Crowe

Smart decisions. Lasting value.™

October 2021

Operational resilience: Why embracing disruption in financial services is critical

An article by John A. Epperson and Ryan C. Luttenton, CPA

Operational resilience is a maturing topic in Europe and the United Kingdom (U.K.). In 2020, Justin Elks of Crowe U.K. authored an article on the topic in which he outlined the potential benefits of operational resilience using six broad categories. He also explained that regulators in the U.K. expressed a fairly strong stance and consistent expectations regarding operational resilience across the financial services sector.[1]

Fast forward 18 months.

Interest in operational resilience has traveled across the Atlantic and is garnering more attention.[2] It is sneaking its way into board room conversations as well as audit committee meetings. The challenges we've faced with the COVID-19 pandemic have prompted us to change how we operate in our personal and professional lives, and as such, we have had to adjust our business models and how we serve our clients.

Now, many financial services organizations in the United States are starting to consider operational resilience as boards and executives respond to inquiries regarding how the organization is able to respond to myriad disruptions. Complex processes and technology, vendor dependency, data collection and usage, cyberthreats, and other factors have made disruptions more frequent and more impactful.

Such disruptions have not escaped the notice of regulators, who seek to confirm that financial services organizations can continue to provide key services, with only limited interruption, when faced with severe, but plausible, operational events. U.K. regulators, including the Bank of England, the Prudential Regulation Authority, and the Financial Conduct Authority have published independent and joint policy papers on building operational resilience.[3] The Basel Committee on Banking Supervision has issued guidance on operational resilience,[4,5] and the Federal Reserve, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corp. published an interagency paper on strengthening operational resilience.[6] Although the regulatory sound practices were meant for the largest banks, the principles apply to organizations of all sizes.[7]

Why? Disruptions are size-agnostic. Because disruptions differ, stakeholders have a vested interest in understanding how business lines – including associated operations, services, functions, and third parties – might experience a material change of revenue, profit, or franchise value if they are disrupted.

Often, organizations approach operational resilience as an extension of operational risk. For example, organizations base their business continuity (BC) and disaster recovery (DR) programs on principles and practices of responding to physical events such as natural disasters, fires, or pandemics. Each department and function usually designs and tests plans as part of annual check-the-box exercises. If a BC or DR plan is executed, it is typically in reaction to something unanticipated and unexpected, not a thoughtful evaluation of the organization's end-to-end continued delivery of services based upon broader firm-specific operational and economic goals. However, BC and DR programs are

company focused. The real mindset change with operational resilience is for companies to thoughtfully consider what stresses and disruptions mean for customers.

This begs the question: Is operational resilience really about operational risk, or is it about something more? We think it's about something more. Operational resilience demands that organizations focus on managing risk versus identifying risk and responding to disruptive events.

Organizations must be nimble to adapt to unexpected events, but disruption comes in many forms – some instantaneous, some delayed, some occurring over time – requiring the organization to adapt, change, move, and improve accordingly. Knowing that disruptions can span across businesses and involve both internal operations and third parties, operational resilience must be treated as a collective whole. Tackling this subject from a siloed business or functional perspective will only lead to shortcomings.

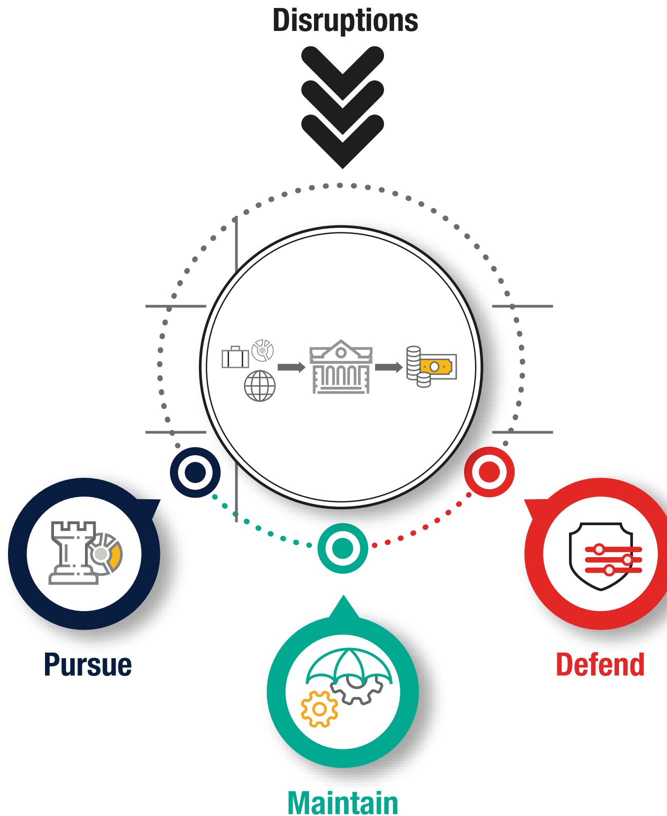
Operational resilience: Beyond core service continuity

What is operational resilience?

> Operational resilience is the ability of a company to build confidence and trust in its capability to adapt to changing circumstances. This is achieved by preventing, responding to, and recovering and learning from stresses and disruptions whilst delivering on promises to customers, achieving critical business objectives, and operating within agreed tolerances.[8]

Operational resilience can create value and has the potential to add competitive advantage. This requires an expanded mindset about the conceptual underpinnings of resilience: What constitutes a disruption? Disruptions can have both positive and negative organizational effects. By defining disruptions as both positive and negative, the organization moves away from operational resilience as a compulsory exercise to a core capability that functions throughout the organization.

Exhibit 1: Evaluating disruptions



Source: Crowe analysis

When risk management and the chief operating officer work together on operational resilience, they can more effectively tie risk to the strategies and objectives of the organization. Risk's definition is uncertainty, having both positive and negative outcomes. Moreover, the breadth of risk covers factors both internal and external to the organization, which is important in defining relevant disruptions across an organization's risk taxonomy.

As a result, disruptions can have a variety of effects. When evaluating the disruption, the organization can choose to pursue potential opportunities, maintain the current set of activities, or take action to mitigate and manage unwanted exposures (see Exhibit 1).

Disruptions also put increasing pressure on the need for operationally resilient activities. Organizational responses will have both board and regulatory interest. Exhibit 2 lists various disruptions and their implications.

Exhibit 2: Disruptions and their implications

Disruption	Implication
Nontraditional competition	Threats to products and services exist from organizations both in and outside financial services that disintermediate or develop models to challenge the status quo.
Continued adoption of digitization	With more digitization comes increasing levels of automation and greater adoption of digital delivery models. Channels can be connected throughout the value chain, from front to back office.
Number and sophistication of cybercriminals	Attackers increasingly are becoming more innovative, exploiting organizational vulnerabilities, making it challenging to identify, prevent, respond, and recover from attacks.
Reliance on and migration from legacy infrastructure	Older technology requires specialized skill sets to operate, integrate with, and maintain new and emerging technologies.
Innovation scale and velocity	Customer demand and competition are driving faster innovation cycles, so moving first and getting to market quickly are more important than ever.
Data increase and use	Structured and unstructured data that can offer support and insight to business decision-making continues to increase. Quality, privacy, quantity, and protection are the variables organizations need to address.
Vendor dependence	Outsourcing strategy places increasing risk on the dependence on third and fourth parties.

Source: Crowe analysis

Why now?

Financial services professionals broadly recognize that operational resilience is and has been crucial to the overall stability of an organization as well as its role within the broader financial system. Exacerbated by recent events such as the COVID-19 pandemic, cyberthreats, and the increasingly prevalent use of technology, regulators, shareholders, and customers want to make sure that organizations can recover from a disruption and take advantage of opportunities.

Taking cues from U.K. and European regulators, U.S. regulators are demonstrating increased interest in understanding and evaluating the efficacy of organizations' operational risk strategies. Policy letters, rules, regulations, and notices are pervasive as agencies not only rely on existing safety and soundness activities but are expanding into specific operational resilience topics such as information technology.

Guidance on operational resilience continues to emerge, including the two Basel Committee papers on operational resilience noted earlier. The diversity of operational resilience topics also is expanding, as is demonstrated by the Committee of Sponsoring Organizations of the Treadway Commission and its environmental, social, and governance guidance.

An operational resilience focus is not purely on the organization itself; it extends to suppliers, third parties, and even customers. It is important to understand

how the organization delivers its products and services, including both in-house and outsourced processes and functions. The third-line audit function increasingly wants to oversee processes and verify that operational resilience policies and activities exist.

Moreover, operational resilience should extend into specific risk management considerations such as risk appetite, tolerance, and the assessment process. The interconnectedness of business and functional activities heightens the need for risk management to understand how risks might manifest themselves across value chains. This holistic focus puts further pressure on adopting organizationwide risk management and rejecting the myopic, siloed approach that traditionally limits a complete understanding of the overarching risk profile.

Benefits of operational resilience

Imagine getting better as an organization after every disruption. Organizations that can do so embrace disruption because they know they are resilient and that they can improve. That is one benefit of operational resilience. Another salient benefit is winning and retaining the trust of customers. If customers are confident that they will matter to the organization, that the organization is focused on the long game, and that the organization is proactively managing its long-term existence, they might be more likely to select and be loyal to that organization.

At Crowe, we encourage our clients and prospects to explore operational resilience and how it functions (if at all) in their organizations. Knowing where capabilities are strong and where gaps exist creates insight into strategic moves, alternatives, and risk decisions. Examples of relationships, services, and functions that might be explored include strategic partnerships and joint ventures, entering and exiting businesses, creation of new products and services, smoothing of earnings, better resource allocation, better capital expenditures, and recognizing control diversification effects.

Across industries, the need to adapt to changing circumstances is a given. Organizations that take proactive steps can employ a collaborative approach across the lines of defense to link operationally resilient processes and activities. In so doing, they can better understand the effects of such processes on the organization's risk profile and the implications on its strategies and objectives.

Learn more

John Epperson
Managing Principal, Financial Services
+1 630 575 4220
john.epperson@crowe.com

Ryan Luttenton
Partner, Financial Services Consulting
+1 630 990 4484
ryan.luttenton@crowe.com

---

[1] Justin Elks, “Operational Resilience: What Is It, and What Does It Mean for the Board and Senior Management?,” Crowe, January 2020, https://www.crowe.com/-/media/Crowe/LLP/folio-pdf-hidden/Operational-Resilience-FW2015-002.pdf

[2] Justin Elks, Madeline Betts, and Daniel Spreckley, “Building Operational Resilience: Key Messages From the March 2021 Policy Statements,” Crowe U.K., March 29, 2021, https://www.crowe.com/uk/insights/building-operational-resilience

[3] Clare Reynolds and Charlotte Hill, “Operational Resilience: Final Policies From UK Regulators,” TaylorWessing, April 19, 2021, https://www.taylorwessing.com/en/insights-and-events/insights/2021/04/operational-resilience---final-policies-from-uk-regulators

[4] Basel Committee on Banking Supervision, “Principles for Operational Resilience,” Bank for International Settlements, March 31, 2021, https://www.bis.org/bcbs/publ/d516.htm

[5] Basel Committee on Banking Supervision, “Revisions to the Principles for the Sound Management of Operational Risk,” Bank for International Settlements, March 31, 2021, https://www.bis.org/bcbs/publ/d515.htm

[6] “SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience,” Board of Governors of the Federal Reserve System, Nov. 2, 2020, https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm

[7] Ibid: “Average total consolidated assets greater than or equal to (a) $250 billion or (b) $100 billion and have $75 billion or more in average cross-jurisdictional activity, average weighted short-term wholesale funding, average nonbank assets, or average off-balance-sheet exposure.”

[8] Elks, p. 2.

crowe.com

“Crowe” is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. “Crowe” may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. © 2021 Crowe LLP.

CFS2299-010B