Did banks develop herd immunity?

The recent guidance issued by Basel Committee on Operational Resilience aims to strengthen the ability of banks to withstand operational risk-related events which could cause significant operational failures or wide-scale disruptions in financial markets, such as pandemics, cyber incidents, technology failures or natural disasters.

.

In this paper, we outline an integrated approach to building operational resilience, its key components, and practical insights on how to address key challenges.

Most Banks like to believe that they have handled the Covid-19 crisis relatively well, given the severity and longevity of this sudden disruption. Banks are yet to undertake any structured "lessons learned" study to identify what worked well and what didn't. Still, the nonoccurrence of any significant operational losses provides them the adequate assurance to reinforce their view. A closer look at the operational loss data published by ORX for the period 2014- 2019 and the first half of 2020, also reflects an overall decrease in the operating risk losses.

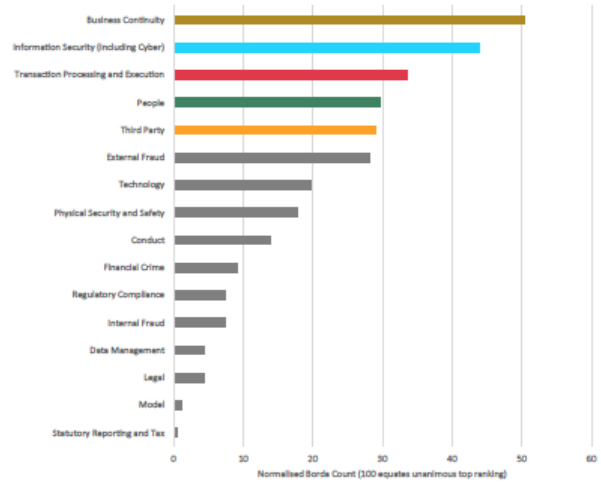
On the other hand, recent supervisory guidance from BIS on "Operational Resilience" indicates that the current preparedness of Banks globally is not adequate, and supervisors expect banks to enhance their operational risk significantly, business continuity management practices to improve their operational resilience. The Prudential Regulatory Authority (PRA), the UK regulator, has been at the forefront of shaping the industry thinking on operational resilience and has published series of consultative papers outlining the overall approach to operational resilience for banking financial services firms.

This article covers critical aspects of building a robust operational resilience framework and outlines the linkages with existing operational risk management and business continuity management.

Defining Operational Resilience

The Basel Committee1 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, and recover and learn from disruptive events to minimise their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should consider its overall risk appetite, risk capacity, and risk profile.

Figure 1. The top current risks facing the industry by rank score.

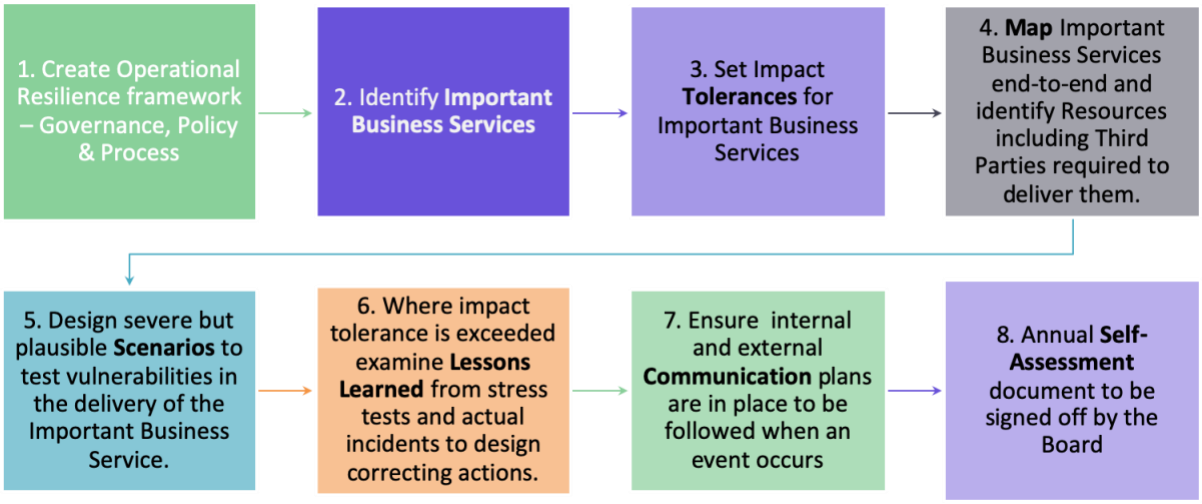


The ORX's COVID Risk Review, published in June 2020, provides the view of the top 5 risks as ranked by industry risk professionals (Figure 1). It is clear that the overall risk profile has evolved considerably since the beginning of the year. The top 5 risks now are the ones that closely relate to the operational resilience areas.

The overriding risk impact concern is operational (including business disruption), with staff/internal impact also a key concern reflecting the current crisis's nature.

Operational Resilience: Key Components

The diagram below highlights key component of an integrated, enterprise wide operational resilience framework



1. **Creating Operational Resilience Framework**: Like most enterprise initiatives, the first and most crucial step is to create an overarching framework for operational resilience, which clearly defines the overall governance structure and lays out the policies and processes for the first, second, and third defense lines. A frequently asked question is – Do we create a new function for operational resilience or embed it in existing OR, BCM function? Though the answer will be particular to each institution, but generally observed trend is to place it under a current OR/BCM process. It is essential to understand the linkages between the existing OR/BCM function and operational resilience, as depicted in the diagram below

	Operational Risk Management	Business Continuity Management	Operational Resilience
1. Business Services	Business Process Focused	IT Business Process	Focus on **Business services** that matters most, horizontal view
2. Impact Tolerances	Risk Appetite, KRI, RCSA, Loss	Loss based on RTO/MTO	Risk appetite based metrices
3. Resource Mapping	People, Process, System	People, Systems, Locations, Suppliers	People, Systems, Process Locations, Third Parties, Information
4. Scenario Design	BAU	Static, Moderate to high impact short duration	Dynamic, Severe but plausible, long duration
5. Testing	QA	Mostly single Point of failure, short duration	End to end
6. Actions	1 LOD and 2 LOD	1 LOD local & 2 LOD with central crisis management oversight	Active Board oversight with 1 LOD and 2 LOD
7. Communication	Communicate events	BCM Communication Plan	Operational Resilience Communication Plan

2. Identify Important Business Services

Operational resilience requires an institution to take a horizontal view of the organization, and to do, so it introduces the term "business service." A business service' is a service that a firm provides to an external end-user. It's important to note that a business service is different from the business process, which is commonly used in the OR/BCM frameworks. A business service delivers the outcome expected by a customer, market participant, or end-user. It is 'what' is delivered. This is different from a business process, which is how the service is delivered, and therefore tends to be more granular and internally focused. Further several business processes may be required to provide the overall outcome expected by a customer. Although not synonymous with business services, the economic functions identified through RRP-related initiatives can help identify these. Institutions should not lose focus on the word "important." Interestingly during the lockdowns, most regulators prioritized and issued specific instructions to banks on what services should continue to be operational.

3. Set impact tolerances for Important Business Services

Once the business services and clearly defined and rank-ordered to reflect their absolute and relative importance, the next step is to set Impact tolerance, which is a firm's tolerance for disruption to a particular business service. While setting the impact tolerances, the firm should take an "outside-in" view rather than an "inside" view considered in the OR/BCM design. The three main impact categories to evaluate the disruption of a business service are:

- Organizational viability: The very existence of the organization could be at risk
- Financial stability: The stability of the market and the broader economy would be threatened
- Customer and other market participants harm: There would be a considerable detriment to end users of the service

It is essential to distinguish these impact tolerances from traditional business impact analysis done by the Bank. Also, detail out the ways to measure outcomes and define metrics for normal & peak times. Separately firm should link these impact tolerances with overall risk appetite and other measures of operational risk.

4. Map Important Business Services to Resources, including Third Parties

COVID 19 has taught some vital lessons where many firms struggled to mobilize resources such as laptops, set up board band connectivity to support a sudden transition to work from home operating model, or handle the massive surge in customer calls.

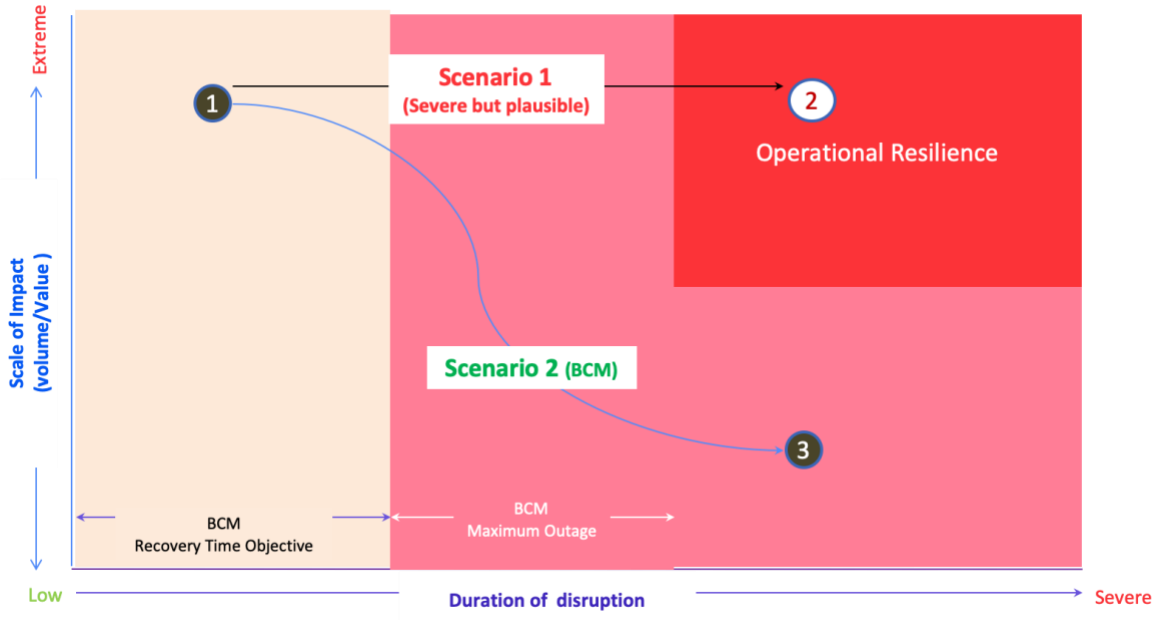
Firms need to identify and document the resources necessary to deliver each of its important business services. The resources are people, processes, technology, facilities, information, and third parties. By mapping resources to each important business service, firms can be assured that an important business service can remain within the impact tolerance it has set. Resources can potentially come from across business areas, entities (intragroup and other

outsourcing), and jurisdictions, which gives the need for a centralized identification for these inputs.

It is critical to outline resource vulnerabilities that will prevent important business service delivery and classify the necessary resources needed to deliver a business service. This requires firms to look at alternate delivery mechanisms ('Plan Bs'), including changes in their operating model, build up during the normal and peak of the duration, and assess substitutability and replaceability. Additionally, the ability to build a control mechanism to augment resources not owned by the firm in the time of disruption.

5. Design severe but plausible Scenarios to test vulnerabilities in the delivery of the Important Business Service

A severe but plausible scenario is when the nature, scale, or scope of the event goes beyond pre-recommended recovery measures and supporting assumptions. A scenario where severity is exceptionally high and duration extends beyond the recovery time objectives (RTO) and maximum outage as defined in the BCM measures. The diagram below depicts this to illustrate this point



6. Self-assessment to test when impact tolerance

Conducting lesson learned exercise based on test scenario used and business services impacted involves Identifying an appropriate range of adverse circumstances varying in nature, severity, and duration relevant to its business and risk profile for which the firm expects to be able to remain within their impact tolerances and which ones they may not. The firm should clearly demonstrate its capability to respond and recover within pre-defined impact tolerance levels. Stress testing should focus on the response and recovery actions firms would take to continue delivering an important business service.

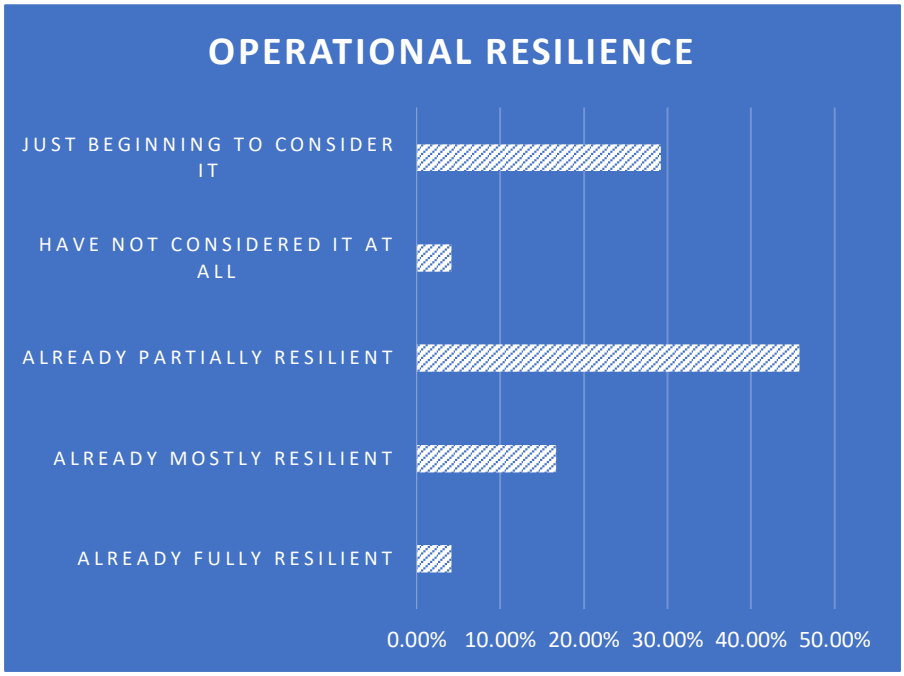
7. **Ensure internal and external Communication plans are in place to be followed when an event occurs**

It is crucial that as a part of operational resilience, firms highlight the strategy and execution for a prompt and meaningful communication arrangements for internal and external parties, including regulators, consumers, and the media.

Before designing the communication, the firm must gather information about the cause, extent, and impact of operational incidents. It should contain an expression of care and concern, a demonstration of control over the situation, an indication of alternative services and redress arrangements, and a commitment to improving.

Internal communication plans should also include the escalation paths firm would use to manage communications during an incident and identify the appropriate decision-makers.

The overview above clearly articulates the significant effort that is required to build an integrated operational resilience framework. In recent years most Banks have done a lot of foundational work as a part of their operational risk and business continuity management, which provides an excellent foundation and starting point.



Before we conclude this introductory paper on operational resilience, I would like to share the results of a recent poll done on the bank's readiness for operational resilience.

From the results it doesn't look like that banks have developed the herd immunity; the regulators certainly don't seem to think so!

Author
Alok Tiwari – Principal, Athena Advisory and Co-founder Aptivaa, Athena's partner firm.