

|

The England and Wales Chapter
of the
Institute of Operational Risk

Operational Resilience
Covid-19 - Lessons Learned
(The Story So Far)

9 June 2020

Covid-19 - Lessons Learned

As 2019 moved to a close, operational resilience discussions in the UK focused on reviewing and responding to the consultation papers issued by the PRA¹ and FCA² and developing operational resilience frameworks, in the main designed to respond to cyber and IT issues. Indeed, the England and Wales Chapter drafted a response to the now delayed consultation and a webinar is being planned to share and consult on the proposed response with the membership. Six months later the Covid-19 pandemic has had unprecedented impacts, including widespread working from home across firms with staff undertaking activities not previously considered as suitable for out of the office.

Whilst the pandemic was not on many firms lists of top operational risks, parts of the banking system have proved very resilient with markets open, payments being made, websites operating, ATMs full, call centre capacity increased and branches operating. As a result, so far, Covid-19 related operational risk events in the public domain for financial services have been very limited. Banks continue to defend against an increase in cyber-crime although retail customers may have fared less well.

Those banks that have demonstrated resilience are those that had well developed pandemic and other recovery plans and have successfully utilised recovery sites, redirected work to other less impacted offices, introduced shift patterns and remote working and triaged non-critical activities. These plans were partially in place due to regulatory pressure from the UK Financial Services Authority at the start of the century and also because the international banks had first-hand experience of SARS and swine flu in their Asian offices. The banks have also been very collegiate - discussing their issues and sharing their solutions amongst themselves, as the crisis continues to develop.

With many pandemic plans being developed, implemented, evolved and live tested during the crisis the England and Wales Chapter of the Institute of Operational Risk feel members could benefit from an insight into some of the actions that firms have undertaken as a result of Covid-19. These actions fall into two categories, actions that should be ongoing after the pandemic is over and actions that should be part of any pandemic response.

Some of the measures that firms have taken during the pandemic should be retained on an ongoing basis to ensure that firms can respond quickly to future pandemics and business continuity incidents:

- Pandemic planning - pandemic plans are, as we have seen above, key and should be constantly refreshed and updated. Sole reliance on Business Continuity Plans (BCP) is significantly less effective, as the

¹ Operational resilience: Impact tolerances for important business services, December 2019 (CP29/19)

² Building operational resilience: Impact tolerances for important business services and feedback to DP18/04, December 2019 (CP19/32)

pandemic has impacted across multiple locations and countries while BCP relates to coping with denial of something e.g. buildings or staff or IT etc. In this instance in the UK denial is primarily access to buildings due to lockdown and secondarily some loss of staff capacity due to primary school closures and concerns over loss of suppliers. Pandemic plans should include full and up-to-date details: the crisis management team; communication arrangements for staff, customers, third parties and regulators; pandemic scenarios for risk management; and lessons learned processes;

- Pandemic scenarios – firms that had regularly run comprehensive and detailed pandemic scenarios with senior management participation to test both the capital and risk management impacts of a pandemic were better prepared for Covid-19 than those that had not. Many firms are currently actively running severe but plausible scenarios on a second wave of Covid-19. These scenarios should be run and tested on an ongoing basis and should include pandemics with even more impact than has been seen this year. Globally other viruses have been seen that have the ability to prove more damaging than Covid-19;
- Red and blue teams – at the start of the pandemic many firms assigned staff to red and blue teams, with the aim of one team working in the office while the other worked from home. While the nature of the pandemic did not result in these teams being utilised for long, if at all, this is a useful discipline that can be triggered quickly and should be retained;
- Working from home – not all firms had the ability to switch seamlessly to all staff working from home and the first few weeks of the pandemic saw some firms moving quickly to ensure all staff had the technical ability to work away from the office. Going forward firms should ensure that all staff can work from home with no advance warning and staff should be required to demonstrate they can do so on a regular basis. As part of this process firms should regularly test their systems to ensure that they have sufficient bandwidth to enable all staff to work out of the office;
- Video conferencing – with staff working from home, video conferencing has become increasingly important as a means of communicating with staff, taking decisions and ensuring staff well-being. Security concerns have been expressed with regard to some video conferencing software and firms should therefore ensure all staff have access to secure video conferencing facilities;
- Staff training and awareness - many firms have responded to the changing risk profile by increasing staff training and awareness, particularly in the areas of conduct and behaviour, information security and phishing. This training should be maintained to enable firms to move seamlessly to working from home.

Firms have also introduced measures in response to the pandemic that have helped them manage and mitigate pandemic specific issues. These actions include:

- Responding to changes in the risk profile - risk profiles have changed significantly as staff has worked from home and some activities have been undertaken out of the office for the first time, including in some cases dealing and trading. Firms have needed to respond in a number of ways, including: developing new controls; increasing control monitoring; heightening monitoring and management of conduct risk; improving monitoring and management of internal and external fraud, including money laundering; and strengthening cyber-crime controls to protect the organisation and its customers. In addition control exceptions have required formal governance arrangements and recording;
- New products and responding to customer needs – firms have responded quickly and positively to customer demands (e.g. increased liquidity) and retail banks successfully rolled out new products to tens of millions in an extremely short time frame after announcements by government to support the economy during the lockdown. In addition, technical developments that were designed to improve service and reduce costs have also helped banks to be more resilient e.g. the rise of cards and contactless payments and on-line banking and the associated decline of cheques, cash and branch banking;
- Communications – firms have increased communications to various parties including customers, staff, third parties and for regulated firms, their supervisors, often several times during the day. Retail firms for example have devoted considerable attention to reassuring customers, providing details of product and service availability and how the organisation could be contacted at a time when call centres may be operating at reduced staff levels. Initially these communications were often based on pandemic scenarios and business continuity plans. These communication plans have evolved as the pandemic continues;
- Third parties - firms have needed to ensure that third party arrangements continue to operate in accordance with approved parameters, third parties themselves were able to manage the pandemic and that communication channels with all suppliers were maintained and effective;
- Crisis management and lessons learned - pandemic issues were monitored and lessons learned were constantly collected and considered with a formal process implemented to ensure that mitigating actions were agreed and implemented. While we are not aware of any banks that had included in their pandemic plans how they would emerge from lockdown the pace of the pandemic has given firms time to plan and respond. These lessons learned should feed into the pandemic and business continuity plans.

The Institute of Operational Risk: <https://www.ior-institute.org>