THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

OPERATIONS

Operational resilience approach

MICHELLE LEON | CARL REPOLI

20
YEAR ANNIVERSARY

OPERATIONAL RESILIENCE

#53 MAY 2021

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

Editor
Shahin Shojai, Global Head, Capco Institute

Advisory Board
Michael Ethelston, Partner, Capco
Michael Pugliese, Partner, Capco
Bodo Schaefer, Partner, Capco

Editorial Board
Franklin Allen, Professor of Finance and Economics and Executive Director of the Brevan Howard Centre, Imperial College London and Professor Emeritus of Finance and Economics, the Wharton School, University of Pennsylvania
Philippe d'Arvisenet, Advisor and former Group Chief Economist, BNP Paribas
Rudi Bogni, former Chief Executive Officer, UBS Private Banking
Bruno Bonati, Former Chairman of the Non-Executive Board, Zuger Kantonalbank, and President, Landis & Gyr Foundation
Dan Breznitz, Munk Chair of Innovation Studies, University of Toronto
Urs Birchler, Professor Emeritus of Banking, University of Zurich
Géry Daeninck, former CEO, Robeco
Jean Dermine, Professor of Banking and Finance, INSEAD
Douglas W. Diamond, Merton H. Miller Distinguished Service Professor of Finance, University of Chicago
Elroy Dimson, Emeritus Professor of Finance, London Business School
Nicholas Economides, Professor of Economics, New York University
Michael Enthoven, Chairman, NL Financial Investments
José Luis Escrivá, President, The Independent Authority for Fiscal Responsibility (AIReF), Spain
George Feiger, Pro-Vice-Chancellor and Executive Dean, Aston Business School
Gregorio de Felice, Head of Research and Chief Economist, Intesa Sanpaolo
Allen Ferrell, Greenfield Professor of Securities Law, Harvard Law School
Peter Gomber, Full Professor, Chair of e-Finance, Goethe University Frankfurt
Wilfried Hauck, Managing Director, Statera Financial Management GmbH
Pierre Hillion, The de Picciotto Professor of Alternative Investments, INSEAD
Andrei A. Kirilenko, Reader in Finance, Cambridge Judge Business School, University of Cambridge
Mitchel Lenson, Former Group Chief Information Officer, Deutsche Bank
David T. Llewellyn, Professor Emeritus of Money and Banking, Loughborough University
Donald A. Marchand, Professor Emeritus of Strategy and Information Management, IMD
Colin Mayer, Peter Moores Professor of Management Studies, Oxford University
Pierpaolo Montana, Group Chief Risk Officer, Mediobanca
John Taysom, Visiting Professor of Computer Science, UCL
D. Sykes Wilford, W. Frank Hipp Distinguished Chair in Business, The Citadel

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 APPROACH

MICHELLE LEON | Managing Principal, Capco[1]
CARL REPOLI | Managing Principal, Capco

ABSTRACT

Operational resilience has risen to the top of board agendas due to ever-increasing customer expectations and the ever-expanding threat landscape of digital disruption, cyber attacks, third party risk, climate change, and geopolitical unrest. Boards and senior management of financial services firms are increasingly focused on reducing the likelihood and impact of disruptions to their business and customers, as well as on continuously delivering services when incidents occur. Moreover, regulatory scrutiny on resilience has intensified as the U.K. supervisory authorities, the U.S. agencies, and the Basel Committee have issued their expectations for improving the resilience of financial services firms. The current environment means that enterprise resilience is an imperative, not a choice. Organizations must approach operational resilience with a holistic strategy and enhanced competencies so that they can support their customers, protect their reputation, and remain competitive. This paper defines operational resilience, explains why adopting a resiliency lens is critical, and outlines the regulatory guidance on resilience. It also describes the steps that organizations should take to achieve and sustain operational resilience, including the set up and maintenance of an operational resilience program.

1. INTRODUCTION

1.1 Background

Operational resilience is the ability of a firm to deliver critical operations and services through disruption. This ability enables a firm 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 services and operations through disruption.[2] Enhancing capabilities to strengthen operational resilience is critical for firms to remain competitive, maintain market confidence, and support financial stability, particularly as customers and market participants expect firms to deliver continuous service. Operational disruptions and the unavailability of important business services have the potential to cause extensive harm to consumers and market integrity, threaten the viability of firms, and cause instability in the financial system. With business disruptions on the rise – including cyber attacks and the resulting outages outages, natural disasters, pandemics, and critical service provider failures – improving operational resilience is a board-level priority across the financial services industry.

Operational disruptions to the products and services that firms/financial market infrastructures (FMIs) provide have the potential to:

- Cause harm to consumers and market participants
- Create instability in the financial system
- Threaten the financial viability of firms/FMIs.

To mitigate harm to clients, the stability and integrity of the market, and firm financial viability, organizations should adopt a resiliency lens when defining strategies to maintain the provision of critical business services. A resiliency perspective recognizes the increased complexity of the environment in which financial institutions operate and the associated challenges of protecting the customer, as well as maintaining the safety and soundness of the firm and the financial system.

[1] We would like to thank Capco's So Jene Kim, Michael Martinen, and Will Packard for their helpful comments on this article.
[2] Bank of England, 2018, "Building the UK financial sector's operational resilience," Bank of England Discussion Paper No. DP01/18, July, https://bit.ly/3spj6kO

Such a broader view requires a shift from a functional to an end-to-end service and customer perspective across the value chain, considering the overall financial ecosystem. As the scope of operational resilience is extensive and encompasses many different areas (e.g., business continuity, cyber and information security, incident management, operational risk, and vendor management), firms will need to integrate siloed activities and establish a cross-functional view for resiliency.

A high-level approach to achieving operational resilience comprises the following three key components:

1. **Preparing for the inevitable:** identify the critical business services offered to customers, set impact tolerances for the critical business services, and map the supporting resources that deliver the services.

2. **Managing the response:** identify, assess, and remediate potential vulnerabilities at each step of the mapped processes. Take corrective action to ensure each service can be managed within its impact tolerance level if and when an event occurs.

3. **Learning:** evaluate the effectiveness of operational resilience measures by conducting scenario testing to assess the firm's response to severe but plausible scenarios. Further remediate identified vulnerabilities where impact tolerances are consistently breached and conduct regular self-assessments that are available to regulators upon request. Role-specific training should be incorporated into annual training programs, as required.

1.2 Regulatory requirements

As of the development of this article, three key regulatory papers related to operational resilience have been released across the U.S. and Europe to define the meaning of operational resilience and articulate the requirements of a strong operational resilience program.

1.2.1 COMMON THEMES ACROSS REGULATORS' APPROACHES TO OPERATIONAL RESILIENCE

Common themes on operational resilience are emerging from major supervisory authorities around the world, providing a foundation for firms/FMIs to establish a compliant and effective operational resilience program. The core regulatory expectations for operational resilience currently include:

- **Governance:** board and senior management buy-in and oversight of operational resilience program execution are imperative for firms to operate in a safe and sound manner and to comply with applicable laws and regulations. Operational resilience governance arrangements can be embedded into existing governance structures to oversee resilience strategies and their efficacy.
- **Mapping of critical services:** the ability to comprehensively understand critical business services and map their interconnectedness/dependencies with supporting internal resources and external service providers is fundamental to achieving operational resilience.
- **Continuous improvement:** existing operational resilience guidance emphasizes vulnerability assessments and scenario testing to demonstrate that critical services can remain within impact tolerances during severe disruptions. Outcomes from these exercises and regular self-assessments can be used to mature and maintain effective operational resilience.
- **Security:** secure and resilient information systems underpin the operational resilience of a firm's critical operations and core business lines. Regulators expect firms to ensure resilient information and communications technology, including cybersecurity, to support and facilitate delivery of critical business services.

2. OPERATIONAL RESILIENCE METHODOLOGY

2.1 Identification and mapping of critical business services

A business service is a service that a firm provides to an external customer, end user, or participant. Business services deliver a specific outcome or product. Resilient business services support financial stability against disruptions that could significantly harm consumers/market participants and threaten the firm's viability or broader sector stability.

The supervisory authorities believe that firms'/FMIs' boards and senior management should focus on the operational resilience of their most critical business services and the resources required to deliver those services. The supervisory authorities' view set out in the U.K. regulators' discussion paper is that business services will be considered critical when their failure could cause an intolerable level of harm to consumers or market participants, harm to market integrity, or threaten the safety and soundness of individual firms or financial stability.

The regulatory authorities propose the following factors that firms should consider when identifying their critical business services:

1. A consideration of those potentially affected by disruption to the service (likely to cause consumer harm):
   - Size and nature of the consumer base, including vulnerable consumers who are more susceptible to harm from a disruption
   - Ability of consumers to obtain the service from other providers (substitutability, availability, and accessibility)
   - Time criticality for consumers receiving the service
   - Sensitivity of data held in the instance of a breach.
2. A consideration of impact on the firm itself, where this could cause consumer harm or harm to market integrity:
   - Impact on the firm's financial position and potential to threaten the firm's viability

Table 1: Key regulatory requirements

	U.K. REGULATORY APPROACH TO OPERATIONAL RESILIENCE	BASEL COMMITTEE'S PRINCIPLES FOR OPERATIONAL RESILIENCE	U.S. REGULATORY GUIDANCE ON OPERATIONAL RESILIENCE
REGULATOR	• Prudential Regulation Authority • Financial Conduct Authority • Bank of England	• Basel Committee on Banking Supervision (BCBS)	• Board of Governors of the Federal Reserve System (FRB) • Office of the Comptroller of the Currency (OCC) • Federal Deposit Insurance Corporation (FDIC)
SUMMARY	• Places operational resilience on equal footing to financial resilience. • States that firms/FMIs need the ability to prevent disruption occurring to the extent practicable; adapt systems and processes to continue to provide services and functions in the event of an incident; and return to normal functioning promptly. • Explains that learning and evolving from both incidents and near misses is critical to building a forward-looking program. • Expects implementation to be proportionate to the nature, scale, and complexity of the organization.	• Builds upon existing guidance and current practices. • Signals the increasing regulatory shift from financial to operational resilience given the impact of the coronavirus. • Sets forth practices that should be integrated into the bank's forward-looking operational resilience program in line with its operational risk appetite, risk capacity, and risk profile. • Proposes a pragmatic, principles-based approach to operational resilience that will facilitate proportional implementation across banks of varied size, complexity, and geographical location.	• Directed to the largest and most complex domestic firms that have average total consolidated assets greater than or equal to: (a) U.S.$250 billion, or (b) U.S.$100 billion and have U.S.$75 billion or more in average cross-jurisdictional activity, average weighted short-term wholesale funding, average nonbank assets, or average off-balance-sheet exposure. • Brings together existing regulations and guidance to develop a comprehensive approach to operational resilience. • Highlights the importance of operational resilience with respect to firms' critical operations and core business lines.
KEY CONCEPTS	The U.K. regulatory authorities recommend the following key components to improve the operational resilience of firms and the overall financial sector: • Identification of important business services that could cause harm to consumers, market integrity, or firm viability if disrupted. • Mapping of the people, processes, technology, facilities, and data that support important business services. • Setting of impact tolerances for each important business service. • Scenario testing to remain within impact tolerances. • Identification and remediation of vulnerabilities. • Lessons learned exercises for continuous improvement. • Internal and external communication plans in the event of disruption. • Self-assessment document outlining the state of operational resilience.	The BCBS' principles of operational resilience are organized across the following categories: • Governance. • Operational risk management. • Business continuity planning and testing. • Mapping of internal and external interconnections and interdependencies of critical operations. • Third party dependency management. • Incident management. • Resilient information and communication technology (ICT), including cybersecurity.	The following pillars underpin the U.S. agencies' approach to operational resilience: • Effective governance. • Robust operational risk management. • Business continuity management. • Third party risk management. • Rigorous scenario analysis. • Secure and resilient information system management. • Ongoing surveillance and reporting.

  - Potential to cause reputational damage, legal or regulatory censure.

3. A consideration of the impact on the country's financial system (likely to cause harm to market integrity):
  - The firm's potential to impact the soundness, stability, or resilience of the country's financial system and its potential to inhibit the functioning of the country's financial system
  - Importance of that service to the country's financial system, which may include market share, sensitive consumers, and consumer concentration.

Critical business services should be identified and mapped across functions to a sufficiently granular level so that an impact tolerance can be applied and tested. Mapping of critical business services should allow firms to:

- Identify and remedy vulnerabilities in the delivery of critical business services within an impact tolerance
- Enable firms to test and demonstrate their ability to remain within impact tolerances across a range of severe and plausible scenarios.

The supervisory authorities also require firms/FMIs to consider the chain of activities that make up a business service and determine which part of the chain is critical to delivery. The supervisory authorities propose that all resources that are required to deliver that part of the service should be operationally resilient. A business services approach is, therefore, an effective way of prioritizing improvements to systems and processes: looking at systems and processes based on the critical business services they support will bring more transparency to, and improve the quality of, decision-making for operational resilience.

2.2 Identification and mapping of associated critical resources

The regulatory authorities highlight that an operationally resilient firm would be expected to have a comprehensive understanding and mapping of the systems and processes that support its critical business services. This includes those systems and processes over which the firm may not have direct control, such as outsourcing and third party service providers.

To have a complete view of their resilience and the risks relevant to their critical business services, firms will need to identify and map/document the resources – people, processes, technology, facilities/locations, information, and business cycles (e.g., key deadlines) – necessary to deliver each critical business service.

By identifying and mapping operational dependencies and key interactions that provide the critical business service, firms can pinpoint where disruptions could have the greatest impact, determine how best to support their resilience, and develop more effective contingency or business continuity plans.

2.3 Definition of impact tolerances

The U.K. regulators' discussion paper defines impact tolerances as "tolerance for disruption, under the assumption that disruption to a particular business service will occur." Impact tolerances could be expressed by specific outcomes and metrics, including the maximum tolerable duration or volume of disruption, number of transactions, or the number of customers affected. Other factors that a firm should consider when setting its impact tolerances include, but are not limited to:

- The potential financial loss to clients
- The potential financial loss or level of reputational damage to the firm where this could harm the firm's clients or pose a risk to the soundness, stability, or resilience of the overall financial system or the orderly operation of financial markets
- The potential impact on market or consumer confidence
- Any potential loss of confidentiality, integrity, or availability of data.

The purpose of setting impact tolerances is to provide clear metrics so that management knows the level of resilience it needs to build for the firm's critical business services. Additionally, these metrics identify harm to consumers or market participants, harm to market integrity, and threat to firm safety and soundness or overall market financial stability. All impact tolerances should include the maximum tolerable duration of such disruption, taking into account the importance of the critical business service.

The supervisory authorities expect that a firm/FMI would be able to explain how the particular impact tolerance has been determined for an critical business service, how it relates to the supervisory authorities' objectives, and in which scenarios a breach of impact tolerances could be acceptable. These are likely to be limited to the most severe but plausible scenarios.

2.4 Scenario testing

The regulatory authorities recommend that firms test their ability to remain within their impact tolerances for each of their critical business services in the event of a severe but plausible disruption of their operations. This enables firms to be assured of the resilience of their critical business services and identify where they might need to act to increase their operational resilience. In carrying out the scenario testing, firms should identify an appropriate range of adverse circumstances varying in nature, severity, and duration relevant to their business and risk profile. They should then consider risks to delivery of the firms' critical business services in those circumstances.

Impact tolerances assume a disruption has occurred. Testing should, therefore, focus on the response and recovery actions firms would take to continue the delivery of a critical business service during/after a disruption. Understanding the circumstances under which it is not possible to stay within an impact tolerance for a particular critical business service will enable firms to identify resilience gaps and assess the actions they may need to take to increase their operational resilience.

When setting scenarios, firms should consider previous incidents or near misses within their organization, across the financial sector, as well as in other sectors and jurisdictions. Firms should also consider "horizon risks", such as evolving cyber threats, technological developments, and business model changes, in addition to the scenario examples below:

- Corruption, deletion, or manipulation of data critical to the delivery of critical business services
- Unavailability of facilities, key people, and third party services that are critical to the delivery of critical business services
- Loss or reduced provision of technology underpinning the delivery of critical business services.

The regulatory authorities also propose that in conjunction with developing testing plans, firms should conduct lessons learned exercises. This is important as continuous improvements to operational resilience require firms to learn from experience as their operations and technology change and their approach matures over time. Firms should remediate deficiencies identified through scenario testing or through practical experience and prioritize actions to address the risks posed by each deficiency.

3. PROGRAM OVERVIEW

3.1 Program objectives

The aim of an "operational resilience program" is to ensure that the approach agreed by the board on operational resilience is executed in the relevant areas of the organization; this involves both the set up of the program initially and its sustainability over time. It should lay out the approach, determine roles and responsibilities, as well as define controls around operational resilience. It should also indicate interlocks with other areas of the firm.

3.2 Roles and responsibilities

Accountability for operational resilience spans various functions. Continuity and resilience-related activities are often disparate and unconnected with activities across business continuity, disaster recovery, cyber-incident response, and crisis management. Few crisis and contingency plans are connected or have common/consistent triggers for escalation and decision-making.

To develop a more cohesive strategy that straddles the many disparate groups and plans, it is important to centralize the organization's resilience functions with specific resilience-related roles and responsibilities.

C-level responsibility for operational resilience as a topic:

- Acts as a link to the risk committee of the board
- Keeps the board abreast of operational resilience events and preparation
- Ensures that sufficient resources are made available to ensure that delivery processes are resilient.

This responsibility should be assumed by the COO with input from the CRO, as operational resilience involves steps to reduce the firm's vulnerability to potentially disruptive events and to respond to disruptions once they occur. The COO is the appropriate individual as the elements required to action operational resilience lie within the COO's scope of responsibility.

The **"operational resilience lead"** manages the "operational resilience program" and is accountable for program delivery; represents operational resilience in various committees reviews new business services from an operational resilience perspective; coordinates the annual self-assessment review

process; maintains the operational resilience methodology – e.g., inventory of critical business services/resources and impact tolerances; and links operational risk threat assessment with BCP planning around impact analysis recovery.

The **"critical service delivery process lead"** manages part of the delivery process (this is not an additional FTE); fully understands the end-to-end process and the inter-relationships and dependencies between process components; engages with the relevant areas within third parties in the delivery process; coordinates the recovery of the process if it is disrupted; is responsible for regularly rehearsing the recovery of the process to ensure all components work; and approves changes to the delivery process elements (e.g., critical services/resources, impact tolerances) from an operational resilience perspective.

To support implementation of an effective cross-functional operational resilience program, key program stakeholders should be identified across the functional areas in each stakeholder segment:

- **Executive sponsors (CRO, COO):** drive engagement at the executive committee level, approve program vision, drive critical decisions, and support program funding and prioritization.
- **Program leads (risk lead, operations lead):** establish and deliver program vision; responsible for day-to-day delivery of operational resilience program and for providing key updates and communications to internal governing bodies and external regulatory stakeholders.
- **Working group (workstream leads, members across operations and risk):** is responsible for ensuring that key aspects of implementation program build-out (including identification of critical services, establishing impact tolerances, and reporting) are structured into workstreams. Working group members will assume some business-as-usual responsibilities for operational resilience as well.
- **Delivery/project team (program and project management, business analysts, and other supporting resources aligned to various workstream leads):** drive the program implementation, aligning with change management standards for program execution, including support of workstream deliverables and documentation requirements.
- **Functional subject matter experts (SMEs) (regulatory relations, internal audit, data, capital management, cyber risk, BCM, and others as needed):** provide ad-hoc input and participation in program forums to understand downstream and upstream impacts of operational resilience program decisions.

3.3 Governance and oversight structure

The firm should structure oversight of operational resilience in a way that is effective and proportionate to its business, using existing committees where possible. The regulatory authorities expect clarity on who is responsible for what in the firm regarding operational resilience. A key principle of managing operational resilience is leadership: leaders are required to ensure they have sufficient clarity on how services are delivered. The board and senior management should be engaged in setting effective standards for operational resilience, as well as establishing the business and risk strategies and the management of the main risks relevant to operational resilience.[3] The regulatory authorities also require that the board has sufficient knowledge, skills, and experience to provide constructive challenge to senior management as part of its oversight responsibilities.

The board should take an integrated, end-to-end approach to identify and prioritize the firm's most critical products, services, and assets, considering a broader set of factors than traditional profit and loss or compliance. To demonstrate effective oversight of operational resilience within the firm, the board should be able to provide evidence that it is satisfied that the firm is meeting its responsibilities with respect to operational resilience. This includes the identification of critical business services, the mapping and setting of impact tolerances, as well as the firm's ability to remain within these tolerances.

While operational resilience outcomes are the responsibility of management, service owners, and risk owners, there should be a central point of responsibility and ownership for the operational resilience framework. The operational resilience organization should be a dedicated first line function where the business-as-usual resilience program can be anchored. A program that operates within the first line with second line coordination and oversight would be an effective means of delivering resilience.

[3] Financial Conduct Authority, 2019, "Building operational resilience: impact tolerances for important business services," and feedback to DP18/04, December https://bit.ly/3sDUrsZ

Although a centralized operational resilience team is our recommended approach, some banks have started their operational resilience journey with a federated model: teams across the enterprise – e.g., the lines of business, operations, IT, cybersecurity, business continuity management, vendor management, compliance, etc. – perform their respective resilience responsibilities, such as identify and map their critical services. If a federated operating model is used, the organization will need to establish an effective interaction/engagement model that integrates the teams' resilience activities and enables a cohesive resilience strategy across the enterprise.

3.4 Implementation roadmap

Implementation of the operational resilience program should be coordinated and integrated with such complementary activities/programs as:

- Business continuity
- Disaster recovery
- Incident management
- Cyber-incident response
- Crisis management
- Issue management.

A cohesive, overarching strategy will need to be developed to centralize these activities under an operational resilience umbrella to ensure a holistic resilience vision for the firm. The key challenge is reconciling varying taxonomies, criteria, and approaches across inter-related programs and activities: these differing perspectives need to be pulled together to provide a unified view of resilience risks and capabilities across the organization.

Implementation of an enterprise operational resilience program will comprise the following activities:

- Refine key process methodology to align with operational resilience guidance on critical business services
- Set clear standards and impact tolerances for disruption to the critical business services
- Map the underpinning resources (people, systems, processes, data, vendors) that support critical business services, assessing how the failure of an individual system or process could impact the business service
- Refine scenario definition and testing for severe but plausible scenarios to ensure that the firm can continue or resume business services when disruptions occur
- Structure the oversight of operational resilience, considering a central point of responsibility and ownership for the operational resilience framework
- Augment internal communication plans, escalation paths, and training to incorporate an operational resilience lens
- Enhance specific external communication plans for critical business services to provide prompt and meaningful information to customers, other market participants, and the supervisory authorities
- Develop an annual self-assessment to evidence that the firm is meeting its operational resilience responsibilities.

4. PROGRAM OVERVIEW – TRANSITION TO BUSINESS-AS-USUAL

4.1 Program objectives

Leadership is expected to create a program structure and empower the appropriate stakeholders to identify vulnerabilities and limit downstream impacts on customers resulting from operational disruptions.

The operational resilience program objectives are as follows:

- Continuously review and refine impact tolerances based on changes in business direction and operational approach
- Identify vulnerabilities (internal and external) for operational disruptions through a robust monitoring program with clear roles and responsibilities and reporting
- Quickly respond and limit damage to customers and the firm's reputation in the event of an operational incident through a comprehensive communication and escalation structure
- Create a culture of continuous improvement – learning from incidents and adapting in real time – with clear identification, accountability, and ongoing training for key stakeholders
- Reinforce program objectives through supporting documentation (including policies, procedures, and frameworks) and adaptation of existing monitoring and risk programs.

4.2 Roles and responsibilities: implementation and transition to business-as-usual

The three lines of defense model should be leveraged to meet operational resilience requirements across traditional risk stripes, lines of business, risk managers, and internal audit. Additionally, the three lines of defense model reinforces regulator-mandated complementary and independent

functions that ensure compliance with regulatory expectations. Clear distinction of roles and responsibilities across the three lines of defense is critical for the operational resilience program's success.

1. **First line of defense:** implements the operational resilience program. The first line of defense contains the critical service owners (lines of business and functions that execute business processes) responsible for identifying, measuring, monitoring, and controlling risks associated with the function. For the operational resilience program, the critical service owners should refine the identification of critical business services according to harm to customers, harm to the market, and harm to the firm; set impact tolerances for critical business services; evolve process mapping to identify critical resources; identify and remediate any vulnerabilities to critical services and resources; perform scenario testing; complete annual self-assessments of operational resilience; and monitor systemic issues and provide reporting on the efficacy of the operational resilience program within their lines of business or function.

2. **Second line of defense:** standard setters and keepers, responsible for developing, implementing, and maintaining oversight of the operational resilience program. In transitioning to a business-as-usual state, the second line of defense will help to ensure consistency in change management processes and identify downstream impacts on related programs that should be considered as part of operational resilience efforts and decisions. The second line of defense is responsible for independent monitoring of operational resilience and evaluation of first line of defense testing; defining and operationalizing adequate governance and oversight mechanisms, frameworks, and programs to meet operational resilience program objectives; and developing, implementing, and maintaining policies, procedures, and processes for managing the operational resilience program.

3. **Third line of defense:** independently assesses the effectiveness of the operational resilience program and reports results to the board, as required. The third line of defense provides independent testing and validation through the internal audit function.

4.3 Governance and oversight structure

Firms should leverage existing governance structures to embed resilience planning and management principles. Governance arrangements for the operational resilience program should be effective, efficient, and demonstrable, with clear accountability for planning, coordination, and management of the program across the enterprise. In particular, governance arrangements concerning operational elements of the program should be robust with no key person dependencies, and individuals across the entire business, front to back, should be involved in supporting the operational resilience program. Finally, timely metrics are required for the identification of disruption and overall service performance and improvements.

4.4 Policies, procedures, and standards

A firm's operational resilience program should leverage existing process and program documentation to support program build-out. Existing documentation can be updated to reflect operational resilience requirements for implementation and the subsequent transition to business-as-usual. Updates should incorporate key aspects of the operational resilience program, including:

- Identification of critical services and resources
- Setting of impact tolerances
- Tailoring of idiosyncratic scenarios
- Issue response, including reporting, and escalation
- Identification and remediation of vulnerabilities
- Business-as-usual activities (annual self-assessments, trainings, annual refresh of program methodology, training, and reporting).

Firms should also consider adding incremental documentation, including desktop procedures for newly defined operational resilience program roles and activities.

4.5 Training and communication

4.5.1 TRAINING

The regulatory authorities expect that board members and relevant staff have the knowledge and skills necessary for the discharge of the operational resilience responsibilities assigned to them. Firms should, therefore, augment their training programs to integrate operational resilience as follows:

- Design training on operational resilience concepts and regulatory requirements, with applicable exercises on definition of critical business services and resources, determination of impact tolerances, identification and remediation of vulnerabilities, scenario testing, and self-assessment processes.

- Deliver training in formal sessions – either instructor-led or on-demand videos – as well as informal dissemination via email, intranet postings, and staff meetings.
- Conduct an annual operational resilience refresher that covers operational resilience requirements for all staff.
- Provide specialized training for specific roles and responsibilities, such as training for business process owners on mapping and updating critical business services/resources, defining and updating impact tolerances, scenario testing, and remediation of vulnerabilities; business continuity planning team on monitoring and testing operations against defined impact tolerances; and risk and internal audit on the annual self-assessment process.
- Conduct tabletop/simulation exercises using severe but plausible scenarios to test the firm's operational resilience arrangements, demonstrate its capability to respond within impact tolerance levels, and build muscle memory.

4.5.2 COMMUNICATION

Fast and effective communication can help mitigate the harm of operational disruption. The regulatory authorities expect that firms have internal and external communication strategies in place for prompt and meaningful communication arrangements to inform, maintain trust and confidence, and provide clear actions to reduce the anticipated harm caused by operational disruptions.

Firms should evolve their communication strategies in compliance with regulatory expectations, ensuring that the following recommendations from the regulatory authorities are incorporated into their communication plans:

- Communications planning should focus on the who, who to, and the how of getting hold of key people and of contacting operational staff. As part of external communication plans, the firm should consider in advance of a disruption how it would quickly provide important warnings/advice to customers and inform other stakeholders such as regulatory authorities, suppliers, and the press, including where there is no direct line of communication. The operational resilience approach will also need to involve communications specialists and confirm the message and suitability of communications channels (such as website, social media, telephone, and call centers) when operating under adverse conditions.
- Firms should establish defined and rehearsed communication plans and procedures, including consideration of any expected increase in call volumes, website hits, and suspected fraud cases, and understanding of vulnerable stakeholders relevant to the business services affected.
- Communication plans should be tailored to specific scenarios and cover key aspects, such as pre-considered actions for customer redress.
- An important aspect will be to ensure communications are an integral part of overall operational resilience capabilities and subject to the same governance and assurance processes. This will require specific training of communications teams and operational functions, as well as including the communications team in all strategic and operational crisis management activities.

4.6 Reporting and escalation

4.6.1 REPORTING

Operational resilience entails ongoing surveillance and reporting of operational risks and dissemination of that information to the board of directors and relevant stakeholders across the firm. Reporting that is already in place at the board of directors, senior management, and business line levels should be enhanced to support proactive management of operational resilience.

In developing their resilience capabilities, firms should mobilize information resources to create a product/service view that is aligned with the way that customers perceive the firm. Operational resilience challenges executives to demonstrate they understand the delivery details of individual services and their criticality to daily operations and the overall market. To achieve this, leadership should aim for a more integrated, collaborative reporting model that will enable a holistic view of service delivery and operational performance.

Accountable stakeholders should be identified to ensure that reporting on operational resilience is comprehensive, accurate, consistent, and actionable across business lines and services. To this end, the first line of defense should provide reporting on any risks from operational failures and disruptions, non-adherence of critical services to impact tolerances, remediation of vulnerabilities, and performance against other pre-defined resilience program metrics.

Reporting should be provided on a timely basis in both normal and stressed market conditions. The frequency of reporting will reflect the risks involved and the pace and nature of changes in the environment.

The results of monitoring resilience activities/metrics should be included in regular management and board reports (e.g., quarterly risk report), as should operational resilience assessments performed by internal/external audit and risk management.

Operational resilience reports should describe the bank's resilience risk profile, including emerging risks and trends (market and firm-specific) that may pose a threat to the continuity of critical business services. Operational resilience reports should include breaches of the bank's impact tolerances, as well as thresholds, limits, or qualitative requirements; a discussion of key and emerging risks assessed and monitored by metrics; critical insights to proactively identify and manage significant resilience risks and exposures; details of recent internal disruption events and losses (with root cause analysis); and relevant external events or regulatory changes and any potential impact on the bank.

4.6.2 ESCALATION

In managing the disruption from operational failures, it is important for firms to establish a cohesive operational resilience strategy with monitoring arrangements that can quickly alert key stakeholders and decision-makers to a disruption, underpinned by clear escalation pathways. Clearly defined escalation paths enable information flows to decision-makers, all the way up to the board for timely decision-making.

Firms' internal communication plans should also include the escalation paths the firm would use to manage communications during an incident, and identify the appropriate decision makers; for example, the plan should address how to contact key individuals, operational staff, suppliers, and the regulators.

A robust governance structure is critical to enabling effective response by senior executives, who are expected to lead the firm's response to disruptions. Tabletop exercises/simulations should be used to build experience ("muscle memory") among staff, senior management, and the board ahead of real disruptions. The exercises should include enacting the escalation path for effective decision-making.

5. CONCLUSION

Operational resilience has become a key agenda item for boards and executive management of financial institutions. The increasing pace of digitization, complexity and interconnectedness of the financial industry, dependence on third parties, and sophistication of malicious cyber criminals have made disruptions more likely and their impact more severe.

Operational resilience extends beyond traditional business continuity and disaster recovery: it is wider reaching, encompassing many different areas across the enterprise, and necessitating the breakdown of organizational silos. Operational resilience views services from the customer's perspective and, therefore, centers on the dependencies and requirements for providing critical business services end to end. Operational resilience requires a mindset shift away from resilience as a "check-the-box" compliance exercise to resilience as a key organizational capability that is every employee's responsibility to sustain and continuously improve.

Financial regulators have published their expectations on resilience oversight, management, and reporting. In response, firms will need to drive improvements of their operational resilience programs to strengthen their resilience to disruption and incidents across technology, data, third parties, facilities, operations, and people.

Embedding resilience processes into day-to-day management and decision-making makes sound business sense. As firms become increasingly digitized and as they aim to deliver against their 24/7 promise to customers, achieving operational resilience is core to each firm's – and the financial services industry's – success and competitiveness.

© 2021 The Capital Markets Company (UK) Limited. All rights reserved.

This document was produced for information purposes only and is for the exclusive use of the recipient.

This publication has been prepared for general guidance purposes, and is indicative and subject to change. It does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (whether express or implied) is given as to the accuracy or completeness of the information contained in this publication and The Capital Markets Company BVBA and its affiliated companies globally (collectively "Capco") does not, to the extent permissible by law, assume any liability or duty of care for any consequences of the acts or omissions of those relying on information contained in this publication, or for any decision taken based upon 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