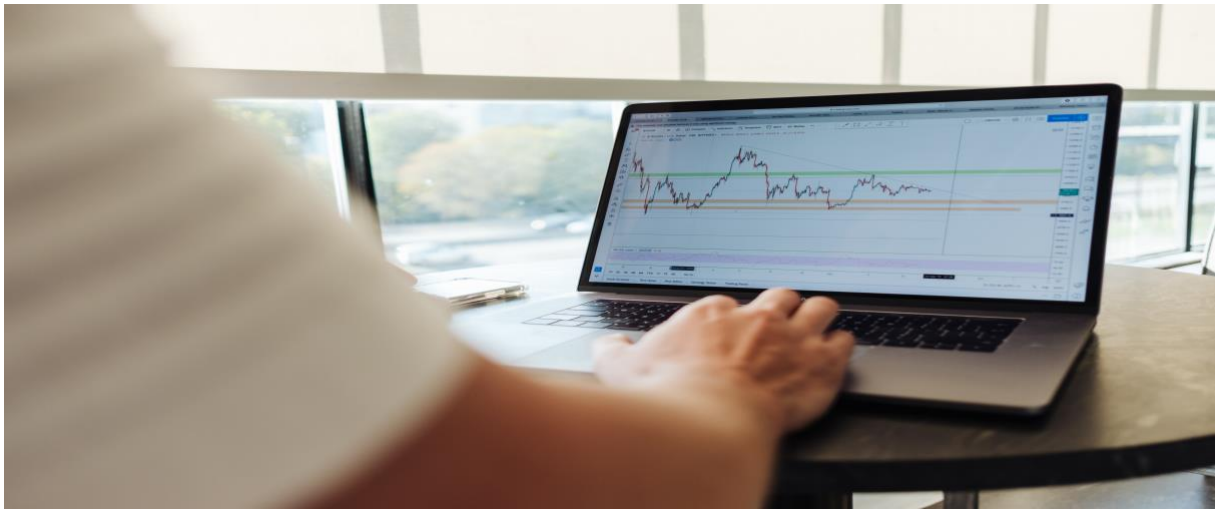
OPERATIONAL RESILIENCE – PRINCIPLES FOR A POST-PANDEMIC WORLD



INTRODUCTION

Operational resilience has been identified by top UK banks as a key area of concern for the near future. Geopolitical changes, technological innovations, and physical events such as Covid-19 or climate-related events have left UK financial institutions anxious about their abilities to continue critical operations during times of crisis. To this end, the UK and European regulatory authorities have published documents outlining risk management approaches that can be taken to ensure operational resilience under various disruptive scenarios.

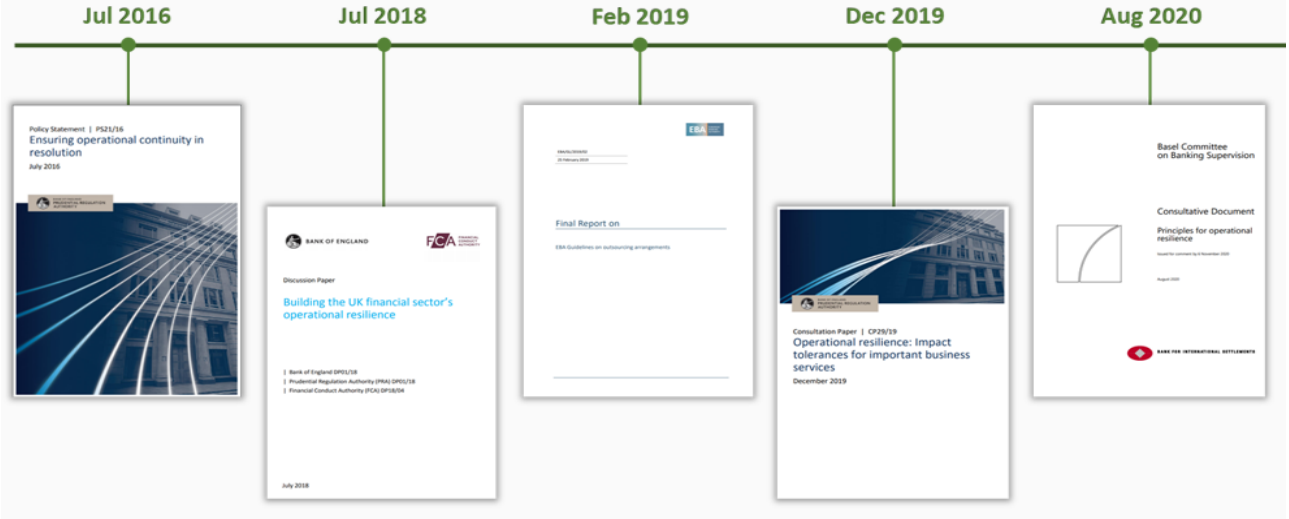
In August 2020, the Basel Committee on Banking Supervision (BCBS) published a *Consultative Document*[1] on the Principles for Operational Resilience. Through this document, BCBS proposes a principles-based approach for enhancing operational resilience of Financial Services (FS) firms, including consideration of challenges created by the Covid-19 pandemic.

As the prudential risk framework evolved after the GFC, regulators noted that better capital and liquidity management are only part of the solution to improve the ability of firms to absorb external shocks. Operational continuity failures, while firms had robust capital and liquidity levels, could also threaten financial stability. There was a gradual realization that FS firms needed to be better at responding to operational events – pandemics, cyber incidents and natural disasters (meta risks) – which can significantly impact their ability to continue operating.

PREVIOUS OPERATIONAL RESILIENCE PUBLICATIONS

This thought process has been reflected through several supervisory statements and expectations issued since 2015 and recent PRA and FCA interactions with firms – a timeline of publications is illustrated in Figure 1. This paper acts as a significant change in the Basel Committee's approach to operational resilience as previous publications on the subject focus on broader issues in operational resilience with little to no actionable resolutions. For example, the PRA's July 2018 paper[2] states that the bank will take a broader approach to operational resilience and does not dive deeper into the functions of operational resilience and potential impacts. By comparison, the PRA's Dec 2019 consultative paper[3] provides a more granular discussion around the functions of sound operational resilience and introduces the topic of impact tolerance with into further details about the required steps to achieve operational resilience and sets up actionable objectives for banks, introducing the expectation to act when a weakness in operational resilience is identified.

Figure 1: Timeline of Operation Resilience Publications issued by the PRA, EBA and BCBS



OPERATIONAL RESILIENCE AND COVID-19

Covid-19 has brought operational resilience-related considerations into sharper relief as many firms grapple with the financial, operational, and technological changes that have occurred since the outbreak in early 2020. The following graphic highlights these impacts:

[1] *Consultative Document: Principles for operational resilience, 6 August 2020, https://www.bis.org/bcbs/publ/d509.htm*
[2] Consultative Document: Building the UK financial sector's operational resilience, July 2018, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf
[3] Consultative Document: Building operational resilience: Impact tolerances for important business services, December 2019, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/building-operational-resilience-impact-tolerances-for-important-business-services.pdf

Figure 2: *Covid-19 impact on operational resilience of banking institutions*

In this context, this Consultative Document aims to guide FS firms in enhancing their approach to operational resilience. As UK banks seek to recover from the financial impact of the pandemic, appropriate steps must be taken using the principles and proposals made in this paper, to ensure that the impact of further systematic disruptions in the future will be minimised. The objective of this paper is to summarize the key changes to the Principles for the Sound Management of Operational Risk (PSMOR) outlined in the Consultative Document as well as highlight the key ways in which Avantage Reply can assist FS firms in improving their operational resilience.

BCBS GUIDE TO OPERATIONAL RESILIENCE

Operational Resilience

The 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 minimise their impact on the delivery of critical operations through disruption. Banks can achieve operational resilience by ensuring that existing risk management frameworks, business continuity plans, and third-party dependency management are implemented consistently within the organisation.

Adopting a pragmatic and flexible approach to operational resilience that is based on the size and nature of the bank which also takes into account the business profile and risk tolerance of the bank, would help banks to ensure that they can face operational challenges arising from changes in the global environment. Risk identification and assessment, as well as appropriate mitigation and monitoring processes, are essential to minimise potential operational losses.

The new BCBS paper breaks down the guidance for operational resilience into seven areas. These categories have not changed from the previous version of the PSMOR, that expectedly can make it easier for banks to implement required amendments. The figure below highlights each of the seven principles of operational resilience.

Figure 2: *Seven Principles of Operational Resilience*

The paper aims to emphasize the importance of maintaining operational resilience focusing on the aforementioned topics and to provide the guidance for banks building on the BCBS approach.

PRINCIPLE 1 – GOVERNANCE: *Banks should utilise their existing governance structure to establish, oversee and implement an operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimise their impact on delivering critical operations through disruption.*

The principle recommends that the board of directors should review and approve operational resilience expectations considering risk appetite, risk capacity and risk profile under a range of extreme yet plausible scenarios. The board is also expected to establish a clear communication network to bank personnel, third parties and intra-group entities to ensure firm-wide awareness of the operational resilience approach. Senior management is encouraged to implement the operational resilience approach ensuring appropriate allocation of resources and provide regular reports on the bank's operational resilience in each business unit.

PRINCIPLE 2 – OPERATIONAL RISK MANAGEMENT: *Banks should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with their operational resilience expectations.*

The principle recommends that the bank's operational risk management function work with other relevant functions in the bank to manage any risks that threaten the delivery of critical operations to yield greater harmonisation in operational resilience approach across the bank. Banks are also expected to establish sufficient controls and procedures to identify threats and vulnerabilities promptly. These controls and procedures are recommended to be regularly assessed to account for any changes in the underlying components of critical operations. Banks should leverage change management capabilities to assess potential effects on the delivery of critical operations.

PRINCIPLE 3 – BUSINESS CONTINUITY PLANNING & TESTING: *Banks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption.*

The principle recommends that banks establish a forward-looking business continuity plan to identify critical operations as well as key internal and external dependencies to assess the risks and potential impact of various disruption scenarios. Business continuity plans should provide detailed guidance for implementing the bank's disaster recovery framework as well as establish roles and responsibilities for managing operational disruptions with a clear plan for internal decision-making processes. Banks should ensure that all operational resilience efforts are harmonised with the business continuity plans to ensure the effective and efficient delivery of critical operations during disruption circumstances.

PRINCIPLE 4 – INTERCONNECTIONS & INTERDEPENDENCIES: *Once a bank has identified its critical operations, the bank should map the relevant internal and external interconnections and interdependencies to set operational resilience expectations that are necessary for the delivery of critical operations.*

The principle recommends that the bank's respective functions should map the personnel, technology, processes, information, facilities, interconnections and interdependencies needed to deliver critical operations with careful attention given to operations dependent upon third parties or intra-group entities. International banks should ensure that operational resilience efforts are harmonised with organisation mappings of critical operations across the bank. Organisational mappings should be sufficiently detailed to allow banks to easily identify vulnerability and test the bank's disruption capability to maintain the bank's risk tolerance.

PRINCIPLE 5 – THIRD-PARTY DEPENDENCIES: *Banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intra-group entities, for the delivery of critical operations.*

The principle recommends that the bank's respective functions conduct a risk assessment and due diligence before entering into third party or intra-group arrangements to ensure consistency with the bank's operational risk management framework, outsourcing risk management policy, and operational resilience expectations. Banks should also verify if the outsourcers have at-least equivalent operational resilience conditions to safeguard the bank's critical operations. Banks are recommended to formalise relationships with third parties and intra-group entities under base case and operational stress case scenarios with agreements reflecting the risk assessment and due diligence carried out. Banks should undertake scenario analysis under the BCP to assess the suitability of third parties that provide services to critical operations or other viable alternatives.

PRINCIPLE 6 – INCIDENT MANAGEMENT: *Banks should develop and implement response and recovery plans to manage incidents that could disrupt the delivery of critical operations in line with the bank's risk tolerance for disruption considering the bank's risk appetite, risk capacity and risk profile. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.*

The principle recommends that banks develop and implement response and recovery plans for different incidents which capture the life cycle of an incident. The incident response plans should include:

- the classification of an incident's severity
- the development, maintenance and testing of incident management procedures
- the implementation of communication plans to report incidents

Banks should periodically test incident response plans to ensure that effective learning is done based on the root cause and is duly reflected when periodically reviewing and updating the incident management program.

PRINCIPLE 7 – ICT MANAGEMENT: *Banks should ensure resilient ICT including cybersecurity that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant information to users on a timely basis in order to fully support and facilitate the delivery of the bank's critical operations.*

The principle recommends that banks have a documented ICT policy, including cybersecurity, with clear oversight requirements, risk ownership, and information security measures. Banks are also encouraged to identify critical information assets and infrastructure to prioritize cybersecurity efforts in critical operations. Banks should ensure that cybersecurity efforts observe all legal and regulatory requirements relating to data protection and confidentiality with plans developed to maintain the integrity of critical information in a cyber-event. When implementing appropriate controls to support remote-working and customer data protection, banks should ensure the confidentiality of information,

appropriate risk mitigation strategies for technology disruptions, and well-defined processes for the management of remote assets. Banks should ensure that ICT including cybersecurity is regularly updated to ensure the efficient delivery of critical operations during periods of disruption.

RESPONDING TO THE CONSULTATIVE DOCUMENT

The Basel Committee has invited a response from financial institutions to its Consultative Document in the form of the questions outlined below.

Questions on the Proposed Principles

1. Has the Committee appropriately captured the necessary requirements of an effective operational resilience approach for banks? Are there any aspects that the Committee could consider further?
2. Do you have any comments on the individual principles and supporting commentary?
3. Are there any specific lessons resulting from the Covid-19 pandemic, including relevant containment measures, that the proposed principles for operational resilience should reflect?
4. Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience?
5. What kind of metrics does your organisation find useful for measuring operational resilience? What data are used to produce these metrics?

HOW CAN REPLY ASSIST?

Given the rapidly changing geopolitical, economic, and technological environments, all banks and financial institutions should re-examine existing risk management practices, business continuity plans, and incident response and recovery plans to ensure operational resilience during times of crisis.

Avantage Reply supports clients with:

- reviewing and assessing governance frameworks to ensure operational resilience
- designing frameworks, policies and processes to monitor and manage operational risks
- designing, reviewing and assessing business continuity plans to ensure operational resilience under various scenarios

CONCLUSION

It has become increasingly clear in light of the Covid-19 pandemic as well as other recent geopolitical shifts, that banks and other financial institutions need to take a serious look at their approaches to operational resilience. Governments and regulators must encourage financial institutions to adjust existing operational risk management practice as well as re-examine business continuity plans, critical operations mapping, and incident response and recovery plans to ensure the continuation of critical operations during crises and delivery disruptions. To that end, financial institutions also have the opportunity to respond to the BCBS Consultative Document regarding any further changes that should be made to the PSMOR.

CONTACTS

Vishwas Khanna, Partner

Vishwas specialises in prudential regulation, risk transformations, programme leadership and new bank authorisations. He is a trusted advisor to the C-Suite and senior management at banks and offers objective, independent advice to his clients to influence strategic decision-making.

vi.khanna@reply.com

Hadrien van der Vaeren, Senior Manager

Hadrien is a senior risk management practitioner specialising in prudential regulation, regulatory reporting, quantitative risk modelling and data and systems implementations. He has experience of delivering complex risk programmes across UK and Europe.

h.vandervaeren@reply.com

Rohan Wilson, Manager

Rohan has significant experience leading regulatory change and risk management projects at key FS clients across challenger and investment banks. He has also supported a European regulator with their internal action plans for resolution of entities.

r.wilson@reply.com

Audrey Weber, Consultant

Audrey joined Avantage Reply after graduating from Cass Business School with a Master's degree in Actuarial Science and the University of Exeter with a Bachelor's in Economics and Finance. Audrey has been working on coding in Python (Regulatory Reporting tool) and on sustainable finance initiatives.

au.weber@reply.com

AVANTAGE REPLY

Avantage Reply, part of the Reply Group, specialises in Financial Services consulting with a focus on Risk Transformations, Treasury and Capital, Quantitative Modelling and Regulatory Advisory. With offices across Europe, Avantage Reply counts some of the world's most significant financial groups among its clients, including in Investment, Retail and Commercial Banking, Custodian Banking, Insurance and Investment Management.