REGULATORY UPDATE - ZAGREB APRIL 2020
Policy note drafted by the Eurofi Secretariat

Ensuring operational resilience at entity and industry level (cyber, outsourcing, operational risks...)

Operational resilience has a broader reach than IT disruption or recovery and resolution

The theme of operational resilience relates to issues that have been the focus of the industry and regulators much before the Covid 19 outbreak, such as business continuity planning, outsourcing, cybersecurity or recovery and resolution. In a recent public speech, Christine Lagarde, the Head of the European Central Bank ("ECB"), has emphasized that the ECB "had a duty to be prepared and to act pre-emptively[1]" to strengthen resilience at the Industry level. The principle of operational resilience is indeed not new. In 2013, in its *Guidance on Identification of Critical Functions and Critical Shared Services*, the FSB warned that failure to provide a critical function or a critical service would be likely to have a material impact on third parties, give rise to contagion or undermine the general confidence of market participants. In 2014, the European Parliament stated in the "BRRD" that Operational continuity is fundamental to maintain services that are essential to the real economy or not to disrupt financial stability due to the size, market share, external and internal interconnectedness of institutions[2]. Resolution tools were defined in order to fail orderly, i.e. to enable failing Institutions to maintain core business lines without disrupting Financial Stability. In 2015, the EBA outlined in its *Comparative report on the approach to determining critical functions and core business lines in recovery plans* that critical functions were of systemic importance, low substitutability and whose discontinuity might have significant impacts on third parties and on the market[3]. Recovery plan had to be set up to ensure continuation of Critical Function under a stress situation.

In July 2018, the Bank of England, the Prudential Regulation Authority ("PRA") and the Financial Conduct Authority ("FCA") published a discussion paper that addressed directly the theme of operational resilience with a broader reach than IT disruption or recovery and resolution. This Discussion Paper defines operational resilience as "the ability of firms, FMIs and the sector as a whole to prevent, respond to, recover and learn from operational disruptions[4]". This ability is required for any firm and for any disruption of service that "has the potential to cause harm to consumers and market participants, threaten the viability of firms and FMIs, and cause instability in the financial system[5]".

The financial industry rather than identifying most important services and improving their ability to recover, has focused so far on an operational risk capital framework

The Covid 19 crisis shed a new light on operational resilience, showing how much the economy was vulnerable to an external shock and how little it was prepared to respond. The focus, to date, of operational risk management in the financial industry, has been on setting up an operational risk capital framework and on the monitoring and prevention of operational risk. Not enough focus and means have been invested on operational resilience, e.g. the ability to recover and respond assuming disruption will occur. The core requirements of operational resilience represent a substantial undertaking for firms to implement.

First a clear understanding of the most important business services is required. This understanding should rely on the mapping of the systems, facilities, people, processes and third parties that support those business services.

Second, firms need to identify how the failure of an individual system or process could impact the provision of business services and assess to what extent these systems or processes are capable of being substituted during disruption so that business services can continue to be delivered.

An assessment of vulnerabilities and concentration risk is then possible. An impact tolerance, the level of disruption than can be tolerated on the provision of the business service, should be defined and set by senior management. Tested plans including internal and external communication would then enable firms to continue or resume business services when disruption occur.

A comprehensive operational risk framework would rely on the definition of the appropriate strategy, governance, and operating model including the ownership of business services, the setting of tolerance, scenario development and testing, definition of role and responsibilities and communication strategy. Ultimately, business as usual processes shall be modified to integrate resilience by design.

Increased scrutiny of supervisors is anticipated

However, for most advanced banks or financial institutions, operational resilience is not totally new. Changing technologies and complexity of cyber threats, increased use of outsourcing and dependence on specific suppliers increase vulnerabilities. The scrutiny of European supervisors on resilience matters is however likely to be increased. Before Covid-19 crisis, UK prudential authority announced that operational resilience stress testing and sectorial exercises would be conducted as well as self-assessments. Lastly, even if a proportionality principle was stated, the British Prudential Authority warned that in some cases impact tolerances metrics might be imposed.

Likewise, at European scale, we should expect greater attention on resilience matters from supervisors. Even before the Covid-19

[1] Remarks on the occasion of receiving the Grand Prix de l'Économie 2019 from Les Echos, Speech by Ms Christine Lagarde, President of the European Central Bank, at the "Grand Prix de l'Économie des Echos pour l'année 2019", Paris, 5 February 2020

[2] BRRD – Directive 2014/59/EU of the European Parliament and of the Council

[3] EBA - Comparative report on the approach to determining critical functions and core business lines in recovery plans

[4] Discussion Paper « Building the UK financial sector's operational resilience", Prudential Regulation Authority (PRA) DP01/18, July 2018, §1.4

[5] Discussion Paper « Building the UK financial sector's operational resilience", Prudential Regulation Authority (PRA) DP01/18, July 2018, §1.6

crisis, in November 2018, the International Conference of Banking Supervisors reminded in the conclusions of a workshop dedicated to Cyber security and operational resilience that cyber resilience "should be embedded in [the] day-to-day activities so as to build processes, services and products that are secure by design.[6]"

However, lack of ready-made guidance to operationalise the resilience was somewhat acknowledged by the BCBS who made clear that it aimed to "provide a more concrete and specific understanding of the main trends, progress and gaps in the pursuit of cyber-resilience in the banking sector[7]". In the end of 2018, expectations effectively became more detailed with the ECB Guidance on *Cyber resilience oversight expectations for financial markets infrastructure* which aimed at "operationalize the Guidance, ensuring [that Firms] are able to foster improvements and enhance their cyber resilience over a sustained period of time[8]". A first positive stage has been completed. The same kind of approach will have to be pursued as regard to the broader operational resilience of financial institutions after Covid-19 crisis.

Some lessons learned from Covid-19 crisis

Some lessons learned from Covid-19 crisis can be leveraged in this perspective:

- **The efficiency of small interconnected teams to manage the crisis**. Small collaborating teams are more responsive to cover a wide range of topics (IT support to remote work, IT maintenance and infrastructure, digital business services to clients, relations with supervisors etc.) and adapt more quickly to evolving situations.
- **The knowledge of the main firm assets.** It is worth using firm's assets all along the crisis to maintain business services running. A detailed and updated inventory of firm's assets may enable to know if any relevant resource can be used to fulfil any operational need during the crisis.
- **The ability to rely on as updated as possible data.** In a crisis context, in which prompt decisions need to be taken by the firm's management, data needs to be as accurate as possible should it has to support smart decisions. This stake is crucial for major groups with multiple branches in various locations.
- **The importance of maintaining an open dialogue with third parties.** A clear and constant dialogue with regulators, public sector stakeholders, business partners, contractors, etc. allows to set up and adjust urgent action plans, if necessary, in a timely manner.

Covid-19 crisis will ultimately serve as an accelerator to identify sound practices to improve the resilience of financial firms. After the crisis, worldwide supervisors will probably rely on financial institutions experience feedback to set up operational rules and guidance.

[6] ICBS 2018, Workshop 6 Cyber-security and Operational resilience, §« From Cyber-security to operational resilience », p.3

[7] ICBS 2018, Workshop 6 Cyber-security and Operational resilience, §Basel Committee work on operational resilience, p.5

[8] Cyber resilience oversight expectations for financial markets infrastructure, §1.2 « Purpose », p.3 – December 2018