CENTRAL BANK OF EGYPT
Egyptian Banking Institute

البنك المركزى المصرى
المعهد المصرفى المصرى

February 2022

Current Trends

Operational Resilience in Banking

www.ebi.gov.eg

February 2022

Current Trends

"In a world where organizations are faced with complex Technology, Cyber, Data and Third Party challenges, enhancing your firms Operational Resilience is rapidly becoming a strategic priority "

Owen Lewis, Head of Management Consulting, KPMG Ireland

Definition:

Operational resilience is generally defined as the ability of an organization to continue to provide underlying business services in the face of severe events by anticipating, preventing, recovering from, and adapting to such events.

Accordingly, operational resilience includes both the resilience of systems, processes, besides the understanding of the existing vulnerabilities, and mitigating their accompanied emerging risks, to ensure that the financial system can withstand and limit the impact of future disruptions.

Basel Committee on Banking Supervision (BCBS) defines 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 assume that disruptions will occur, and consider its overall risk appetite and tolerance for disruption. The Committee defines tolerance for disruption as the level of disruption a bank is willing to accept given a range of severe but reasonable scenarios.

Principles of Operational Resilience:

The Basel Committee on Banking Supervision (BCBS) established **seven principles for operational resilience** aiming to promote a principle-based approach to improving the operational resilience of banks, making them better able to withstand, adapt to and recover from severe events:

- **Principle 1: Governance:**

Banks should utilize their existing governance structure, or even re-structuring its current one if necessary to establish, oversee and implement an effective operational resilience approach that enables banks to respond and adapt to, as well as recover and learn from, disruptive events in order to minimize their negative impact on delivering critical operations through disruption.

- **Principle 2: Operational Risk Management**

Banks should leverage their major key functions to manage their operational risk through identifying & detecting external and internal threats, such as: potential failures in people, processes and systems on a regular basis, in addition to immediately assess the weaknesses in its critical operations to manage the resulting risks, in accordance with their operational resilience expectations.

- **Principle 3: Business Continuity Planning &Testing**

Banks should have business continuity plans in place and conduct business continuity practices under a range of severe but logical scenarios, in order to test the BCM plan's ability to survive and deliver critical functions through disruption. An effective business continuity plan should identify critical operations, key internal and external dependencies, business impact analyses, and recovery strategies.

- **Principle 4: Mapping Interconnections & Interdependencies**

Once a bank has identified its critical operations, the bank should map the relevant internal and external interconnections and interdependencies that are necessary for the delivery of those critical operations, and to be consistent with the bank's approach to operational resilience.

- **Principle 5: Third-party Dependency Management**

This principle highlights the importance of managing relationships including those of, but not limited to third parties. This includes assessing risk before establishing any sort of relationship, and ensuring that any third party has an equivalent operational resilience approach in place.

- **Principle 6: Incident Management**

Banks should develop and implement response and recovery plans to manage incidents that could disrupt the delivery of its main operations in line with the bank's risk tolerance for disruption. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.

- **Principle 7: Information & Communication Technology (ICT) including cyber security**

ICT policies and cyber security measures should effectively support and facilitate the organization's delivery of critical operations while staying in-line with legal requirements concerning the protection of data and confidentiality. These systems should be tested regularly alongside other processes and systems within the organization to ensure optimal security, performance, and ability to overcome disruptions.

Operational Resilience Framework:

A comprehensive operational resilience framework is important to limit the impact of failures and provide continued market resilience for the organization (not only resilience within the organization). Such a framework should have the following essential elements:

- **Discovery & Documentation:**

The organization should start by discovering then documenting its main business services and aligning them to its underlying technology's infrastructure (cloud infrastructure, data centers, applications, etc.), and business processes (disaster recovery, cyber-incident response plans, etc.).

- **Assessment:**

These underlying technologies tools and their related processes should be assessed against Key **Performance Indicators (KPIs) & Key Risk Indicators (KRIs).** This step is used to create a risk score for each business service which is then reviewed against agreed impact tolerances. Hence, Impact tolerances should also be reviewed regularly as business strategies change, customer expectations develop, technology advances, and regulations evolve.

- **Disaster Recovery/ Remediation Plans:**

After the assessment, a disaster recovery plan should be developed, which gives priority to the business services with the largest disparity between risk score and acceptable impact tolerance.

Remediation plans should not only cover the impact of operational disruption but also extend to the organizations' ability to solve & contain such disruptions. Afterward, remedial actions should be identified to create a stronger resilience framework.

- **Testing:**

An important step in the process is testing, which is also prioritized by the risk degree of key business functions & services. Outcomes from testing should cycle back into the resilience assessment process and remediation planning. Regular testing and audits (including red teaming[1] and disaster recovery/business continuity testing) should be used to assess the resilience levels across critical operations' functions within the organization.

[1] Red teams are "ethical hackers" who help test an organization's defenses by identifying vulnerabilities and launching attacks in a controlled environment. Red teams are opposed by defenders called blue teams, and both parties work together to provide a comprehensive picture of organizational security readiness.

- **Technology:**

Technology assets should be kept up to date appropriately to defend against potential cyber threats, that may threaten the whole organization's operations & functions resiliency.

- **Third parties:**

Operational resilience should be an ongoing consideration for the organization's relationship with third-parties. Resilience shouldn't be limited to the organization's internal relationships, but extends to include all third parties that the organization interacts with. Therefore, effective internal and external communication plans should be updated regularly.

- **Cultural change:**

A key element of a resilient organization is its human capital. A cultural change is, therefore, crucial to make operational resilience a priority across the whole organization, and that everyone is engaged and working towards that end. This includes training staff to understand what operational resilience entails, alongside communication from senior management to ensure that all employees understand the resilience framework, how they fit into it, and its importance to the continuity of the whole organization.

- **Ownership:**

Clearly defined ownership & accountability of key elements & risks within the operational resilience framework, and how to mitigate them, is essential so that necessary functions are running as they should and key responsibility roles are well-assigned.

Why managing operational resilience is challenging?

Operational resilience management is challenging for the following reasons:

- **Accountability for resilience:**

It becomes a major challenge in case ownership and accountability of key roles & responsibilities within the operational resilience framework, are not well defined, among senior management & board of directors levels.

- **Scope of resilience assessments:**

In case there is a gap between the existing business continuity/ remediation plans, and how the emerging incidents are actually managed.

- **Testing and scenario analysis:**

There is a need for enhanced testing, scenarios, and simulation tools, which provide additional insight into sudden events. Therefore, there should be multiple event scenarios in place that can support future planning and preparations for disruptions.

- **Making a long-term commitment:**

Achieving operational resilience requires an organization to make a long-term commitment to perform & deliver its main functions & activities with consistency. The activities involved in the operational resilience management must become part of the whole organization's daily habits.

- **Understanding the big picture:**

To be operationally resilient, organizations must address operational risk on many dimensions simultaneously, including disqualified staff, advanced technology, facilities, supply-chain management. This requires careful planning, coordination, and training across many interdependent domains, as well as understanding how the organization's capabilities along these dimensions contribute to the organization's survival & continuity.

Recommended sources for Operational Resilience disclosures by global institutions:

- **Bank of England, the UK Prudential Regulation Authority, and The Financial Conduct Authority (FCA)** published a joint discussion paper entitled **"Building the UK Financial Sector's Operational Resilience"**, which referred to the crucial role of financial market infrastructures (FMIS), and senior management in setting the business and operational strategies, and overseeing their execution in order to ensure operational resilience." The paper also lays out an expansive approach addressing how the continuity of the services that organizations provide can be maintained regardless of the cause of the disruption.

https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf

- **The Central Bank of Ireland (CBI)** published ***"Cross-Industry Guidance on Operational Resilience".*** The objective of this Guidance is to communicate to the industry's stakeholders how to prepare for, respond to, recover and learn from an operational disruption that affects the delivery of crucial business services. The Guidance aims to enhance operational resilience and recognize the interconnections and interdependencies, within the financial system, that result from the complex and dynamic environment in which the organizations operate.

https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cross-industry-guidance-on-operational-resilience.pdf?sfvrsn=5

- **The European Commission (EC)** issued a consultative document on ***"Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure".*** The document focuses on strengthening the digital operational resilience of the EU financial sector. The consultative document has noted the need for a dedicated approach to enhance what can be referred to as the digital operational resilience of financial institutions in the context of the increase in outsourcing arrangements, third-party dependencies, and the emerging risks related to ICT.

https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf

- **The Office of the Superintendent of Financial Institutions (OSFI) Canada**, an independent federal government agency, issued a discussion paper titled ***'Developing Financial Sector Resilience in a Digital World'.*** The paper touches on several technology-related themes, including the priority risk areas of (a) cybersecurity (b) advanced analytics (c) third party ecosystem (d) digital data.

  The OSFI has observed that the increasing number of incidents, shifts in the severity of the emerging risks, require a better understanding among institutions and regulators.

https://www.osfi-bsif.gc.ca/Eng/Docs/tchrsk.pdf

- **Reserve Bank of New Zealand**, issued the ***"Guidance on Cyber Resilience".*** This guidance draws upon leading international and national cybersecurity standards and guidelines, and is intended to provide high-level principle-based recommendations for entities. This guidance primarily serves as a comprehensive framework for the governance and management of cyber risk, which entities can tailor to their own specific needs, rather than as an explicitly detailed or technical set of instructions.

https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Policy-development/Cyber%20resilience/Guidance-on-cyber-resilience.pdf?la=en&revision=46701795-9cc8-457f-8376-0dd45eb55416

February 2022

Currtent Trends

HOTLINE
15200
One number to better serve you!

Headquarters – Nasr City
22 A, Dr. Anwar El Mofty St., Tiba 2000
P.O.Box: 8164 Nasr City, Cairo, Egypt

www.ebi.gov.eg

Like us on
facebook.com/EgyptianBankingInstitute

Follow us on
twitter.com/EBItweets

Join us on
linkedin.com/company/egyptian-banking-institute

Watch us on
YouTube Channel: Egyptian Banking Institute (EBI)