OPERATIONAL RESILIENCE:
Where are We?

NOVEMBER 2020

Author: Kevin Nye, *Executive in Residence, Global Risk Institute*

In recent years, financial institutions have been severely challenged by cyber-attacks, technology failures and the current pandemic. This has put both clients and the wider financial markets at risk. These disruptions will continue and with that in mind, how to make firms more operationally resilient has become a priority in many regulatory jurisdictions. There are a number of approaches under consideration and whether regulators ultimately respond by providing workable globally-compatible guidance is yet to be determined. Regardless, firms need to act now to better protect their clients, themselves and overall market integrity.

To begin, it is important to understand how traditional operational risk management and operational resilience differ. Operational Risk is defined as "the risk of loss from inadequate or failed internal processes, people and systems or from external events."[1] Operational Resilience is defined as "the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions."[2] To move forward however, we must go beyond these formal regulatory definitions.

At the highest level, the difference between managing operational risk and being operational resilient is a change in mindset, moving from being focused on the impact on the firm to being focused on the impact on the client. It is not about how to recover the functionality of a particular system *if an event happens*, it's about how to ensure you can meet your clients' needs when that event happens. It puts the client at the centre of what you do.

All firms like to think of themselves as client centric and that meeting their clients' needs is paramount. Over time however, these needs have become much more specific and granular. Providing bundled banking products is no longer sufficient. Today, clients look at each service separately (e.g. ability to check your balance online, the ability to withdraw cash from an ATM) and they expect the delivery of each of these services to be seamless, 24/7, without delay or interruption. Those who can deliver this, even in times of crisis, will see improved customer loyalty and trust. Not being able to meet your clients' needs at that level of granularity in times of distress can result in severe reputational damage and often loss of client, both extremely costly to the firm.

At this point, global and domestic regulatory approaches to operational resilience vary. The Basel Committee on Banking Supervision (BCBS) and the UK Regulatory Authorities (UK) are taking a principles-based approach, albeit with varying degrees of prescriptiveness, while the U.S., Australia and Canada are more focused on specific technologies (e.g. cybersecurity). The current position of the various regulatory bodies is as follows:

BASEL COMMITTEE ON BANKING SUPERVISION (BCBS)

Consultative Document — Principles for operational resilience. Issued August 2020 for comment by November 6, 2020.

- This paper takes a very high-level, principles-based approach. "The Committee believes that a pragmatic flexible approach to operational resilience can enhance the ability of banks to withstand, adapt to and recover from potential hazards and thereby mitigate potentially adverse impacts."[3]

- This Consultation Document should be reviewed in conjunction with the Consultation Document – Revisions to the sound management of operational risk,[4] which was released concurrently.

- Principles are organized as follows; governance, operational risk management, business continuity planning and testing, mapping of interconnections and interdependencies of critical operations, third-party dependency management, incident management, and resilient information and communication technology (ICT) including cybersecurity.

- Looks to build on and not replace existing guidance, "the principles for operational resilience… are largely derived and adapted from existing guidance that has already been issued by the Committee or national supervisors over a number of years."[5]

- Recognizes work in progress in various jurisdictions and "seeks to promote greater cross-sectoral collaboration."[6] This has allowed for a fair degree of freedom as to how domestic regulators will move the operational resilience agenda forward.

UK REGULATORY AUTHORITIES (BANK OF ENGLAND, FINANCIAL CONDUCT AUTHORITY AND PRUDENTIAL REGULATION AUTHORITY)

Joint Consultation Paper – Building operational resilience. Issued December 2019 for comment by October 1, 2020 (extended from March 20, 2020)

The principles underpinning the approach taken by the UK Regulatory Authorities are aligned with those put forward by the BCBS. That said, the UK Consultation Paper is much more detailed as to their expectations (60 pages) than the BCBS Consultative Document (9 pages). It is client focused, business services oriented and provides a clear outline of what needs to be done to improve resilience. This includes:

- Requiring firms to identify their important business services, which if disrupted could cause undue hardship to either their clients or the financial markets; "Focusing on business services encourages firms to consider alternative ways the service may be delivered in a way that monitoring individual components and processes cannot."[7]

- In identifying important business services, consideration should include identifying those most likely impacted by the disruption, the potential impact on the firm, as well as the impact on the wider UK financial system.

- Detailed mapping of processes and technology supporting the delivery of these services is required; "To have a complete view of resilience, firms will need to identify and document the people, processes, technology, facilities and information necessary to deliver each of the firm's important business services."[8]

- Firms would be required to set impact tolerances detailing maximum tolerable outages and impact on clients.

- Continuous testing, self-assessment and lessons learned is required.

- Firms are expected to invest to remedy shortcomings in resiliency, including improved processes, infrastructure and systems to further protect clients and financial markets.

- Similar to the BCBS, the intent is not to replace prior direction, "our proposals are not intended to conflict with or supersede existing requirements to manage operational risk or business continuity planning, but rather aim to set new requirements that enhance operational resilience."[9] That said, at this point, it is unclear the degree to which work done in other areas (e.g. disaster recovery) can be leveraged.

OTHER INTERNATIONAL REGULATORY GUIDANCE

In addition to those noted above, other regulators have issued guidance on resilience which tend to be more specific as to areas of focus. These include:

- *European Banking Authority – Cyber resilience testing framework for significant market participants (April 2019)*

- *Federal Financial Institutions Examination Council – Continuity Management Handbook (November 2019)*

- *Australian Securities and Investments Council – Market integrity rules to promote technological and operational resilience (June 2019)*

OFFICE OF THE SUPERINTENDENT OF FINANCIAL INSTITUTIONS (OSFI)

Discussion Paper — Developing Financial Sector Resilience in a Digital World — published September 15, 2020 with feedback requested by December 15, 2020.

This paper focuses more on financial sector resilience in general rather than providing specific views as to what will need to be done domestically to improve operational resilience specifically, "At this time, OSFI is not advancing any firm proposals and intends to follow this consultation process with one or more consultative documents."[10]

Highlights:

- Financial sector resilience is motivated by the rapid advancement in digital technologies and technology more broadly

- A high-level discussion paper focused on ensuring constituents, "are better prepared to identify and develop resilience to non-financial risks before they negatively affect their financial condition"[11]

- Focuses on three OSFI priority risk areas; cybersecurity, advanced analytics and the third-party ecosystem

- Takes a principles-based approach building on existing guidance in other areas of operational risk

- Recognizes that operational resilience differs from more established operational risk management, "Whereas ORM tends to be process-oriented, operational resilience takes a more outcomes-based approach to a given adverse event"[12]

- Stresses the need for a holistic approach to operational risk management and operational resilience, "Authorities, including OSFI, are beginning to assess the merits of an operational resilience perspective, and reassess the adequacy of existing ORM frameworks in relation to operational resilience"[13]

As can be seen by the above, the subject of operational resilience is still very much open to consultation and discussion. From a Canadian perspective, where does this leave us?

At this point in time, the UK is leading the way on operational resilience. The expectations are detailed and clear, and while not embraced globally, it is reasonable to assume that, as has been the case in the past, Canada will lean more in this direction than not.

Firms with operations in the UK can reasonably expect that those businesses will need to follow the UK approach once the consultation process is completed and the directive issued. While the implementation date has yet to be determined, given the scope and detail of the processes being contemplated by the UK, time to achieve compliance will no doubt test their resources.

Ideally, regulators, both globally and domestically, should help drive firms to become more operationally resilient by aligning as to their expectations and direction. That said, putting the client at the centre of what you do should not be dependent on further regulatory guidance. Becoming more operationally resilient is good for the client, is good for the firm and should be done now.

ENDNOTES

1. Basel Committee on Banking Supervision: Principles for the Sound Management of Operational Risk, June 2011 (www.bis.org)

2. The View from the Regulator on Operational Resilience: December 2019 (www.fca.org.uk)

3. Basel Committee on Banking Supervision: Principles for Operational Resilience, August 2020 (www.bis.org)

4. Basel Committee on Banking Supervision: Revisions to principles for the sound management of operational risk. August 2020, (www.bis.org)

5., 6. Basel Committee on Banking Supervision: Principles for Operational Resilience, August 2020 (www.bis.org)

7., 8. ,9. Financial Conduct Authority: Building Operational Resilience. December 2019 (www.bankofengland.cp.uk)

10., 11., 12., 13. Office of the Supervision of Financial Institutions: Developing Financial Sector Resilience in a Digital World: September 2020 (www.osfi-bsif.gc.ca)