OLIVER WYMAN

STRIVING FOR OPERATIONAL RESILIENCE

THE QUESTIONS BOARDS AND SENIOR MANAGEMENT SHOULD ASK

AUTHORS
Rico Brandenburg
Tom Ivell
Evan Sekeris
Matthew Gruber
Paul Lewis

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

EXECUTIVE SUMMARY

Operational resilience has become a key agenda item for boards and senior management. Increasing complexity in processes and IT, dependence on third parties, interconnectedness and data sharing, and sophistication of malicious actors have made disruptions more likely and their impact more severe. High-profile examples of business and operational disruptions abound, covering all segments of the financial services industry.

Resilience is fundamentally different from traditional business continuity (BC) and disaster recovery (DR). These disciplines have historically been heavily focused on physical events, were designed and tested in organizational silos, and are, by most organizations, primarily viewed as a compliance exercise. Operational resilience, instead, focuses on the adaptability to emerging threats, the dependencies and requirements for providing critical business services end-to-end (crossing organizational silos), and the broader economic as well as firm-specific impact of adverse operational events. It requires a mindset shift in the organization away from resilience as a compliance exercise to resilience as a key organizational capability that is everyone's responsibility to maintain and continuously improve.

Financial regulators have started to stipulate expectations around management of resilience, resilience reporting, and effective oversight. In response, many firms are embarking or will need to embark on transformational programs to strengthen their resilience to disruption, incidents, and attacks across all operational resilience domains – technology, data, third parties, facilities, operations, and people. In addition, boards and senior management need to provide effective challenge of their organization's resilience ambitions, program, and critical risks that remain to their day-to-day operations.

Achieving operational resilience is inherently challenging given the increasing complexity of processes, technology infrastructure, and organizational silos. However, the business benefits go beyond pure risk and compliance, often forming an inherent part of a firm's value proposition.

This paper explores the key questions that boards and senior management should ask about their organization's level of operational resilience.

WHY NOW?

NEED FOR OPERATIONAL RESILIENCE

Continuity of service has always been a priority for financial firms. After all, disruptions can impact revenue, client experience, and franchise value.

Operational resilience is the ability of an organization to continue to provide business services in the face of adverse operational events by anticipating, preventing, recovering from, and adapting to such events.

BC and DR have historically emphasized physical events (e.g., natural disaster, active shooter), are limited by organizational boundaries, and are, by most organizations, primarily viewed as a "check the box" exercise rather than true risk management.

However, several trends in financial services have sharply increased the need for more mature operational resilience practices. Exhibit 1 below explores the most important trends, which we expect to continue to elevate the topic to discussions at the top table.

Exhibit 1: Drivers of exposure to disruption

	DRIVER	IMPACT ON EXPOSURE TO DISRUPTION
SCALE AND PACE OF INNOVATION	Competition and customer demand are driving the need for more disruptive innovations and faster innovation cycles	Increasing complexity of processes and infrastructure required for product and service delivery, and risk of imbalance between time to market and security/resilience
CONTINUED DIGITIZATION	Availability of new technology, customer expectations, and desires for efficiency are driving increasing levels of automation and faster adoption of digital delivery capabilities	Traditional (manual) fallback methods no longer viable, and more challenging to identify the "weakest link" among connected digital systems
RELIANCE ON LEGACY INFRASTRUCTURE	Incumbent institutions rely on older technology infrastructure that is less flexible, requires specialized knowledge to maintain, and is difficult to integrate with new technologies and processes	Challenging to embed risk and resilience requirements in technology, which increases the exposure to disruptive events
EXTENSION OF THE SUPPLY CHAIN	Institutions are increasingly adopting outsourcing as a business strategy, expanding their reliance on third parties (and their third parties' third parties)	More difficult to gain a comprehensive view of the firm's third-party dependencies and exposure, as well as to assess the risk and resilience posture of all relevant third parties
INTERCONNECTEDNESS AND SHARING	Financial institutions are sharing more information and services more broadly (partly through deliberate government policy)	More likely to be affected by vulnerabilities and disruptions in another part of the ecosystem
CONTINUED RISE IN SOPHISTICATION OF MALICIOUS ACTORS	Cyber attackers are innovating rapidly to identify new means of attack and ways of exploiting firms' vulnerabilities	More challenging to prevent, detect, respond, and recover from cyber attacks

These drivers have manifested themselves in high-profile business and operational disruptions across the financial services industry, both through internally-driven operational failures and externally-driven malicious acts. These disruptions illustrate some of the shortcomings of traditional BC and DR approaches:

- Firm have more dependencies for service delivery than ever before, but traditional approaches focus on assets in siloes and ignore potentially critical components of end-to-end service delivery.
- In a rapidly changing environment, traditional "check the box" and reactive approaches focused solely on recovery make firms much slower to adapt.
- By focusing on a standard set of disruption scenarios, traditional approaches provide a false sense of comfort that institutions are prepared for all scenarios.

Additionally, financial firms recognize the need for greater operational excellence (efficiency and effectiveness). Organizations that manage to effectively address the combined need for operational resilience and excellence will be able to unlock significant benefits across the organization (e.g., operational loss, operational cost and complexity reduction, ability to support faster innovation cycles, effective investment into operational capabilities).

BEND, BUT DON'T BREAK

OPERATIONAL RESILIENCE APPROACH

Operational resilience is the ability of an organization to continue to provide business services in the face of adverse operational events by anticipating, preventing, recovering from, and adapting to such events. The fundamental principle is "bend, but don't break."

Even for many advanced institutions, adopting an operational resilience approach will imply significant changes from traditional (more compliance-focused) BC and DR. Whereas these traditional approaches focus solely on recovery, operational resilience has a broader scope and needs to be integrated into the risk-mitigation fabric of the organization.

Resilient organizations focus on anticipation, prevention and adaptation, rather than recovery actions once the "horse has bolted." In addition, resilient organizations have creative ways to provide critical business services in the event of a disruption, beyond simply getting the technology up and running again (e.g., using branches to service customers at scale when digital channels might be down). Exhibit 2 shows the key characteristics of an operational resilience approach compared to most organizations' starting point – traditional BC and DR.

Exhibit 2: Key characteristics of operational resilience

CATEGORY	OPERATIONAL RESILIENCE APPROACH	TRADITIONAL APPROACH (BC/DR)
GOVERNANCE	• Clearly defined accountability of board and senior management • Resilience incorporated into risk appetite statements and metrics across operational risk types • Comprehensive and actionable reporting to drive continuous improvement	• Role of board and senior management limited to post-event response • Resilience not an explicit consideration in risk appetite statements and metrics • "Compliance-type" update on exercises
ORGANIZATIONAL FOCUS	• Critical business services end-to-end (ignoring organizational silos) • Broader economic impact of disruption, in addition to firm-specific impact	• Individual business units or specific technology assets • Firm-specific impact of disruption
INTEGRATION	• Comprehensive view of dependencies of critical business service on organizational assets (systems, data, third parties, facilities, processes, and people) • Resilience considerations embedded in the upfront design of business services and organizational assets	• View of dependencies in most cases limited to the business unit or directly linked technology assets • Continuity and recovery capabilities bolted on to satisfy requirements
MEASUREMENT	• Business disruption scenarios tailored to each critical service based on an aligned and forward-looking risk assessment • Tolerances for business disruption (impact tolerances) based on bespoke scenarios	• Standard business disruption scenarios across business units • Standard tolerances for business disruption (recovery time/point objectives) for all scenarios
PREPAREDNESS	• Single incident response regime (unified incident command) for all incident types • Plans and capabilities monitored, tested, and adapted continuously • Emphasis on building trust among crisis management team to enable effective response	• Distinct incident response regimes for different incident types, which may negatively impact response times • Plans and capabilities tested infrequently (e.g., annually) • Little attention paid to dynamics of crisis management team

Financial services regulators have begun to take note and are beginning to focus on promoting operational resilience, versus traditional BC and DR. The principles outlined in Exhibit 2 are reflected in an increasing body of regulatory consultation and guidance papers.

With the lessons from the financial crisis still fresh, regulators have overlaid a "systemic" lens, prompting firms to explicitly consider and measure how disruptions would impact the broader market. At the same time, they are emphasizing that resilience is applicable to all institutions, even if the objectives for each institution might differ. For example, Financial Market Infrastructure's (FMI) resilience objectives will likely focus on avoiding systemic disruptions, while smaller institutions' objectives will likely focus on maintaining shareholder value.

Global institutions will need to pay particularly close attention to regulatory developments, as regulators in different jurisdictions have not yet aligned on their expectations for firms.

RECENT RESILIENCE-RELATED REGULATORY PUBLICATIONS

JULY 2018

Bank of England/Prudential Regulation Authority/Financial Conduct Authority discussion paper, "Building the UK financial sector's operational resilience"

DECEMBER 2018

European Central Bank guidance, "Cyber resilience oversight expectations for financial market infrastructures"

European Banking Authority consultation paper, "Guidelines on ICT and security risk management"

MARCH 2019

Monetary Authority of Singapore consultation papers, "Proposed Revisions to Guidelines on Business Continuity Management" and "Technology Risk Management Guidelines"

IMPORTANT QUESTIONS TO ASK ABOUT OPERATIONAL RESILIENCE

Achieving operational resilience is inherently challenging and complex:

- It requires organizations to understand how all domains (technology, data, third parties, facilities, operations, and people) impact critical service delivery and to build a consistent set of resilience capabilities and controls across these domains.
- It depends on cross-functional, specialized expertise to evaluate and measure the resilience of the organization in light of the specific risks it faces.
- It relies on extensive coordination, collaboration, and preparation to ensure that the organization appropriately considers resilience in all activities and is ready when the worst happens.

Given the complexity of the topic, it is difficult for boards and senior management to assess the current level of operational resilience and determine whether the organization is making resilience investments in the right areas.

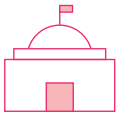
What questions should boards and senior management be asking to provide meaningful challenge and oversight?

We believe that boards and senior management should focus on understanding the risk levels of their firms, assessing their firms' readiness for disruptive scenarios, and gaining comfort that their firms have a robust approach to resilience. Boards and senior management should also demand a minimum level of data to support ongoing oversight of risk levels and the progress made along the resilience journey.

Exhibit 3 contains a list of key questions on resilience that boards and senior management should ask their management teams.

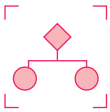
If the answers to these questions are unsatisfactory, it could signal that the organization needs to increase focus on resilience. In this case, boards and senior management should request that their organizations establish a formal maturity baseline and refocus existing initiatives or launch a new program to uplift their resilience.

Exhibit 3: Resilience questions for boards and senior management



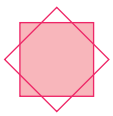
GOVERNANCE

- ☐ What is our risk appetite for resilience risk?
- ☐ What KRIs and KPIs provide us with a comprehensive view of our maturity and uplift program?
- ☐ Who is accountable in the 1st and 2nd lines of defense for managing, monitoring, and reporting on resilience?



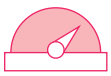
ORGANIZATIONAL FOCUS

- ☐ Does the organization understand the dependencies of critical business services on organizational assets?
- ☐ What are our most critical assets that impact service delivery?
- ☐ How does our approach to resilience change the way we manage operations, technology, and third parties?



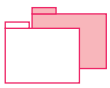
INTEGRATION

- ☐ What is our measure of criticality?
- ☐ What are our critical business services and why?
- ☐ How are we leveraging existing definitions of criticality and critical business services (e.g., from resolution planning)?
- ☐ What is our impact on customers and the financial system?



MEASUREMENT

- ☐ What are the most important resilience risks for the organization?
- ☐ How do we monitor and manage the level of resilience of the organization?
- ☐ How is risk appetite reflected in our impact tolerances?
- ☐ In which scenarios are we outside of our defined impact tolerances?



PREPAREDNESS

- ☐ How do we make sure we are effectively prepared for different disruption events?
- ☐ How frequently are we testing our response and recovery capabilities for different disruptive scenarios?

GETTING STARTED

For firms needing to launch or reset their programs, we recommend starting small, providing transparency to the boards and senior management, and getting resilience right for one critical service before expanding the program.

Exhibit 4 lays out an approach to establishing an effective operational resilience program that allows the organization to enhance its capabilities without being overwhelmed by the scale of the effort.

Exhibit 4: Key steps for establishing an effective operational resilience program

Organizations that manage to establish effective operational resilience programs will be able to realize the benefits of better resilience as well as related business benefits:

- Reduce and optimize their risk exposure, with improved visibility into their risks, better monitoring, a more proactive approach to controls, and ability to deliver services even when things go wrong.
- Better focus the organization and drive investment towards the most important areas, based on a prioritization of their critical business services.
- Be able to support the innovation agenda of the business and enable faster innovation cycles without compromising on risk management by ensuring the organization is adaptable and considers resilience up front.
- Be more effective and efficient, leveraging a clear understanding of critical service delivery to reduce costs (e.g., optimize outsourcing relationships), streamline processes (e.g., introduce tools and automation), and enhance efficacy (e.g., identify and remediate steps that introduce errors).

However, building an effective program is not easy. It will require new skillsets; closer integration and alignment of risk, IT, and the business; a cultural shift away from "operational resilience is IT's responsibility" to "operational resilience is everyone's responsibility;" and fundamental changes to how the organization operates.

Boards and senior management can help their organizations overcome these challenges. They can encourage the right level of investment, drive a "tone from the top" to break siloes and change culture, and set clear expectations for progress.

Ultimately, by asking the right questions and demanding accountability when the answers are unsatisfactory, boards and senior management can play a pivotal role in enabling their organizations to achieve resilience. With the growing complexity in financial services, it is incumbent on every organization to take resilience seriously, and it is incumbent on boards and senior management to make sure their organization's resilience program is on track.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertisein strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

ABOUT THE AUTHORS

Rico Brandenburg
Partner in the Risk & Public Policy and Digital practices, New York
rico.brandenburg@oliverwyman.com

Tom Ivell
Partner in the Risk & Public Policy practice, Zurich
tom.ivell@oliverwyman.com

Evan Sekeris
Partner in the Risk & Public Policy practice, Washington, D.C.
evan.sekeris@oliverwyman.com

Matthew Gruber
Engagement Manager in the Risk & Public Policy and Digital practices, New York
matthew.gruber@oliverwyman.com

Paul Lewis
Principal in the Risk & Public Policy practice, London
paul.lewis@oliverwyman.com

www.oliverwyman.com

OLIVER WYMAN