THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

OPERATIONS

Operational resilience:
Industry benchmarking

MATT PAISLEY | WILL PACKARD
SAMER BAGHDADI | CHRIS RHODES

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: INDUSTRY BENCHMARKING

MATT PAISLEY | Principal Consultant, Capco
WILL PACKARD | Managing Principal, Capco
SAMER BAGHDADI | Principal Consultant, Capco
CHRIS RHODES | Consultant, Capco

ABSTRACT

In a series of conversations with financial executives across Canada, we discussed the current state of operational resilience planning and their organizations' plans for the future. The primary challenges mentioned were a high dependency on third (and fourth) party providers, increased organizational complexity, getting appropriate buy-in and focus across the organization, and regional variations in regulatory requirements. To address these challenges, and heighten their resilience, organizations are finding and pursuing several opportunities, which include mechanisms for identifying and prioritizing their critical services, as well as leveraging a global workforce to provide distributed capabilities. Organizations also discussed approaches for dealing with differing regulations globally. In terms of resilience structure, organizations have looked at their governance frameworks and ensuring they are fit for purpose, as well as utilizing stress and scenario testing to assess their capabilities. An effective training program underpins a solid resilience plan, and organizations discussed their approaches here as well. In a mid- to post-pandemic world, an effective resilience strategy has been, and will continue to be, integral to the success of financial institutions. The current environment provides a compelling reason for firms to bolster their capabilities.

1. INTRODUCTION

Early one Monday morning in July, one of Singapore's biggest banks was alerted to an outage that had taken its systems – including ATMs – completely offline. Escalation and response were prompt, and by 10am the systems were restored. By this time, however, the outage had caught the attention of the Monetary Authority of Singapore (MAS), the country's central bank, which indicated that subsequent action was required to strengthen the system, and supervisory action could be taken where necessary.[1] Investigations proceeded with the bank's main IT vendor, whose resiliency systems had been expected to prevent these types of failures.

The Singapore event highlights some of the challenges financial institutions are facing today as they prepare their operational resilience plans. Organizations and systems are increasingly complex and interconnected; additionally, many organizations have dependencies on several third and fourth party service providers, whose own resilience preparations can directly impact recovery from an event. Client tolerance for downtime continues to diminish, and through the megaphone of social media, resilience incidents can have a material impact on reputation and brand.

We spoke with several financial institutions, industry bodies, and regulators across Canada to understand their perspectives on the challenges, and the paths they were pursuing to

[1] Reuters, 2010, "Singapore bank suffers massive IT failure," July 6, https://reut.rs/3cEOG7E

address them, as it relates to operational resilience. From those discussions certain themes emerged that paint a picture of the road to resilience, including both the challenges that financial institutions regularly face and some of the proactive measures put forth.

2. CHALLENGES

During our conversations, we heard a variety of challenges and priorities that are top of mind among financial executives. A few specific themes emerged, consistently coming up in conversations as focus areas across the industry.

2.1 High dependency on third and fourth party providers

The standout response among the banks and regulatory bodies interviewed was the inherent difficulties in managing supply chain risk. It was widely acknowledged that organizations increasingly rely on an often complex and expansive web of third party providers, whether to support the delivery of a critical service or, in some cases, even deliver the critical service in its entirety.

The specific challenges raised are two-fold. The first is simply understanding what external dependencies exist. Not only do organizations need to understand their internal workings inside out to effectively identify critical activities, but they also need to understand how each of these activities are unpinned by third party suppliers. Considering the size and scale of financial institutions, this is no simple task, and yet more complexity is added by the fact that supply chains are multi-layered. Organizations must look beyond the contractual supplier and ask the question: Who are my suppliers' suppliers? Introducing fourth party service providers considerably expands the scope of the supply chain, making it increasingly difficult to truly understand an organization's external dependencies, and their path to recovery.

The second challenge identified relates to how external parties are included within an organization's resilience program. In most cases, the resilience programs discussed are in their relative infancy, so it is not surprising that external party involvement has not been a priority, particularly given the challenges of gaining internal buy in. However, it was widely emphasized that given the importance of external parties, they must be involved going forward. Among the ways mentioned to do this is the inclusion of external parties in resilience tests and exercises. Other practices include the use of resilience audits to ensure suppliers have adequate internal controls in place, including resilience requirements within the procurement process and contractual terms. Additionally, viable alternative suppliers and workarounds must be identified in case of service interruption or unavailability.

2.2 Increased organizational complexity

Most organizations acknowledged that their aim is to have an enterprise-wide, holistic resilience program in place, but that, in reality, this is not easily achieved. Particularly for banks, implementing any centralized initiative is challenging considering the complex organizational structures, distributed IT architecture, and global footprint. In many cases, current resilience planning is siloed, limited to specific lines of business, teams, or even particular systems. Business continuity planning has focused on specific business areas without consideration for the wider impact and internal dependencies across the organization. Testing has also been restricted, focused on technical recovery of a specific system, rather than a cohesive, multifaceted response to a disruption. The challenge, therefore, is to understand how to govern resilience planning from the top down, ensuring an appropriate level of consistency and cooperation across the organization.

2.3 Getting the right focus

To have an enterprise program, buy-in from varied groups is essential. For most organizations, it was noted that operational resilience is a top priority with reasonable attention given at C-suite and board level. One organization noted that cybersecurity gets priority focus at the top level, and this ripples through the enterprise. For most organizations, though, getting the right level of focus on resilience across the organization was viewed as a key challenge. As noted above, in some cases efforts are siloed, and enhancements in one area do not cascade to, or consider the impact on, other parts of the business.

A regulatory body highlighted the challenges of moving beyond a traditional focus on business continuity, and moving towards a more holistic perspective that resilience brings. Resourcing was also viewed as a challenge, where very few organizations have staff explicitly dedicated to operational resilience. Instead, responsibility is folded into the remit of existing risk or technology teams. Where funding was not deemed to be an immediate challenge, it was recognized that as the program looks to mature, increasing investment is required. The ever-present issue of competing priorities was also noted as a challenge.

2.4 Differing regulatory expectations

Accommodating different regulatory requirements and expectations is a challenge for all financial organizations operating across multiple sectors and jurisdictions. This is no different when it comes to operational resilience. Regulations, or at least regulatory guidance, around resilience is relatively new and for that reason there is no blanket alignment across global regulators. For example, looking at the consultation papers issued by the U.K. regulators (Prudential Regulatory Authority and Financial Conduct Authority) and the Basel Committee on Banking Supervision (BCBS), as well as the guidance provided by the U.S. regulators (Federal Reserve Board, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation), it is clear that there are key differences among them. The U.K. paper introduces new regulations applicable to all relevant regulated entities, with the key focus being to minimize disruption to customers. The BCBS paper sets out principles for operational resilience but differs from the U.K. paper in that there is no requirement to set impact tolerances in terms of impact on customers, a key priority for U.K. regulators. The U.S. paper serves as guidance applicable to only the largest U.S. organizations, with the key focus being to limit financial impact to the organization itself and preserve national financial stability.

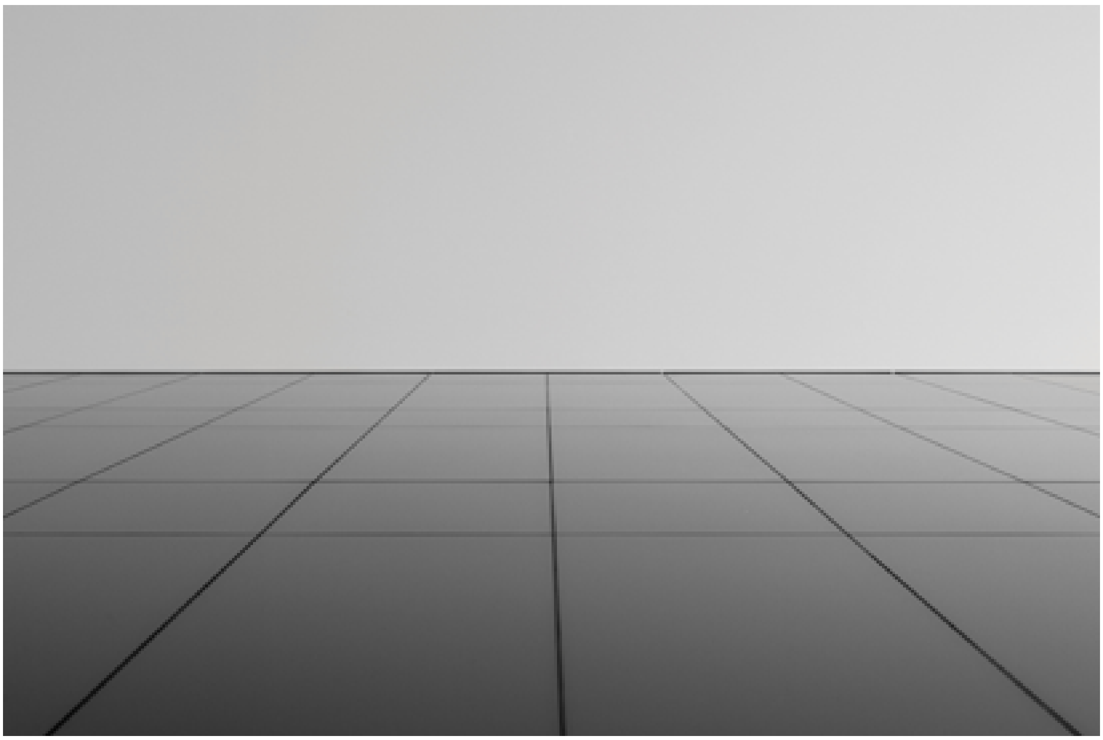
Such differences create a clear challenge for organizations looking to implement an enterprise-wide approach to resilience. Firms have addressed these in differing fashions, as described in more detail below.

3. APPROACHES TO RESILIENCE

As financial institutions continue to navigate the aforementioned challenges and operate in an ever-evolving landscape with increased barriers, it will be imperative to focus on operational resilience and strengthen required controls to stay ahead. Throughout our conversations, we found the following areas to be of particular interest to financial institutions in their efforts to create more resilient operations.

3.1 Identifying and prioritizing critical services

Organizations have implemented various processes for identifying and prioritizing critical services as best fits their operations. For transactional services, this can involve using a defined schema that categorizes functions based on volume and value; for example, prioritizing services relating to high-volume, high-value payments to ensure these continue uninterrupted. In other cases, organizations start from a scenario basis and look at the client impact – for both internal and external clients – to evaluate what services cannot be



interrupted without impacting the client experience. This can include a review of business objectives, applying a risk lens to ensure critical services fall within the organization's risk appetite. This can also be overlaid with traditional business continuity planning (BCP) and planning based on recovery time objectives (RTOs). In other cases, organizations have prioritized corporate service processes as critical to ensure their employees and bills are paid on time with minimal disruption.

It is important to consider timing when determining priority. Tax processing, for example, can have a materially different impact if taken offline the day before filing; on a random weekday mid-year, it may be less critical for immediate recovery.

For new process and technology development, organizations are looking to build-in operational resilience. While there will continue to be legacy processes that require resilience built around them after the fact, having a resilience mindset heading into the design and implementation phases can reduce the effort required to harden.

The perspective of U.K. regulators on this matter is worth noting. U.K. regulators have mandated that in-scope firms identify "important business services" based on harm to customers, market stability and integrity, and soundness of the firm. While the methods discussed in our interview series touched on one or more of these elements, there is an opportunity for organizations to approach resilience more holistically as best practice.

3.2 Increasing resilience through global workforce

For financial institutions, staff are increasingly dispersed, be it in separate cities or different continents. For most organizations we spoke with, this is a net positive for resilience: while there are productivity impacts where rapid and regular collaboration is required, having a distributed workforce means that critical processes can be more readily shifted to other locations as needed. One organization shifted workload to other countries in adjacent time zones, during social unrest in one country, and minimized customer impact that way.

One of the unexpected impacts of the pandemic has been the rapid scaling of remote work capabilities, with its associated resilience benefits. As some clients noted, a pandemic is not necessarily a resilience test, given the advanced warning and limited impact to critical infrastructure, but it has allowed organizations to prove out their capabilities to continue operating as normal even when denied access to their primary place of business.

3.3 Managing regional regulatory requirements

The regulatory requirements for resilience planning can be materially different between regions and this requires careful planning. In some cases, regulatory changes in a region can impact organizations even if they have no footprint there; for example, European General Data Protection Regulation (GDPR) applies to organizations touching protected data, regardless of where they are in the world. Handing over functions, and the associated data, across regions during an event can have cascading implications for organizations' regulatory obligations.

In this complex and interconnected environment, aligning with regulatory obligations across regions is increasingly important. One way in which to address this, as noted by several banks, is to establish a minimum base standard across global programs, meeting the requirements set out by all relevant regulators. For cybersecurity, the Payment Card Industry Data Security Standard (PCI DSS) has been highlighted as a model that is scalable, while also detailed enough to provide practical points of action.[2]

In Canada, the Office of the Superintendent of Financial Institutions (OSFI) is engaging with Canadian banks to observe their operational resilience efforts during the significant disruption that has arisen because of the COVID-19 pandemic. Banks should consider having clear ownership and accountability within different levels of their organization to strengthen operational resilience; primarily by identifying and prioritizing critical business services. Evidence collection of frequent testing on critical services is an area that may see increased attention to ensure resilience is being highlighted and embedded in daily operations.

[2] Available in the PCI document library: https://bit.ly/30XN186

Furthermore, transparency and communication with governing bodies is important to provide visibility on the steps taken to comply with both the letter and the spirit of the regulation.

3.4 Strengthening governance frameworks

Resilience governance, both as it relates to the identification and prioritization of critical services and resilience standards or requirements, does not seem to fall under a single banner at the enterprise level within most organizations. In some instances, governance falls under IT (mostly IT resilience) and in others it falls under operational risk teams (operational resilience). Involvement from executive management (C-suite) has been present in most organizations, with a split ownership between the chief risk officer and the chief information/technology officer, including an acceptable level of engagement and collaboration.

General guidance from the regulators has been to introduce operational resilience accountability at various levels, while owned by the C-suite and approved and governed by the board, to ensure effective implementation and challenge where required. In most organizations, the board has clear visibility to operational resilience, but would benefit from increased key performance indicator (KPI) and key risk indicator (KRI) reporting specific for resilience.

3.5 Maturing critical services through stress and scenario testing

Testing programs, specifically as part of disaster recovery, have been a focal point for financial institutions in strengthening their resilience. General agreement within the industry is that testing at all three lines of defense, where applicable, contributes to building maturity and allows for identifying issues and challenges early on. Stress and scenario testing for critical business services has been a priority for all financial institutions as advised by regulatory bodies, nationally and globally.

However, scenario testing needs to continue to evolve and be completed as part of identifying and prioritizing critical businesses, and to ensure resilience and sustainability of services is top of mind for management and the board as part of the overall enterprise risk governance framework. Collaboration between business and technology teams in conducting tests will be increasingly important. While scripted testing for system failures can be appropriate, the outcomes of those tests and the implied impact should also feed scenario planning.

3.6 Empowering employees through required training

A key part of an effective recovery strategy is ensuring employees have their marching orders well in advance of an event. This is complicated by people regularly moving into new positions. Since many teams may see a sizeable change in their makeup within a few years, regular training refreshers are key. With an average C-suite tenure of approximately five years, the people who managed through one crisis event (and the lessons they learned in that crucible) will likely have moved on for the next event.

Having executive and C-suite buy-in and support for this training is vital. Some organizations used simulations, where technically feasible. Many teams ran tabletop exercises, where a scenario is played out and people discuss what their response would be, and the impact of those decisions. Running these drills as close as possible to reality, with diversity in approach, helps make them more memorable and the lessons more readily applicable. As one participant noted, overly scripted testing is like "training everyone with a dog biscuit" – they all respond in a certain way, which does not necessarily align with reality in a crisis.

4. CONCLUSION

A business resilience executive at a global investment bank once confided, "I expect to have six months after a crisis to get my wish list prioritized and delivered. After that, memories fade, and focus and budgets go elsewhere."

Practically, every organization we spoke to – both industry participants and regulators – indicated that operational resilience was a top priority of theirs. Additionally, one of the challenges consistently mentioned was getting mindshare and budget to effect change in this area. The global pandemic has both elevated the priority of resilience and lent tremendous focus to the topic. While the pandemic has provided a proving ground for the industry's resilience plans, it has also presented an opportunity to identify gaps and prioritize improvements. Most organizations have wish lists of their own to implement, and the iron is hot for the striking.

In the words of Peter Grant from the Canadian Securities Transition Office (CSTO), "Never let a crisis go to waste… if there was ever a time to make a case for improving resiliency, COVID is it."

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

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C001648

WWW.CAPCO.COM

CAPCO