Operational Resilience: Preparing for the Next Global Crisis

Although resilience in business operations has been a priority for organizations since before the onset of the COVID-19 pandemic, the ongoing global pandemic has made resilience more critical than ever. Even the smallest organizations have made business continuity, backups and succession planning considerations within routine operations. This newly established importance of operational resilience will have a lasting impact on enterprises.

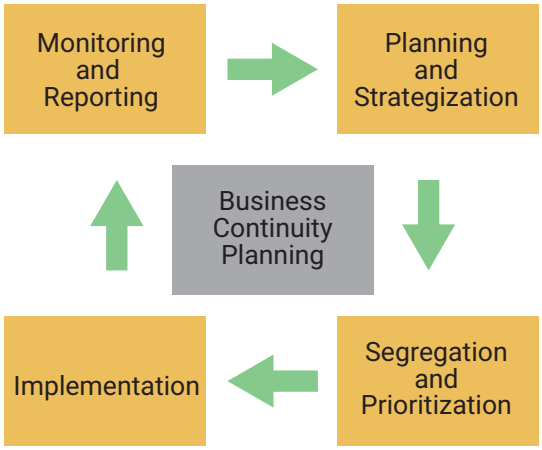
Operational resilience is a term that can be used in a wide range of industries; it cannot be narrowed down to one specific sector. The COVID-19 pandemic has equalized enterprises across all sectors and industries in terms of operational resilience. Though much work has been done to achieve resilience throughout the last two years, this is a developing area and there is a long way to go for all involved, especially because the world continues to deal with the ramifications of the pandemic.

Many organizations believe that operational resilience is the outcome of effective operational risk management (ORM). Although some enterprises may merge operational resilience with ORM, others work on it parallel with ORM or use input from ORM to achieve it. But there is more to it. It is worth examining a new outlook toward operational resilience, the challenges it introduces and some ways to address them. The traditional BCP practices implemented by organizations need insights and inputs from external situations to be prepared for any crisis situation at a given point in time. Organizations need to connect the dots across existing risk mitigation and governance requirements, including, but not limited to, cybersecurity, data protection, business continuity, outsourcing and risk culture.

Implementation

Business continuity planning (BCP) has been a part of organizations' usual business and operations policies and procedures for quite some time. The main concept of BCP is to be prepared for crisis events based on different scenarios. Every department and function in an organization has different critical activities and processes that need varying degrees of planning during crisis. BCP consists of four basic phases (**figure 1**).

FIGURE 1
The Basic BCP Cycle



However, the lessons learned from the global pandemic demand more. Operational resilience goes a step ahead of BCP, in that a resilient organization learns, adjusts and fine-tunes the business continuity activities and practices based on current external situations related to those activities. Between the planning phase and the monitoring phase, there is a sub-phase that is required: situational analysis. This phase involves keeping tabs on external situations related to business practices and then fine-tuning plans. One example of this change would be organizations adopting a work-from-home or hybrid working model due to the COVID-19 pandemic. This phase is crucial to prepare for any sudden emergence

SUMEDHA ADAVADE | CISA

Is a risk manager at DBS Bank. She has 14 years of experience in risk, compliance, audit and information security, providing risk-mitigating solutions and assurance to banks and other financial institutions.

of adverse events affecting resources, processes or controls in an organization and being able to immediately adapt to the change.

Considering this new sub-phase of situational analysis, there are five steps that may help an enterprise achieve operational resilience: defining important business activities, setting impact tolerances, determining process and system ownership and accountability, ensuring third-party resilience, and adhering to regulatory requirements.

Step 1: Defining Important Business Activities

The first step to making any business continuity plan is identifying important business activities. An ORX survey conducted in 2020 about important business activities in active banks in the United Kingdom showed that participating organizations had quantities of important activities ranging from as low as 10 to as high as 100.[1]

Due to the pandemic, organizations' legacy activities and processes that had not previously encountered any setbacks began to experience issues. For example, consider branch banking operational processes. During initial lockdown periods, bank branches were operating in staggered working hours to curtail the infection rate. Less technology-aware customers who live in remote locations without much digitization that are used to walking into branches faced issues in carrying out banking transactions during these times. Examples such as these establish the importance of not leaving any loose ends when planning for operational resilience.

"When setting impact tolerances, there are generally no prior experiences or lessons to draw guidance from because this exercise is unique for every organization."

What makes business activities important? For successful implementation of operational resilience, any activity or process which, if interrupted, has the potential to affect business operations beyond an organization's tolerance may be considered important. Based on external circumstances, activities may be added or withdrawn from an organization's list. They also may move up and down the list as the activity becomes more or less urgent.

However, there are some challenges in defining important business activities, including:

- Multiple definitions and benchmarks may be used to define the same important activity.
- Regulatory guidelines for an industry may vary globally.
- Standard practices followed within the same industry may vary by enterprise.
- Uncertainty of external circumstances may find an organization unprepared to conduct activities that had previously been taken for granted.

Fortunately, these challenges can be addressed by:

- Thoroughly understanding all processes and activities and their alignment with business strategy
- Defining a single point of harm and collating all activities that are likely to be impacted by it. This is different than determining an organization's standard risk appetite, as the defined point of harm may need frequent revisions and fine-tuning based on external circumstances until it reaches a specific maturity level. Note that the point of harm should still align with the organization's risk appetite.
- Prioritizing activities based on BCP definitions (e.g., recovery time objective [RTO], recovery point objective [RPO])
- Testing business continuity plans diligently based on a frequency that is determined after considering the aforementioned steps

- Using lessons learned during testing to adjust the point of harm and prioritize activities as needed

Step 2: Setting Impact Tolerances

When setting impact tolerances, there are generally no prior experiences or lessons to draw guidance from because this exercise is unique for every organization. Thus, it is important that organizations consider all potential factors that could affect the tolerance-setting process.

What has worked in previous routine BCP plans may not work again. The point of harm needs to be judiciously set using a self-learning and adjusting mode based on external circumstances. This can be difficult to achieve immediately.

Additional challenges when setting impact tolerances may include:

- Setting universal tolerance limits for processes affecting different business units, functions or geographies
- Setting tolerance limits for interrelated processes and activities
- Setting tolerance limits for activities for which there are only contingency plans in place for parts of the activities
- Continuous monitoring and learning from uncertain external situations to readjust and fine-tune the point of harm

To address these challenges, the following actions can be taken:

- The single, master point of harm can be determined using a prudent approach that considers global circumstances and organizational policies and processes. This may be locally tuned per geographies and market conditions. For example, if the acceptable downtime for a critical IT system is x hours, it can be fine-tuned to x+1/-1 hours based on changing trends, the service provider's situation and market practices. This value of x hours can be adopted as is by all offices of the organization in different geographies or it can be readjusted to suit the particular geography if it requires different values based on local regulations. If this process is performed carefully, such values (i.e., x hours) should not be much different from each other.
- For activities impacting multiple business units, tolerance limits should be set with a consensus from all impacted units. For example, the credit card department and transaction execution department can jointly set tolerance limits for transaction processing–related activities, considering local circumstances, regulatory guidelines and organizational policies.
- Operational risk management tools such as scenario assessment and risk control self-assessment can be used for setting impact tolerances.
- For scenario assessment, new scenarios can be added annually. Assumptions and loss calculations can be adjusted per external circumstances (e.g., a new malware attack can be used to adopt processes in a scenario such as a cyberattack on the IT system of an organization), along with internal changes and impact. This is useful when adjusting the point of harm.
- The assessment of controls during risk control self-assessment exercises should consider impacts on the process from external circumstances, wherever relevant and applicable. The addition of new risk and, accordingly, controls, can also be considered.

> "Operational resilience cannot be achieved simply by implementing robust business continuity plans and disaster recovery drills."

Step 3: Process and System Ownership and Accountability

Operational resilience cannot be achieved simply by implementing robust business continuity plans and disaster recovery (DR) drills. It requires a cultural shift within an organization and a change in employee mindsets. Establishing ownership and accountability for any process and system may seem simple on the surface. However, there is much more to it. A single process or activity may involve multiple people from different business units and functions. Getting every stakeholder in line can be burdensome. For example, an organization may require an early launch of a new feature in a product, but it may not be ready or fully secure in terms of IT security until the launch date. Compromising on security of digital payment products can prove dangerous to an organization.

LOOKING FOR MORE?

- Read *Supply Chain Resilience and Continuity. www.isaca.org/supply-chain-continuity-2020*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Process and system ownership and accountability can introduce several challenges, including:

- Collaborating on interconnected processes and activities may require work from employees across different departments. Asking someone to perform recurring tasks outside of their job description may be taxing on employees.
- Achieving segregation of duties (SoD) while establishing ownership of processes. For example, there may be a resource crunch due to an increasing infection rate during a pandemic, which may cause difficulty in allotting duties to available staff.
- Mapping of processes and activities with impacted units and operating units to ensure accountability. A process or an activity may hold different significance to different functions; hence, it may be difficult to map. For example, an operations unit may input values of a key risk indicator (KRI), but the threshold breach of that indicator may be fully owned by the business because it is related to a business product/process.
- Considering impact of external circumstances on processes, identifying new process risk, and implementing new controls and ownership for them. For example, due to sudden changes in government restrictions due to infection trends, transportation may be affected, which may impact processes such as document warehousing in physical locations.
- Identifying and implementing completely new processes or activities, hiring new resources if required, and establishing roles and responsibilities related to new processes. For example, due to an increase in potential fraud because of transaction processing in the work-from-home (WFH) environment, banks had to invest in new specialized security products and hire and train resources to operate them.

These challenges can be mitigated to some extent by:

- Establishing accountability by mapping all processes and activities to their respective owners
- Selecting metrics for important business activities, taking cues from operational key risk indicators (KRIs)
- Clarifying the roles and responsibilities of every process owner to achieve appropriate SoD
- Ensuring all stakeholders are working toward the same objective as part of organizational strategy

Step 4: Third-Party Resilience

With the ever-increasing dependence on outsourced service providers and the inherent risk of outsourcing, assurance on resilience of all third parties serving an organization is of the utmost importance. Since the onset the COVID-19 pandemic, risk related to outsourcing activities has increased manifold.[2] As critical systems were accessed and processes were conducted from home by contract employees, governance became even more critical—and very difficult. Even more difficult was ensuring business continuity throughout the supply chain and all associated resources as offices closed and services were limited during national lockdowns and COVID-19 restrictions.

Additional obstacles to achieving third-party resilience include:

- Establishing the criticality of service providers can be a tedious task. The supplier that provides the most value may not be the most critical supplier in terms of operational resilience.
- The resilience of subcontractors of service providers may be unknown.
- It may be difficult to gain visibility into third-party concentration risk.
- Complete transparency and visibility from systemically important service providers such as cloud computing service providers is not realistic.
- Service providers' increased adoption of new technologies impacts operational resilience.[3]

To address these challenges, consider the following solutions:

- Assign materiality to each outsourced service provider based on impact to operations, business, finance, customers, liquidity, geographies or regulatory impact if the service provider is unable to provide services.
- Testing, audits and their frequency may differ for all outsourced service providers. For example, cybersecurity tests, such as vulnerability assessment and penetration testing, are important for service providers who provide automated teller machine (ATM) operations services but can be waived for a service provider that warehouses physical documents.
- Ratings can be provided annually to all service providers and the weakest link in the system can be identified through the lowest rating, allowing vulnerabilities to be addressed.

- Disaster recovery drills, reports and business continuity plans of the outsourced service provider should be diligently checked and governed.
- The subcontractors of materially outsourced service providers can also be subject to tests and audits based on criticality. These can be performed based on an agreement between all three parties.

Step 5: Regulatory Requirements on Operational Resilience

Globally, operational resilience is a key focus area for regulators. However, the requirements set by regulators focus on different actions organizations are expected to take. For example, the UK regulatory framework PS6/21 *Operational Resilience: Impact Tolerances for Important Business* focuses on the delivery of important business services.[4] The European Commission has been focusing on cybersecurity and IT risk as opposed to resilience threats more broadly. Alternatively, Switzerland's Basel Committee on Banking Supervision (BCBS) has a strong emphasis on governance and board oversight on planning and risk tolerance.[5]

Compliance with regulatory requirements for operational resilience can prove challenging for two reasons:

1. Regulators around the world continue to fine-tune the approaches and requirements needed to achieve operational resilience. Organizations have been able to comply with existing guidelines up until this point, but the current situation created due to pandemic demands more.
2. A one-size-fits-all approach will not effectively satisfy all regulatory requirements. Some regulators provide general guidelines and leave their implementation open to interpretation by organizations, while some provide concise requirements. In the case of the former, an organization could make an incorrect or incomplete interpretation, resulting in noncompliance; in the latter, it may be difficult to meet every requirement.

To better understand and obtain regulatory compliance, consider the following guidelines:

- When there is a difference between regulatory guidelines and internal policies and processes, it is best to implement the stricter of the two.
- Guidelines related to operational resilience may not include drastic changes from what existed previously. The approaches for identifying business critical activities, mapping activities and setting impact tolerances may undergo refinement. These need to be reflected in respective operational resilience exercises.
- Organizations must strive to interpret regulatory guidelines correctly. Compliance teams must be aware of any new guidelines, interpretations or clearings of doubt that regulators may issue.
- The regulators who are focusing on operational resilience should also provide implementation support to organizations and recommend industrywide best practices. This can be done through workshops or seminars on operational resilience. Recognition can also be given to organizations who lead in such practical implementation.

"The subcontractors of materially outsourced service providers can also be subject to tests and audits based on criticality."

Next Steps

Organizations may take various approaches to pilot operational resilience. Some organizations start by identifying critical business activities, some start by testing resilience and some survey existing business activities to establish their criticality.[6]

For example, consider security of data in a bank where employees work from home. Banks have implemented a technology of dynamic watermarking for staff who work from home. It creates a unique pattern that appears in the background of screens for staff connecting to home or other networks. This technology establishes accountability in an event of data leakage, but it may also impact the speed of certain applications, causing disruptions to business. It may be best to implement it first for limited staff and then slowly expand it.

There is no right or wrong approach. The piloting of operational resilience will differ in terms of operations, processes, business strategy, resources, geographical context, market practices, applicable regulations and standards followed. However, the underlying principles remain the same.

"To be prepared for future global crises, it is crucial that operational resilience be managed proactively and with conscious effort."

Conclusion

The global COVID-19 pandemic has made it clear that the modern world is volatile, uncertain, complex and ambiguous (VUCA).[7] Moving forward, operational resilience will be at the heart of every enterprise. To be prepared for future global crises, it is crucial that operational resilience be managed proactively and with conscious effort. Hence, operational resilience should begin as part of an organization's business strategy; senior management should be involved at all stages, allowing for efforts to percolate down to ground-level operations so that the organization is prepared to handle unexpected, widely impacting scenarios. To better understand the bigger picture of operational resilience, business continuity should be industrialized with more strategic initiatives from government and public organizations, such as online or physical workshops, best practice–sharing seminars, and recognition for the most resilient organizations. This will help enterprises remain crisis ready and contribute to building a resilient economy, secure social life and sustainable use of available resources.

Endnotes

1 ORX, *Progressing Operational Resilience*, Switzerland, 21 June 2021, *https://members.orx.org/orx-publications/progressing-operational-resilience*

2 Sangani, P.; "Companies Expected to Outsource More Work Due to Covid-19 Pandemic: NTT," *The Economic Times*, 6 May 2020, *https://m.economictimes.com/tech/ites/companies-expected-to-outsource-more-work-due-to-covid-19-pandemic-ntt/amp_articleshow/75573710.cms*

3 ORX, *Operational Resilience Development and Implementation Study*, Switzerland, 3 January 2022, *https://members.orx.org/operational-resilience-resources*

4 Bank of England, *Operational Resilience: Impact Tolerances for Important Business Services*, United Kingdom, March 2021, *https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=D6335BA4712B414730C697DC8BEB353F3EE5A628*

5 Bishop S.; M. Lavallin; L. Carrivick; "Developments in Operational Resilience in the Financial Sector," The ORX Operational Risk Podcast, July 2021, *https://engage.orx.org/the-orx-operational-risk-podcast#episode10*

6 *Op cit Progressing Operational Resilience*

7 Bennet, N.; G. J. Lemoine; "What VUCA Really Means for You," *Harvard Business Review*, January–February 2014, *https://hbr.org/2014/01/what-vuca-really-means-for-you*