of England
- Barclays
- BNP Paribas
- Close Brothers
- Curve
- De Silva
- Deutsche Bank
- Hiscox
- HSBC
- ISP
- Klarna
- Legal & General
- Lloyds
- London Stock Exchange
- M&G
- Metrobank
- Miller Insurance
- Monese
- Monzo
- Nationwide
- NORDEA
- Osper
- Planet Payments
- Quilter
- RBS
- Revolut
- Schroders
- Skrill
- Standard Chartered
- Starling Bank
- Stripe
- Transferwise

# Die fünf Säulen der Digital Operational Resilience

**Obwohl es nicht einfach ist, sich auf eine Gesetzesnovelle vorzubereiten, die noch sehr abstrakt wirkt und deren einschränkende Auswirkungen noch nicht vollständig definiert sind, ist zum jetzigen Zeitpunkt genug über die bevorstehende DORA-Verordnung bekannt, um die Grundlagen für eine präventive Compliance-Strategie zu schaffen. Fest steht, dass DORA einen noch nie dagewesenen Rahmen für die Überwachung der Cybersicherheit für Anbieter von Technologiedienstleistungen darstellen wird. Ein besonderer Schwerpunkt liegt auf Cloud Computing und „systemrelevanten" Betriebsfunktionen.**

Das ist eine gewaltige Aufgabe, dennoch ist DORA nur eine von vielen Stationen auf dem Weg zur Umsetzung von umfassender Digital Operational Resilience. Expleo hat sich verpflichtet, Unternehmen auf diesem neuen Weg beratend zur Seite zu stehen.

„Wir verstehen DORA als einen weiteren wichtigen Baustein der Risikomanagementarchitektur von Finanzinstituten. Deshalb haben wir einen Fünf-Stufen-Plan entwickelt, um Unternehmen in diesem neuen Terrain zu begleiten und sie bei ihren Compliance-Strategien zu unterstützen."

Olaf Bartelt, Head of Market Business Unit Banking & Financial Services, Expleo Technology Germany

## 01

### Bewusstsein für DOR schaffen

Bei jeder neuen Gesetzgebung gibt es eine notwendige Findungsphase, in der die Richtung der Compliance-Strategien definiert wird. Als ersten Schritt sollten Sie den Umfang der erforderlichen Arbeiten ermitteln, die entsprechenden Ressourcen zuweisen und die Chancen erkennen, die sich aus einer erweiterten DOR ergeben. Diese Aufklärungsarbeit ist die Grundlage für die richtige Vorgehensweise und für das Verständnis möglicher regulatorischer Folgen, die sich auf den aktuellen Modus Operandi des eigenen Unternehmens beziehen.

„Echte Resilienz muss bei der Unternehmensstrategie beginnen und sich durch die gesamte Organisation ziehen."

Rachel Saunders, Client Director bei Moorhouse (einem Unternehmen der Expleo Group)

## 02
## Schulung und Coaching

Es ist wichtig, dass Mitarbeiter mit den Auswirkungen von DORA auf ihr Unternehmen vertraut sind. Wir haben ein Programm ausgearbeitet, das die Mitarbeiter im Change Management begleitet. Dadurch können sich Mitarbeiter auf die neuen Prozesse einstellen, um eine neue Compliance-Strategie zu untermauern. Mitarbeiter müssen mit den neuen Standards für die Klassifizierung von Vorfällen, der neuen Terminologie und den Akronymen im Zusammenhang mit den neuen Rechtsvorschriften vertraut sein. Für die Mitarbeiter, die für die Prüfung und Überwachung verantwortlich sind, ist eine maßgeschneiderte Schulung erforderlich, ebenso wie eine AML-Schulung (Geldwäschebekämpfung) inklusive entsprechendem Coaching. Zusätzlich sind Kontrollen unabdingbar, um die Wirksamkeit der Überwachung zu messen. Mitarbeiter sind die Augen und Ohren des Unternehmens im Bereich der Resilienz und sollten umfassend geschult werden, um Systemschwächen zu erkennen, die die allgemeine betriebliche Widerstandsfähigkeit gefährden könnten.

## 03
## Überprüfung von Drittanbietern

Viele Finanzinstitute greifen auf die Dienste von Drittanbietern zurück, um die Kundenbetreuung zu unterstützen und ihr gesamtes Serviceangebot zu verbessern. Die Nutzung eines Netzwerks von Dienstleistern kann zwar durchaus Vorteile bringen, schränkt aber auch die Möglichkeiten eines Instituts ein, sein operatives Schicksal selbst zu kontrollieren. Deshalb ist es wichtig, ein Verzeichnis aller Drittanbieter zu erstellen. Wenn bedeutende Bereiche der Customer Journey ausgelagert werden, muss man wissen, wie zuverlässig diese funktionieren. Es ist ratsam, die Folgen einschätzen zu können, die solch eine Abhängigkeit von Outsourcing bringt. Wie schnell kann zum Beispiel Ersatz gefunden werden? Was würde passieren, wenn es eine Gefährdung durch die outgesourcte Stelle gäbe oder gar ein Ausfall droht? Die ordnungsgemäße Bewertung der Zuverlässigkeit dieser Anbieter und die Ermittlung etwaiger Schwachstellen ist Pflicht, wenn es um die Umsetzung einer soliden DOR-Strategie geht. Schließlich benötigen Sie Drittanbieter, die über den technischen Sachverstand, das Ansehen in der Branche und das Repertoire an Werkzeugen verfügen, um eine schnelle und vorschriftenkonforme DOR zu ermöglichen.

## 04
## Strenge Prüfverfahren

Es müssen ungeschönte Bewertungen der internen Teststrukturen und -prozesse durchgeführt werden. Einige Anforderungen von DORA werden technische Tests erfordern, so dass Sie die Auswirkungen auf Ihre Systeme und Mitarbeiter genau abschätzen können. Wie lässt sich das bewerkstelligen, und wer wird es tun? Wie regelmäßig werden die Tests durchgeführt und wie werden Ergebnisse geliefert? Und schließlich - und das ist entscheidend - welche Maßnahmen werden aufgrund der Ergebnisse ergriffen? Dies sind nur einige der wichtigsten Fragen, über die man nachdenken sollte. Die Sicherheit und Integrität der Systemarchitektur ist von grundlegender Bedeutung für die Einhaltung der Vorschriften. Systemausfälle sind ein schwarzer Fleck in der Bilanz einer Plattform. Sie untergräbt die Glaubwürdigkeit bei Kunden. In Anbetracht des hohen Einsatzes lohnt es sich, Zeit und Sorgfalt in die Entwicklung solider Testverfahren zu investieren.

## 05
## Mechanismen zur Berichterstattung

Wurde ein konsequentes Test- und Prüfverfahren installiert, ist die Einrichtung einer erstklassigen Dokumentation und eines Reportings der nächste Schritt, der für die Einhaltung der Vorschriften folgen muss. Die Entwicklung und Implementierung neuer Standards für das Reporting erfordert eine fachkundige Anleitung. Zudem können unsere umfassenden technischen Berichts- und Prüfdienste wertvolle Dienste bei den kommenden Herausforderungen leisten. Unternehmen werden sich an eine vollkommen neue Form des Reportings gewöhnen müssen. Die Kommunikation in Bezug auf etwaige Zwischenfälle müssen gestrafft, entsprechende Prozesse besser etabliert werden. Expleo hilft Ihnen bei der Ausarbeitung eines klaren Plans für das interne Reporting, bevor dieser Report an die Aufsichtsbehörde weitergeleitet wird. Sobald eine kontinuierliche Reporting-Struktur etabliert ist, wird es für Unternehmen einfacher, die Reporting-Anforderungen mit geringem Aufwand zu erfüllen.

# Branchenanalyse von Reed Smith LLP

**Reed Smith LLP ist eine führende weltweit tätige Anwaltskanzlei. Sie ist für 48 der 50 global agierenden Banken tätig und unterstützt DOR-Rechts- und Compliance-Strategien mit erstklassiger Beratung.**

**Howard Womersley Smith**
Partner, Reed Smith LLP

## 1. Welche Erkenntnisse können Sie aus Ihrer früheren Tätigkeit bei der Standard Chartered Bank über die Umsetzung von Vorschriften der Regulierungsbehörden innerhalb einer Bank mitnehmen?

Die wichtigste Erkenntnis, die ich aus meiner Arbeit in der Bank gewonnen habe, ist die, dass alle Projekte ein erhebliches Maß an abteilungsübergreifender Zusammenarbeit und Interaktion erfordern. Das gilt besonders für die, die durch Regulierungsbehörden ausgelöst werden. Erst wenn alle betroffenen Abteilungen involviert sind, lässt sich ein durchgängiger Prozess von der Durchführbarkeit über die Due-Diligence-Prüfung bis hin zur Implementierung im Unternehmen implementieren. Eine der Bestandteile in diesem Prozess sind Fragen hinsichtlich Recht und Compliance, die in meinen Aufgabenbereich fallen. Um die Einhaltung der Vorschriften zu erreichen, ist es wichtig, die Auswirkungen aus interner Sicht, aus Sicht von Kunden und aus der von Drittanbietern zu verstehen. Dies erfordert oft eine Änderung der Art und Weise, wie ein Unternehmen, das unter Aufsicht einer Behörde steht, sein Tagesgeschäft führt und wie sich die Mitarbeiter innerhalb des Unternehmens verhalten. Auch kann es erforderlich sein, die vertraglichen Beziehungen zwischen einem Unternehmen und seinen Kunden oder Lieferanten sowie die Geschäftsbeziehungen zu weiteren Geschäftspartnern zu überprüfen und zu optimieren.

Zuweilen können sogar viele Punkte eine Rolle spielen und ineinander greifen, da manchmal auch die Kommunikation solcher Unternehmen angepasst werden muss. Ein Beispiel aus der Praxis: Die Regulierungsbehörde hat in einem Fall verlangt, dass Verbrauchern bei der Vergabe eines Kredits bestimmte Informationen zur Verfügung gestellt werden müssen.

## **2.** Wie können Finanzinstitute sicherstellen, dass sie ihre Dienstleistungen auch angesichts von Bedrohungen von außen dauerhaft erbringen können?

Das ist die entscheidende Frage, vor allem im Zusammenhang mit dem relativ neuen Thema betriebliche Resilienz, die beschreibt, wie eine Organisation die Geschäfte aufrechterhalten kann, wenn sie von einem Ereignis schlagartig betroffen ist. Solche Ereignisse, ausgelöst zum Beispiel durch Hackerangriffe, können den Betrieb eines Unternehmens destabilisieren. Durch die Umsetzung bestimmter Vorbereitungen kann man jedoch sicherstellen, dass der Geschäftsbetrieb weitgehend unbeeinträchtigt bleibt. So ist es möglich, auf abrupte Ereignisse zu reagieren und ihre Auswirkungen zu verringern. Diese Vorbereitungen sind der Schlüssel zur Aufrechterhaltung der Leistungsfähigkeit bei externen Bedrohungen, die ein Unternehmen lahmlegen können. Der Schlüssel zu einer soliden Vorbereitungsstrategie ist die Berücksichtigung der Kundenperspektive.

Eine wichtige Frage, die sich regulierte Unternehmen im Zusammenhang mit der betrieblichen Resilienz stellen müssen, lautet: Wie kann sich eine externe Bedrohung auf meine Kunden oder Klienten auswirken? Befassen wir uns mit den gängigen externen Bedrohungen, geht es bei den von den Finanzaufsichtsbehörden genannten Herausforderungen in der Regel um Cyberangriffe und damit um Cyberrisiken. Cyberangriffe zielen auf Technologiesysteme und die darin gespeicherten Daten ab. Technologie ist jedoch etwas, auf das alle regulierten Unternehmen angewiesen sind. Insbesondere Banken sind in hohem Maße von ihnen abhängig, um ihre Dienstleistungen für Verbraucher zu erbringen, sei es durch Online-Banking, Geldautomaten oder Back-Office-Verarbeitung. Werden die mit dieser Technologie erzeugten Kundendaten in einer Cloud-Umgebung gespeichert, wird das Risiko externer Bedrohungen allgegenwärtig.

Die Vorschriften für die betriebliche Widerstandsfähigkeit stellen regulierte Unternehmen vor die Herausforderung, einen Weg zu finden, den Geschäftsbetrieb auch dann aufrechtzuerhalten, wenn ihre Technologie und/oder ihr Betrieb angegriffen oder anderweitig gestört wurde. Dies kann nur durch eine sorgfältige Definition der wichtigen Geschäftsdienstleistungen erreicht werden sowie durch eine Zuordnung der Systeme und Prozesse, die zu deren Unterstützung verwendet werden. Das aber schließt unweigerlich auch Drittanbieter oder ausgelagerte Dienstleister ein. Berücksichtigt werden muss auch, wie hoch die Toleranzgrenze (Auswirkungstoleranz) gegenüber eventuellen Störungen gesetzt wird, bevor das Dienstleistungsangebot für Kunden beeinträchtigt wird.

Zur Bewertung dieser Auswirkungstoleranz werden Testszenarien empfohlen, und es müssen Anpassungen vorgenommen werden, um diese Toleranz zu erhöhen, wenn sie sich als zu gering erweist.

Die britischen Finanzaufsichtsbehörden z.B. sind sich darüber im Klaren, dass es nicht möglich ist, jeden Bestandteil der Geschäftstätigkeit eines beaufsichtigten Unternehmens vollständig gegen Betriebsstörungen zu schützen. Es wäre auch kein effizienter Einsatz von Ressourcen mehr möglich. Sie erkennen an, dass Unternehmen ihren wichtigsten Geschäftsdienstleistungen Vorrang einräumen müssen.

Das wichtige Unterscheidungsmerkmal der betrieblichen Resilienz gegenüber dem betrieblichen Risiko ist zum Beispiel die Anforderung, sich darauf zu konzentrieren, wie der Kundenstamm eines beaufsichtigten Unternehmens weiterhin bedient werden kann. Die Beherrschung des Risikos, das beispielsweise in der Qualität der verwendeten IT-Systeme oder der darin verwendeten Sicherheitsmechanismen liegen kann, ist eine Schlüsselkomponente, um dieses Ergebnis erreichen zu können.

Dieser ergebnisorientierte Ansatz verlangt von Unternehmen, dass sie ihre Risikobewertung beim Kunden beginnen und sich von dort aus in die Backend-Infrastruktur des Unternehmens vorarbeiten, indem sie ihre Systeme und Prozesse auf diesem Weg untersuchen.

## 3. Wie sehen Sie persönlich die wachsende Bedeutung von Digital Operational Resilience auf Vorstandsebene?

Operational Resilience wird von den Finanzaufsichtsbehörden als ebenso wichtig angesehen wie finanzielle Resilienz. Diese Einschätzung unterstreicht die Bedeutung von OpRes, die als Ergebnis der Finanzkrise von 2008 entstanden ist. Wenn das nicht die Aufmerksamkeit der Vorstandsetagen erregt, was dann? Außerdem wird DORA weitreichende Auswirkungen auf Finanzdienstleistungsunternehmen haben, da es sich mit allgegenwärtigen Problemen wie Cyberrisiken befasst, die naturgemäß das gesamte Geschäft eines regulierten Unternehmens betreffen werden. DORA verdient daher die besondere Aufmerksamkeit auf Vorstandsebene.

## 4. Können Sie vorhersagen, wie Institute den künftigen Fahrplan für die digitale betriebliche Resilienz bewältigen werden?

Sie werden den Weg, der vor ihnen liegt, nur schwer bewältigen. Offen gesagt haben sie noch nicht die richtige Einstellung gefunden. Regulierte Unternehmen, die in den Geltungsbereich des Digital Operational Resilience Act (DORA) in Europa und der entsprechenden Vorschriften in Großbritannien fallen, kämpfen noch immer mit den Regeln für Outsourcing und dem Risiko Dritter wie den EBA-Leitlinien für Outsourcing. Viele von ihnen haben noch nicht den Grad an Konformität erreicht, der bis zum Ende 2021 war.

Werden diese Organisationen mit zusätzlichen Vorschriften konfrontiert, die noch ausgefeilter und durchdringender sind und einen tieferen Blick unter die Motorhaube erfordern, um ein bestimmtes Ergebnis zu erzielen (was wiederum eine Änderung der Compliance-Mentalität erfordern kann), wird dies eine sehr steile Lernkurve nach sich ziehen.

Die britische PRA ist sich dessen bewusst und kündigte in einer Rede Anfang des Jahres an, dass sie nicht damit rechnet, dass Unternehmen bis zum Ende der Frist im März 2022 alle erforderlichen Maßnahmen getroffen haben werden. Sie geht jedoch davon aus, dass betroffene Unternehmen bis dahin eine überzeugende Bestandsanalyse durchgeführt haben, um feststellen zu können, wo die größten Schwachstellen liegen und in welchen Bereichen mehr Engagement erforderlich ist.

# Bewusstsein für digitale und technologische Risiken

**Auf die Frage nach dem Verständnis für digitale und technologische Risiken wird Digital Operational Resilience (DOR) von etwas mehr als der Hälfte der Befragten ausdrücklich als Risikokategorie anerkannt.**

**#1**

In der Kategorie „digitales Risiko" steht das Thema (Daten-) Sicherheit an erster Stelle bei den befragten Unternehmen.

Etwas mehr als die Hälfte aller Unternehmen räumte ein, dass es sich um ein Datenmanagement-Risiko handelt.

**>50%**

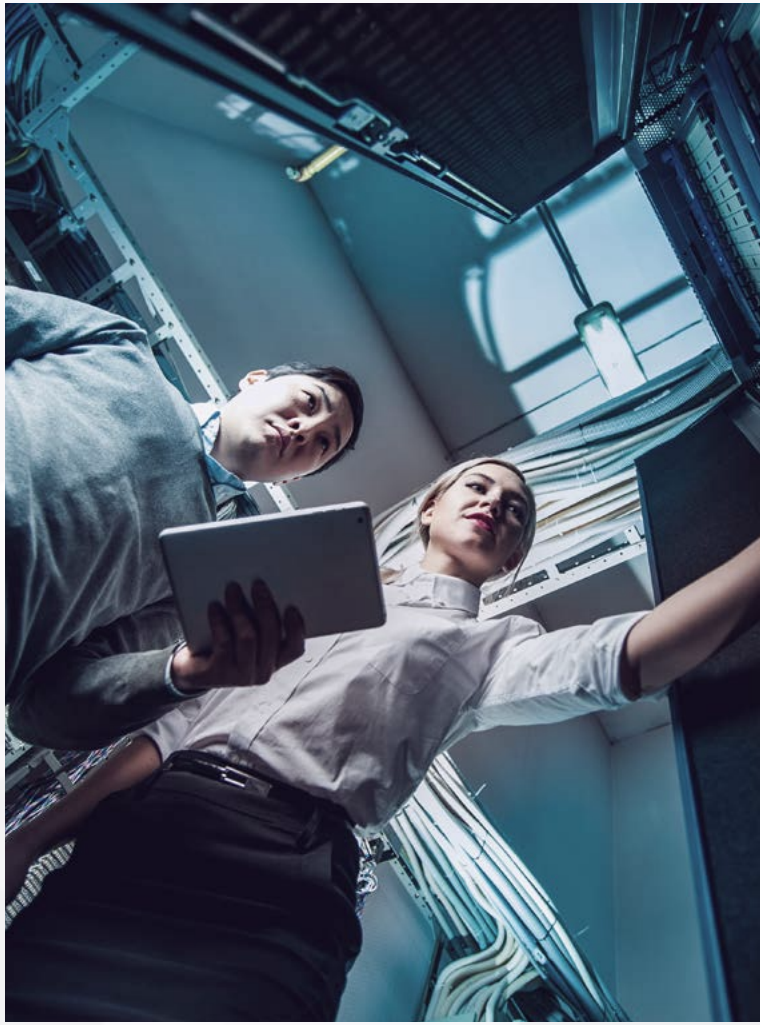
**Von nur**

**20%**

**aller Unternehmen wurde die Softwarequalität als Risikobereich wahrgenommen.**

**Selbst unter den Unternehmen, die DOR ausdrücklich als wichtig einstuften, betrug der Anteil nur**

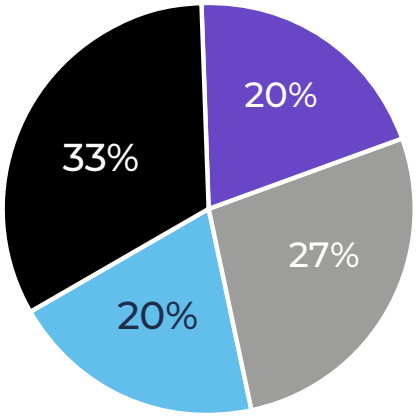
**25%**



**47% der Unternehmen verschärfen Ihren Fokus aufgrund der regulatorischen Änderungen.**

## Der Digital Operational Resilience Act (DORA) stand kaum auf der Tagesordnung – für nur 20% der Unternehmen spielte die geplante Gesetzgebung eine Rolle

### Reaktionen auf DORA




- Wir haben von DORA gehört und bereiten uns jetzt vor
- Wir planen keine Reaktion / erwarten keine Auswirkungen
- Wir passen uns an, wenn DORA in Kraft tritt
- Wir sind unentschlossen / komplett unwissend

## „Ich bin diesbezüglich nicht auf dem neuesten Stand, dabei kenne ich jede Menge Vorschriften."

**Zitat eines Vertreters einer Versicherung**

Während DORA nicht im Bewusstsein von Banken und Assekuranzen verankert ist, konstatieren sie dennoch eine Zunahme der Vorschriften und Regularien. Die dafür verantwortlichen Behörden Financial Service Authority (FCA) und Prudential Regulation Authority (PRA) fokussieren sich aktuell auf die Cybersicherheit und die betriebliche Resilienz als Ganzes, wobei Banken auf die für 2022 erwarteten Änderungen in diesem Bereich hinweisen. In 50% der Unternehmen gerät nach Aussagen der Befragten die betriebliche digitale Resilienz verstärkt in den Fokus.

Grund ist die Zunahme der zeitlichen Verfügbarkeit von Systemen (24/7) sowie zunehmende Auflagen von Aufsichtsbehörden.

## Eine Bank richtete eigens eine Abteilung zur Kontinuität und Sicherheit ein, um die Verfügbarkeit von Systemen sicherzustellen und eine schnelle Reaktion bei Ausfällen zu gewährleisten.

Dies gilt insbesondere in Zeiten gesteigerter Fernzugriffe.

## Verantwortlichkeiten

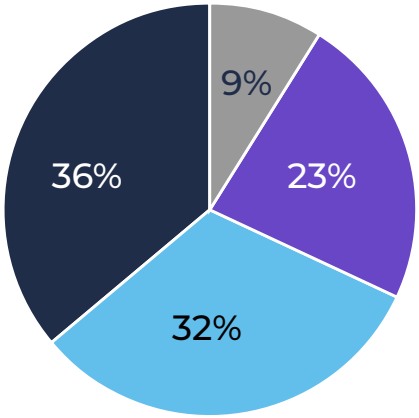
Die Verantwortlichkeiten variieren zwischen verschiedenen Sektoren hinweg und innerhalb einzelner Sektoren.

Unternehmen, die über **Vorstandsmitglieder aus dem Bereich Technologie** verfügen, legen mehr Wert auf die digitale betriebliche Widerstandsfähigkeit durch verbesserte Systeme und Prozesse und definieren einen klaren und direkten Weg über Rechenschaftspflichten gegenüber dem Vorstand. Außerdem haben diese Unternehmen oft mehrere Wege der Rechenschaftspflicht installiert, normalerweise parallel zum CTO und CRO oder dem Risikoausschuss.

Bei **Banken** waren die Wege der Rechenschaftspflicht oft besonders klar definiert, da sie in den vergangenen Jahren bereits Änderungen vorgenommen haben, etwa durch die Erstellung neuer Richtlinien oder die Abtrennung von Positionen wie CISO von der Technologieabteilung.

Nur bei einem **Fintech-Unternehmen** und einem einzigen Vermögensverwalter beschränkte sich die Rechenschaftspflicht noch auf die lokale oder die Abteilungsebene. Dies wird sich bei den Vermögensverwaltern wahrscheinlich ändern, weil sie festgestellt haben, dass Audits in den letzten fünf Jahren stark angestiegen sind und der Wandel im Unternehmen weiter voranschreitet.

**Anteil der Unternehmen, deren Rechenschaftspflichts-Wege bis zum Vorstand oder CRO reichen**




- Beteiligung der technologischen Basis
- Weg bis zum Vorstand
- Fokus auf opRes
- Unentschlossen/ komplett unwissend

## Auswirkungen auf die Personalbeschaffung

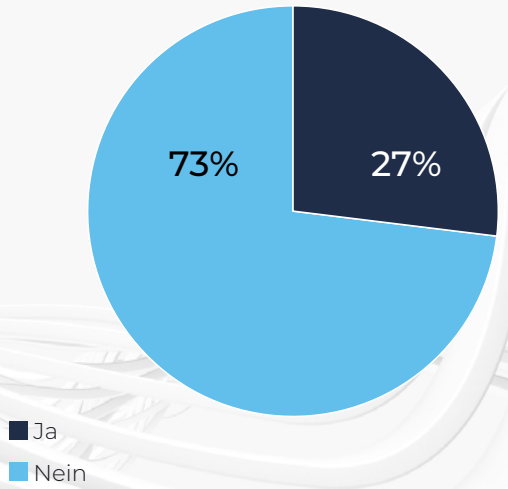
Nahezu alle anderen befragten Unternehmen haben die Verantwortung entweder einem Vorstandsmitglied oder dem Vorstand übertragen, mitunter auch dem CEO. Ein Versicherer hat sogar eine externe Organisation, die die Rechenschaftspflicht der Anbieter überwacht. Ein anderes Unternehmen lässt sich von externen Experten beraten, um CRO und COO in Bezug auf die Rechenschaftspflicht zu kontrollieren. Die Entwicklung der Standortzuverlässigkeit steht nur selten im Vordergrund. Während Unternehmen, die sich in Richtung DevOps bewegen, Automatisierung und CI/CD erwähnen, gehört die Skalierbarkeit von Systemen nicht zu den Schwerpunkten. Der zusätzliche Fokus auf die digitale Ausfallsicherheit hat Auswirkungen auf die Rollenverteilung. CSOs, CISOs und Sicherheitsarchitekten spielen die Hauptrolle, wenn es darum geht, Änderungen zu veranlassen. Kein Wunder, der Schwerpunkt liegt schließlich auf den Bereichen Sicherheitsrisiken und Regulierung.

**Die Größe der Testteams hat sich generell erhöht, in den letzten fünf Jahren manchmal sogar verdreifacht.**

Eine generelle Auswirkung auf CI/CD und Sicherheitsintegration wurde von den anderen Unternehmen nicht wahrgenommen.

Am stärksten betroffen sind die Bereiche Datenmanagement und Zuverlässigkeitstests. Ein Versicherer erklärte, dass dieser Umstand auf die Erfüllung der vom strategischen Informationssicherheitsbeauftragten geforderten Maßnahmen zurückzuführen ist. Bei Fintechs gab es kaum Auswirkungen auf das Release-Management oder das Datenmanagement, während die Sicherheitsaspekte allerdings den Bedarf an zuverlässiger Programmierung erhöhten.

**Prozentsatz der Unternehmen, die von direkten Auswirkungen auf die Einstellungspraktiken auf Vorstandsebene berichten**



## Erfolgsmodelle

Es gibt zwei primäre Motivationen für Veränderungen im Bereich der betrieblichen Ausfallsicherheit. Die eine speist sich aus der Entwicklung des regulatorischen Umfelds.

> **Einige Experten gehen davon aus, dass über DORA versucht werden wird, Geldstrafen in Höhe von 1% des durchschnittlichen Tagesumsatzes als Folge von Softwareproblemen der Anbieter zu verhängen.**

Selbst für Unternehmen außerhalb der EU ist DORA ein Faktor – ein leitender Angestellter einer britischen Aufsichtsbehörde wies auf die Verpflichtung hin, sicherstellen zu müssen, dass britische Vorschriften und Standards ausreichend berücksichtigt werden, damit Unternehmen über EU-Grenzen hinweg tätig sein können. In Großbritannien und weiteren Nicht-EU-Ländern bilden digitale Faktoren und Prozesse einen wachsenden Teil des regulatorischen Rahmens.

Zweitens führt die Notwendigkeit einer 24-stündigen Erreichbarkeit von Systemen für Mitarbeiter und Kunden zu einem Bedarf an hoher Verfügbarkeit und größerer Ausfallsicherheit. Mehrere Unternehmen gaben an, dass dieser Umstand Hauptgrund für digitale Resilienz sei.

## Sollten Sie sich vorbereiten?

Während nur 20% der Unternehmen, die von DORA gehört haben, bereits im Vorfeld Maßnahmen ergreifen wollen, will sich knapp die Hälfte erst darauf einstellen, wenn DORA wirklich aktiv diskutiert wird. Fintechs waren hier vergleichsweise unwissend. Sie gaben zu Protokoll, erst auf Anforderungen reagieren zu wollen, sobald sie in Kraft treten. Auch einige Banken und Versicherer schlossen sich dieser Sichtweise an. Doch mit dieser Strategie riskieren Unternehmen einen Schockmoment und eine Fehlverteilung von Ressourcen, wenn in den letzten Monaten vor DORA alle Anforderungen umgesetzt müssen.

Einige Unternehmen bereiten sich bereits auf die Änderungen der FCA-Richtlinien für das Management und den Rechenschaftsbericht über die operative Resilienz im März 2022 vor, wobei eine Bank bereits Kontrollinstanzen für das operative Risiko etablieren will.

## Wie kann bereits jetzt eine Anpassung an DORA erfolgen?

Auch wenn der Gesetzestext noch nicht gänzlich vorliegt, können einige Aspekte bereits berücksichtigt werden. Anbieter sollten Softwarequalitätsstandards strikt einhalten, anstatt sich selbst zu zertifizieren.

## Bewährte Verfahren für die Risikoberichterstattung

Aus den Interviews geht eindeutig hervor, dass Unternehmen, die technologieorientierte Vorstände einstellen, über bessere Systeme für Reportings und Rechenschaftspflichten verfügen. Hier existieren eine oder mehrere klar geregelte Kommunikationsketten bis hinauf zur Vorstandsebene.

In den Gesprächen wurde klar, dass sich einige Qualitätsmanager derzeit nicht der regulatorischen Anforderungen bewusst sind und lediglich stückweise auf Anforderungen reagieren, die an sie weitergegeben werden. Durch bessere Kommunikationswege und die Rechenschaftspflicht werden diese Mitglieder künftig besser informiert sein und den Anforderungen eine größere Bedeutung beimessen. Es könnte notwendig werden, Anbietern zusätzliche Zeit oder Budgets einzuräumen, um sicherzustellen, dass sie zertifizieren und verbesserte Tests und Messverfahren bereitstellen.

Durch die Verbesserung von Reportings vereinfacht sich die Kontrolle, so dass Unternehmen eine Ursachenanalyse durchführen können. Ein gut vorbereiteter Versicherer verlangt von Anbietern, dass sie ihre Haftungsrichtlinien innerhalb von zehn Tagen protokollieren. Mehrere Banken berichteten, dass verbesserte Teststrategien eine größere Transparenz und Verantwortlichkeit im gesamten Unternehmen ermöglichen.

> **Ein Fintech-Unternehmen meldete die Einführung eines neuen Teams für den CRO, das sich auf die operative Widerstandsfähigkeit konzentriert.**

Zwei Unternehmen wollten einen externen Berater zur Risikobewertung hinzuziehen, der direkt an den CRO oder den Vorstand berichtet.

## Fazit

Die meisten Unternehmen sind auf dem Rückzug, wenn es darum geht, auf bevorstehende regulatorische Anforderungen zu reagieren. Dazu gehört DORA. In der Realität erkennt nur etwas mehr als die Hälfte die Bedeutung eines erweiterten und vertieften Ansatzes für das digitale Betriebsrisiko. Insbesondere Sicherheit und Datenmanagement werden in der Branche als wichtige Risikokategorien angesehen.

Der stärkste Antrieb für Veränderungen in diesem Bereich sind die geschäftlichen Anforderungen, einen “Always-on”-Service zu etablieren. Mit DORA und anderen FCA/PRA-Vorschriften wird ein größerer Schwerpunkt auf die Softwarequalität gelegt werden müssen, mit entsprechenden Überarbeitungen der Risikobeherrschung. Dieser Faktor wird nur von 20% der Unternehmen wahrgenommen.

Die derzeitigen Verantwortungs- und Meldeketten erstrecken sich nicht immer bis zum Vorstand, obwohl etwas mehr als die Hälfte der Unternehmen klare Kommunikationswege installiert hat. Dieser Umstand ließe sich einfach durch eine Stärkung des Vorstands mit technologisch versierteren Mitgliedern verbessern, die bei etablierteren Banken, Vermögensverwaltern und den meisten Versicherern allerdings eher spärlich gesät sind.

# Über die Autoren


## Olaf Bartelt

**Head of Market Business Unit**
**Banking & Financial Services**


Expleo ist ein weltweit tätiger Anbieter von Ingenieurs-, Technologie- und Beratungsdienstleistungen, der führende Unternehmen partnerschaftlich in ihrer Geschäftstransformation begleitet und sie bei der Realisierung operativer Spitzenleistungen und zukunftssicherer Geschäftstätigkeiten unterstützt. Expleo profitiert von mehr als 40 Jahren Erfahrung in der Entwicklung komplexer Produkte, der Optimierung von Fertigungsprozessen und der Qualitätssicherung von Informationssystemen. Mit fundierten Branchenkenntnissen und umfassendem Fachwissen in Bereichen wie KI-Engineering, Digitalisierung, Hyperautomatisierung, Cybersicherheit und Datenwissenschaft, verfügt die Expleo global über eine weitreichende Präsenz, mit über 15.000 hochqualifizierten Expertinnen und Experten, die in 30 Ländern Mehrwert schaffen.


olaf.bartelt@expleogroup.com
expleo.com
@ExpleoGroup
@ExpleoGroup



## Howard Womersley Smith

**Partner**


At Reed Smith, we believe that the practice of law has the power to drive progress. We know your time is valuable and your matters are important. We are focused on outcomes, are highly collaborative, and have deep industry insight that, when coupled with our local market knowledge, allows us to anticipate and address your needs. You deserve purposeful, highly engaged client service that drives progress for your business.


https://www.linkedin.com/company/reed-smith-llp/
reedsmith.com/en

# Über die Autoren


## Justyn Trenner

**Director**


QA Financial ist ein unabhängiger Anbieter von Forschung, Informationen und Analysen. QA Financial konzentriert sich auf die Software-Qualitätssicherung und die Treiber eines verbesserten Software-Risikomanagement bei Finanzunternehmen.


+44 (0)7703 162363

justyn@qa-financial.com
info@qa-financial.com

www.qa-financial.com

@QA Media



## Jamie Merritt

**CEO**


Accourt ist ein führender Anbieter von strategischen und operativen Beratungsdienstleistungen für die Zahlungsverkehrsbranche weltweit.

Accourt hat sich auf die Lösung von Problemen spezialisiert, die die Zahlungsverkehrsbranche betreffen. Unsere einzigartige Mischung aus erfahrenen Branchenspezialisten und lokaler Marktkenntnis hat uns zum bevorzugten Berater für die Marktführer der Branche gemacht.


+44 (0)7880 958880

jamie.merritt@accourt.com


QA Financial

expleo

accourt
PAYMENTS SPECIALISTS

ReedSmith