THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

TECHNOLOGY

Operational resilience in the financial sector: Evolution and opportunity

AENGUS HALLINAN

20
YEAR ANNIVERSARY

OPERATIONAL RESILIENCE

#53 MAY 2021

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

OPERATIONS

TECHNOLOGY

MILITARY

DEAR READER,

Welcome to this landmark 20th anniversary edition of the Capco Institute Journal of Financial Transformation.

Launched in 2001, the Journal has followed and supported the transformative journey of the financial services industry over the first 20 years of this millennium – years that have seen significant and progressive shifts in the global economy, ecosystem, consumer behavior and society as a whole.

True to its mission of advancing the field of applied finance, the Journal has featured papers from over 25 Nobel Laureates and over 500 senior financial executives, regulators and distinguished academics, providing insight and thought leadership around a wealth of topics affecting financial services organizations.

I am hugely proud to celebrate this 20th anniversary with the 53rd edition of this Journal, focused on 'Operational Resilience'.

There has never been a more relevant time to focus on the theme of resilience which has become an organizational and regulatory priority. No organization has been left untouched by the events of the past couple of years including the global pandemic. We have seen that operational resilience needs to consider issues far beyond traditional business continuity planning and disaster recovery.

Also, the increasing pace of digitalization, the complexity and interconnectedness of the financial services industry, and the sophistication of cybercrime have made operational disruption more likely and the potential consequences more severe.

The papers in this edition highlight the importance of this topic and include lessons from the military, as well as technology perspectives. As ever, you can expect the highest caliber of research and practical guidance from our distinguished contributors. I hope that these contributions will catalyze your own thinking around how to build the resilience needed to operate in these challenging and disruptive times.

Thank you to all our contributors, in this edition and over the past 20 years, and thank you, our readership, for your continued support!

Lance Levy, **Capco CEO**

OPERATIONAL RESILIENCE IN THE FINANCIAL SECTOR: EVOLUTION AND OPPORTUNITY

AENGUS HALLINAN | Chief Technology Risk Officer, BNY Mellon

ABSTRACT

The 2008 global financial crisis served to illustrate the interconnectedness and the global nature of the world's increasingly complicated financial services sector. While the concept of financial resilience has been front of mind for regulators for decades, the broader concept of operational resilience has gathered momentum and increasing focus over the past 10 years. The financial system has shown itself to be robust in the face of the COVID-19 pandemic to date, however, the pandemic has also served to further illustrate the broad nature of disruption that can quickly spread across the world. Regulators, boards, and senior executives have shifted their view from resilience being about responsiveness to specific events, such as a cybersecurity incident, to the wider multi-faceted question of operational resilience and preparedness for severe disruption – regardless of cause. Regulators across the globe are converging on a common definition and it is broader than ever before, with expectations around preparing for, responding and adapting to, and recovering and learning from severe disruption. There is recognition that vulnerability at a single firm, financial utility, or third party provider can result in substantial negative consequences across the financial system. Boundaries are greyer and wider than ever – and previously considered individual risks are converging faster. Regulators are focused on ensuring operational resilience is paramount in protecting financial stability as an essential service. While firms need to be prepared, they should also see operational resilience as an opportunity to positively differentiate themselves in the eyes of their clients and other key stakeholders.

1. INTRODUCTION

As financial organizations have increased in complexity and as the interconnectivity of the financial system has grown dramatically over the past 20 years, there is a heightened focus on a broad definition of "operational resilience". Regulators are increasingly concerned about the vulnerability of this complex financial system, as opposed to an individual firm's ability to withstand specific disruptions. The overall financial ecosystem now consists of a complex interplay between traditional banks, financial market utilities/infrastructure players (FMU/FMI), vendors, out/insourcers, regulatory and government agencies, and a diverse array of clients, market participants, and financial instruments on a global basis. It is difficult to consider any single factor in isolation, for example, a cybersecurity incident may impact specific components of the financial ecosystem but quickly contaminate the broader environment. A single central counterparty (CCP) may sit at the center of a complex web of dependencies where even an isolated problem could cause havoc across the ecosystem. Where once a regulator might have focused independently on a firm's cybersecurity and readiness, it is now just one component of a more overarching interest in a firm's operational resilience.

The Bank of England (BoE) is notable in its early prioritization of a focus on operational resilience – but financial regulators around the world are increasingly embracing the concept in their interactions and guidance. The Bank of England sees operational resilience as "the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions." [FCA (2018)]. This provides a useful lens through which to consider the topic and is entirely in keeping with the overall mission of regulatory bodies to ensure important financial business services are

maintained and disruptions that might "cause wide-reaching harm to consumers and market integrity, threaten the viability of firms and cause instability in the financial system" are kept to a minimum [FCA (2018)].

Prior to the more formal definitions and expectations set by regulators, financial institutions did, of course, recognize the need to consider their operational resilience – or simply put, how well their organization was able to withstand and respond to stress. Resilient organizations with resilient processes might bend, but should not break, in the face of these stresses.

A challenge to date has concerned codifying definitions and expectations when it comes to operational resilience and to differentiate it from the traditional risk management discipline of "operational risk". Sound operational risk management is certainly a prerequisite for operational resilience, but it is not the same thing.

2. OPERATIONAL RISK VERSUS OPERATIONAL RESILIENCE

Operational risk management should provide a robust framework for key controls, reporting and oversight to avoid loss. As per the Basel Committee on Banking Supervision (BCBS), operational risk is defined as the "risk of loss resulting from inadequate or failed internal processes, people and systems or external events" [BCBS (2011)]. The issue with this definition is that it can frequently be inherently backward looking, driven by control failings and losses after they have happened. A process that does not appear to have a great deal of operational risk around it based on empirical evidence (e.g., very few actual losses) may in fact be inherently unsound with a very low tolerance for any disruption – and hence, not at all operationally resilient. It may go from appearing to operate in a consistently "stable" fashion to not operating at all once a stress is applied.

It is entirely conceivable that a highly inefficient and non-resilient business process could appear under normal operating conditions to be running satisfactorily with no operational losses and few errors or customer complaints. Under normal circumstances, the operational risk may appear low. But when an unanticipated stress is placed on the system – e.g., a highly manual process experiences mass staff attrition or volumes spike – the lack of resilience is exposed with a consequent increase in operational incidents, possible losses, and customer complaints. Simply put, viewing existing business processes through a resiliency lens may provide a different perspective in advance of having to respond to a significant increase in operational risk once a stress is applied.

Clearly, the measures we might consider in the context of operational resilience are different from those we might traditionally consider when thinking about operational risk. For operational resilience, we should be more concerned about leading indicators – such as staff turnover, ratio of manual to automated processes, concentration of activity in one location, differentiation between "critical" and "ancillary" processes, or success of recovery tests – while, of course, continuing to monitor the more obvious and typical operational risk indicators, such as incidents, fail rates, errors, and unresolved breaks that are often backward looking.

3. EVOLUTION NOT REVOLUTION

As reinforced by much of the recent regulatory discussion, the expectations regarding operational resilience are far more about connecting the dots between existing regulation and existing internal organizational units and responses. The Basel Committee is explicit in its promotion of a "principles-based approach to improving operational resilience" and draws from "previously issued principles on corporate governance for banks, as well as outsourcing-, business continuity- and relevant risk management-related guidance" [BCBS (2020)]. The Federal Reserve Board/Office of the Comptroller of the Currency/Federal Deposit Insurance Corporation [FRB/OCC/FDIC (2020)] interagency paper notes that it "does not set forth any new regulations or guidance… but brings together the existing regulations and guidance in one place to assist in the development of comprehensive approaches to operational resilience." Even the U.K.'s Prudential Regulation Authority (PRA), which has been somewhat more prescriptive in its expectations, emphasizes that much of its most recent policy is supported by existing PRA policy. Thus, recent regulatory guidance is not "new" – but it is certainly more comprehensive when it comes to operational resilience.

That is not to say that there is nothing to be done and no additional cost to be incurred; where the key components exist, this should not necessarily require a revolutionary, large scale, and expensive implementation program. Rather a more holistic approach, linking services and responses that may today be acting in siloes; bringing together existing risk functions, business continuity management, IT resilience teams, supply chain and third party management, cybersecurity, and so forth. Individual risk management frameworks, continuity planning, scenarios, and tolerances likely exist. The focus on

operational resilience, however, requires that these be brought together in a cohesive manner to ensure that critical business processes and services are operationally resilient end-to-end regardless of the source of disruption or where in the process chain it manifests. This is also reflected in the regulators' expectations.

4. CONVERGING REGULATORY DEFINITIONS OF OPERATIONAL RESILIENCE

Different regulators define operational resilience in different ways. The interagency paper [FRB/OCC/FDIC (2020)] describes it as the "ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions." It is not possible to predict every possible disruption, but it is possible to consider thematically how prepared a firm is and how well it is able to respond. Notably, the COVID-19 pandemic was not necessarily the type of disruption that was at the forefront of regulatory considerations (that honor might have gone more deliberately to a cybersecurity event, which remains a major potential threat), but it is precisely the kind of widespread, systemically relevant thematic disruption regulators want to ensure the financial system is robust enough to withstand.

As noted previously, the Bank of England, in a paper published jointly with the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), defines operational resilience as "the ability of firms and FMIs (financial market infrastructures) and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions" [FCA (2018)]. Increasingly, since the 2008 Global Financial Crisis, U.K. regulators have recognized that "a lack of operational resilience represents a threat to each of the supervisory authorities' objectives, as well as to their shared goal of maintaining financial stability" [FCA (2018)]. More specifically, the FCA (2018) states that "operational disruptions and the unavailability of important business services have the potential to cause wide-reaching harm to consumers and market integrity, threaten viability of firms and cause instability in the financial system." Clearly, the U.K. authorities are focused on the resilience of the overall financial system, with every participant having a role to play.

Figure 1: Regulatory landscape – operational resilience

The Basel Committee on Banking Supervision (BCBS) goes further and references operational resilience as "the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimize their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should take into account its overall risk appetite, risk capacity and risk profile." BCBS (2020) also notes that "operational resilience is an outcome that benefits from the effective management of operational risk. ... An operationally resilient bank is less prone to incur untimely lapses in its operations and losses from disruptions, thus lessening their impact on critical operations and their related services, functions and systems."

We have seen over the past few years that despite the various definitions of operational resilience from numerous regulators at varying times, at their core, they all thematically speak to the ability to continue to deliver critical operations through disruption from any hazard. Regulators have been moving beyond simply the question of business continuity management or how an individual firm deals with an incident or a specific event and are seeking a much more holistic response – an overall level of resilience end-to-end regardless of the breadth or nature of the disruption. Unsurprisingly, the key concepts of "prevent, adapt and respond, recover and learn" will resonate with those familiar with the widely-adopted NIST (National Institute of Standards and Technology, U.S. Department of Commerce) cybersecurity framework given the importance of cybersecurity to operational resilience.

From this, we can derive a common amalgam definition that can be applied across a global organization and should be equally applicable to all components of the interconnected financial system. Operational resilience is thus, "the ability of firms and the financial sector as a whole to deliver critical operations and core business lines through a disruption from any hazard. Firms and the financial sector must be able to anticipate and prepare for, respond and adapt to, and recover and learn from disruptive events in order to minimize their impact on the delivery of critical operations during significant disruption."

There are clearly core expectations regarding the existence of effective operational risk management frameworks, controls, reporting, and oversight. There is also a need to differentiate "critical operations" and "core business lines" from the many operations of a firm. Business continuity management and crisis management responses must extend beyond the firm's own perimeter and consider third and even fourth party exposures and dependencies. Recovery goes beyond the traditional infrastructure recovery. And "learning" from disruptive events is both considered in terms of lessons learned (whether due to incidents experienced by the firm itself or others) as well as lessons to be considered in terms of scenarios, testing, and exercises to prepare for events that have not happened, but well might. It is almost entirely open ended, but some differentiation based on business criticality is possible.

5. DIFFERENTIATION BY BUSINESS PROCESS

It is understood (including by regulators) that not all activities that a firm or a segment of the financial system perform are of equal importance or criticality. Some activities are absolutely critical and require near constant availability with (near) zero tolerance for disruption or down time. Others may be less time sensitive and can be deferred for a period. This differentiation is crucial to a firm's abilities to prioritize and focus accordingly on the most essential elements of its operations in the face of an extreme disruption.

Preparation must include a systematic and robust way to identify and differentiate a firm's critical operations. Per the U.S. regulatory guidance, critical operations are those "operations of the firm, including associated services, functions, and support, the failure and discontinuance of which would pose a threat to the financial stability of the United States" [FRB/OCC/FDIC (2020)]. It is a much broader definition than simply how the firm perceives its most valuable or profitable business lines, moving as it does into the realm of the financial system in its entirety.

Differentiation of critical operations does allow for a differentiated response in terms of resiliency expectations, such as redundancy, recovery time, availability, and so forth. It is also imperative, however, that the full range of end-to-end dependencies to sustain a critical operation or business are understood. This will likely include a combination of people, processes, facilities, and systems and may be further complicated by dependencies on third and fourth party providers – including critical infrastructure providers (e.g., telecommunications and other utilities), business process outsourcing providers (which may themselves exhibit concentration risk, increasingly providing outsourced services to many consumers), financial market utility providers (e.g., clearing houses, brokers, etc.), and, increasingly, inter-affiliate relationships.

If firms are to be able to meet the expectations of regulators, senior management, and other stakeholders, they will have to be able to identify, define, and map out their critical operations in a complete, comprehensive, and sustainable fashion that can adapt to changing circumstances such that operational resilience can be maintained. This must include the full array of dependencies to allow the business service to continue to operate in the face of disruption. Determining operational resilience for critical business services requires a full end-to-end understanding and recognition of the key people, key systems, key data, key supply chain dependencies, key facilities, key providers, and key processes. A lot of keys.

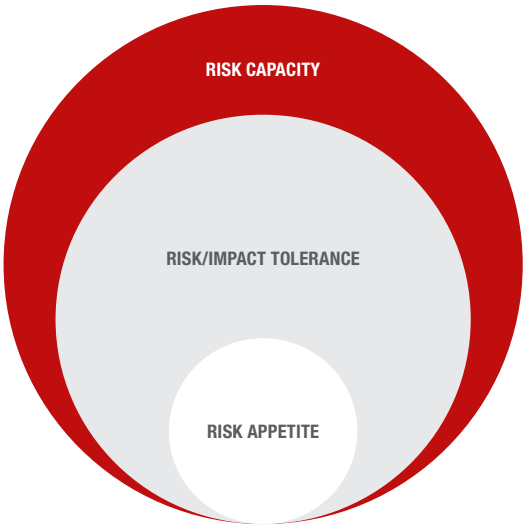
6. REDEFINING BOUNDARIES

The challenge is that the traditional "perimeter" that a firm is defending is frequently expanding and the boundaries are far less clear-cut. Firms are increasingly migrating at least some of their platform away from traditional, physical single occupier data centers to virtual, cloud-based providers, where they may not know where the machines running their core services are physically located. They are using third party firms to provide business processing outsourcing services in cheaper and more efficient locations. The third parties are using their own providers to create a fourth party exposure. It is not uncommon for a firm to have an exposure to, for example, a telecommunication provider with which it has no direct relationship by virtue of its third party providers using that telecommunication provider, creating a fourth party exposure.

In many ways, the resilience of the financial system has been strengthened by these developments as has been seen through the COVID-19 pandemic in 2020 and into 2021. Firms' abilities to rapidly adapt and operate remotely with little disruption has largely been due to these developments, where specialist providers can service multiple consumer firms far better than if each firm were to try to develop these specialist capabilities themselves (leveraging the provision of cloud services offered by specialist providers being but one example). It is widely acknowledged that the pandemic has evidenced a resilience in the interconnected financial system that had not been previously tested to this extent, but which has performed remarkably well.

Since the 2008 Global Financial Crisis, financial organizations have also increased their dependency on financial market utilities such as central counterparties and clearing houses. To reduce the opaqueness that became apparent with the fallout from the financial crisis, regulators moved to dramatically increase the engagement of central clearing houses for greater transparency. In so doing, there is additional concentration risk regarding these (often regulated) entities and a need for firms to look beyond just credit exposure and more towards their operational risk exposure to these entities in assessing their operational resilience.

Figure 2: Risk appetite, tolerance, and capacity



Risk appetite is the level of risk an organization is willing to accept in pursuit of its objectives.

Impact tolerance represents the tolerance of an organization to survive severe but plausible disruptions, even while exceeding risk appetite.

Risk capacity is the maximum risk an organization can afford to take.

It is not that the extending of perimeters and boundaries, and the dependency on third and fourth parties, are necessarily a bad thing with regard to resilience, but it certainly introduces greater complexity as firms must be able to identify all these dependencies for their critical operations and ensure that in assessing their operational resilience they are also able to assess the resilience of those they depend upon.

7. RISK APPETITE, IMPACT TOLERANCE, AND RISK CAPACITY

Firms in the financial services sector are used to talking about risk capacity and risk appetite. Regulators, particularly in the U.K., are increasingly also talking of "impact tolerance" in the context of operational resilience.

While "risk appetite" is established to represent the level of risk an organization is willing to take in the course of its day-to-day operations in pursuit of its strategic objectives, it is recognized by the regulators and senior executives that there will be periods of time when disruptions will impair an organization's ability to operate business-as-usual and its risk appetite will be exceeded. In these circumstances, firms have begun to increasingly identify "impact tolerances" for each of their core business services, which represent specific maximum levels of disruption that they can tolerate (and for what period) without critically impacting their ability to provide essential services or to remain economically viable. FCA (2018) puts it like this: "firms should set their impact tolerances at the first point at which a disruption to an important business service would cause intolerable levels of harm to consumers or market integrity. It is different from risk appetite because it assumes a risk has crystallized and may go beyond a firm's RTO (recovery time objective). It is also different to business impact analysis as it is determined with reference to the FCA's public interest in reducing harm to consumers and market integrity."

Such tolerances may relate to "service level agreement" (SLA) breaches, loss of access for a set maximum period, maximum delay in execution of certain services, loss of critical information/data, financial impact to customers, and so forth. The key being to design the critical services to ensure they can stay within those impact tolerances in the face of severe but plausible disruption. The focus must be on maintaining critical services to an acceptable standard in the face of severe disruption (e.g., how long can this service take to recover before it has a substantial impact on customers or the financial system), which clearly ties in well with regulatory expectations with regard to operational resilience and the soundness of the financial system and is represented in how regulators (in the example above, the FCA) are defining impact tolerances.

Noting that identifying and mapping critical business operations or services requires a full and comprehensive identification of all dependencies and elements, it is also important to recognize that establishing such impact tolerances may extend beyond the typical system outage, customer losses, and time to recover. Where dependencies exist on third party providers (which could range from business process outsourcing to critical utility providers), this will also have to be accounted for in establishing and testing against impact tolerances.

One useful yardstick to consider is that operating within risk appetite should be the domain of business-as-usual risk management, acknowledging that risk appetite will be exceeded for periods of time and in specific areas but can be managed through the normal course of business with minimal disruption. Once actual risk levels approach impact tolerances, a firm enters crisis management/business continuity management mode, operating at elevated risk levels but maintaining critical business services. If the situation escalates further, such that critical business services are no longer able to be maintained and risk capacity is exceeded, a firm may be entering the realm of "recovery and resolution" and some kind of external intervention could be an extreme consequence, as we saw with the bank bailouts in the face of the Global Financial Crisis in 2008. In fact, when impact tolerances are exceeded, it is possible that the full consequences may not immediately take effect, but irreparable damage has been done that may yet put a firm's existence at risk, even many months later.

8. CONVERGING VERSUS EMERGING RISKS

A recurring theme when considering a firm's operational resilience is the concept of the ability to withstand the impact of "severe but plausible disruptions". It would be impossible to precisely define every conceivable scenario of such disruptions, but it is assumed that severe disruptions will occur on occasion, impacting the ability of a firm to operate business-as-usual and exceeding risk appetite. As noted, the key is to test whether the firm can continue to provide critical services within predefined impact tolerances. Defining representative scenarios that can be used to test a firm's ability to operate within these impact tolerances in the face of such stress is a critical tool in ensuring, and being able to illustrate, a level of operational resilience.

While impossible to define every possible scenario, it may be helpful to consider the following scenario buckets:

- **Existing threats and risks:** identified risks, which are impacting the organization today and being actively managed, but which may still pose a future threat to the organization over time or under changing circumstances, e.g., severe weather events.
- **Emerging threats and risks:** identified risks that are not yet having a material impact on the organization (they may be impacting other organizations or industries, for example), but which a firm should prepare for given the likelihood that they will impact the organization in the

future, increase in frequency over time, and could result in a severe but plausible disruption, e.g., new types of cybersecurity incidents, climate change, etc.

- **Converging threats and risks:** identified risks that individually may threaten the organization but which, if compounded, could present a much higher level of aggregate risk that may require a multi-faceted response, e.g., a cyber attack on cloud services or a severe weather event during a pandemic.
- **New threats and risks:** there may be value in blue skies thinking as it is not possible to accurately predict what kinds of entirely new threats or risks may need to be considered, looking further ahead. But frequently, new and even emerging threats and risks are often that manifestation of converging threats and risks being newly enabled. Bank robbery has been around for a long time, but cyber capabilities have provided an entirely new and magnified "attack" vector.

The recent SolarWinds cybersecurity breach is a timely reminder of risk convergence – a sophisticated adversary (likely a nation state) leveraging cyber vulnerability to penetrate a vendor product that is a key supply chain element used by many organizations and institutions across multiple industries.

Ultimately, even while defining scenarios to help test the ability of critical operations to remain within their impact tolerances is a helpful tool, depending on the critical operation in question, there are still characteristics that will make sense to focus specifically on depending on the nature of the service being provided. Examples might include loss of service to online banking, loss of confidential data in private client services, inability to clear transactions, disruption to payment capability, etc.

The key is not to plan for every eventuality, but to be creative in how to consider broad scenarios and broad responses. Senior executives need to be naturally inquisitive, asking questions and exploring lessons learned and what might have been. They need to adapt to circumstances and challenge preconceptions. As we have seen through the COVID-19 pandemic, the definition of infrastructure resiliency has been changing as firms consider resilient responses such as "work from home" to no longer be our "backup" plan, but increasingly as our primary mitigant and response when staff are no longer able to operate from impacted facilities (be that, for example, due to a pandemic, weather event, or terrorist threat).

Without question, when the dust settles from the global COVID-19 pandemic, regulators will only increase their focus on operational resilience. The financial services sector has fared remarkably well, but in addition to considering future scenarios, there is also the opportunity now for firms to consider what lessons can be learned from more recent experiences and adapt accordingly before the heat is turned up further.

9. THE OPPORTUNITY – DIFFERENTIATION THROUGH RESILIENCE

While this paper focuses on regulatory expectations and changing definitions regarding operational resilience, it is important to note that establishing and maintaining operational resilience should be far more an opportunity to positively differentiate than a response to regulatory edict. Resilient firms not only survive but may even thrive in the face of disruption. Firms that embed operational resilience into their business-as-usual can expect substantial ancillary benefits related to not just improved resilience in and of itself, but also to a more cohesive approach and cultural shift. While the immediate concern may be an organization's ability to recover quickly and effectively from a significant disruption, most aspects of a resilient operation are equally relevant to business-as-usual activities, supporting an ability to respond more quickly, more boldly, and with greater confidence to take advantage of opportunities, meet client expectations, and, in some cases, take on more risk secure in the knowledge that their operations can accommodate.

- **Increase client trust and stickiness:** through the COVID-19 pandemic, those firms that have been able to continue to provide essential services reliably and consistently have benefited tremendously. Customers go to the providers they trust, and they will stick with those providers, regardless of industry. Financial services have shown themselves to be robust and reliable, in contrast to the reputational damage experienced during the financial crisis in 2008. A "flight to quality" in a crisis will lead to the most resilient and reliable firms.
- **Better prioritization and allocation of resource:** the process of identifying critical business services and all associated dependencies allows firms to prioritize where to focus and invest to ensure that their "cannot fail" services are well supported and robust. Scenarios and established tolerances help to identify where to invest. A culture of

operational resilience should drive improved identification of the core set of knowledge, resources, and dependencies that is vital to the organization – not just during adversity.

- **Ability to take risk:** where a firm's operational resilience is understood, there is greater confidence to take risk – through innovation, partnerships, outsourcing, and expansion. Knowing the degree to which an organization or business process can bend without breaking is a strategic advantage in decision making. Resilient firms are agile and well positioned to take advantage of opportunities as they present themselves, and able to adapt without fear of breaking along the way.
- **Gain advantage at the exit:** more resilient firms will exit any widespread disruption or crisis in better shape than their less resilient competition. They will be able to focus on core business objectives and gaining market share rather than having to invest to "fix" what broke during the disruption. In a resilient organization, those areas under stress should spring back into place, ready to expand and grow coming out of the period of stress.
- **Better outcomes overall:** understanding operational resilience and ensuring boundaries are understood should allow a firm to be agile and react more quickly and effectively, maintain services through disruption, change suppliers where necessary, expand customer loyalty, and build reputational capital based on how well it has demonstrated its response to crisis. Inevitably, a firm that is operationally resilient will also be more robust under business-as-usual, driving process efficiencies with fewer operational losses during periods of stability as well as under stress.

It stands to reason that in an "always on", immediate gratification world where clients expect 24/7 availability and are able to move quickly from one provider to the next, that those firms who are seen as the most reliable and most dependable when they are needed the most (i.e., in a crisis) will be the most successful. These are the same firms that will best serve clients, markets, and the stability of the broader financial ecosystem.

10. CONCLUSION

The regulatory posture regarding operational resilience has become clearer in recent years and while different regulators have different definitions, the financial services sector has largely settled on a common definition. As firms consider their approach, the regulatory view of "prepare for, respond and adapt to, and recover and learn from" provides a helpful blueprint – as seen in numerous papers from different consulting firms and the language used by regulators when addressing this topic.

As noted, operational resilience should be seen as an evolution and not a revolution – bringing together existing concepts and frameworks from risk management, business continuity, supply chain and third party management, cybersecurity risk, and security and IT resilience. It is important to take a more holistic approach across these functions and disciplines and plan deliberately for periods of heightened stress with clearly defined maximum tolerances within which operational processes need to operate under severe but plausible disruption. These impact tolerances are not the same as a firm's business-as-usual risk appetite, and scenarios can be used to test a firm's ability to maintain service within these tolerances under severe disruption.

It is not assumed that all business services are of an equivalent criticality, so differentiation is required – identifying and defining critical business processes and all associated dependencies, some of which may extend outside of a firm's direct control. This adds additional complexity as traditional boundaries are extended to third and fourth parties. But understanding those dependencies is critical to being able to maintain a resilient end-to-end process for provision of critical services.

Finally, while establishing and maintaining operational resilience for a firm's most critical business processes is not trivial, it does provide substantial long-term benefits and significant competitive advantage. Operational resilience should be a positive differentiator in acquiring and retaining clients – your customers will remember how you responded under stress and should reward you for it.

REFERENCES

BCBS, 2011, "Principles for the sound management of operational risk," Basel Committee on Banking Supervision, https://bit.ly/3tw6fhg

BCBS, 2020, "Principles for operational resilience," Basel Committee on Banking Supervision, https://bit.ly/3shtjQo

FCA, 2018, "CP19/32: Building operational resilience: impact tolerances for important business services," Financial Conduct Authority, https://bit.ly/3raE2es

FRB/OCC/FDIC, 2020, "SR 20-24: Interagency paper on sound practices to strengthen operational resilience," Federal Reserve Board/ Office of the Comptroller of the Currency/Federal Deposit Insurance Corporation, https://bit.ly/3c54fqi

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO