Financial Stability Institute | BIS

FSI Briefs

No 2

Covid-19 and operational resilience: addressing financial institutions' operational challenges in a pandemic

Rodrigo Coelho and Jermy Prenio

April 2020

FSI Briefs are written by staff members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), sometimes in cooperation with other experts. They are short notes on regulatory and supervisory subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS or Basel-based standard setting bodies.

Authorised by the Chairman of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2708-1117 (online)
ISBN 978-92-9259-364-3 (online)

Covid-19 and operational resilience: addressing financial institutions' operational challenges in a pandemic[1]

Highlights

- *Guidance issued by financial sector authorities in response to the Covid-19 crisis seems to suggest that international efforts to come up with operational resilience standards should take into account at least the following elements:*

– *Critical/essential employees: identifying the critical functions and employees that support important business services, as well as ensuring employees' safety and that they can safely resume their duties (remotely, if necessary).*

– *IT infrastructure: ensuring that IT infrastructure can support a sharp increase in usage over an extended period and taking steps to safeguard information security.*

– *Third-party service providers: ensuring that external service providers and/or critical suppliers are taking adequate measures and are sufficiently prepared for a scenario in which there will be heavy reliance on their services.*

– *Cyber resilience: remaining vigilant in order to identify and protect vulnerable systems, and detect, respond and recover from cyber attacks.*

1. Introduction

Financial institutions have to deal with two challenges in the face of the Covid-19 pandemic. The first challenge is financial – how to address and mitigate the sharp drop in the value of financial assets or loss of liquidity. The second challenge is operational – how to address the risk of failure of resources (people, processes, technology, facilities and information) to deliver business services.

Financial sector authorities are concerned with both sets of challenges, given that the response of financial institutions has implications for the provision of the financial services that support the economy. Since the onset of the Covid-19 pandemic, some authorities have issued guidance to help financial institutions address these challenges. This paper looks at some of the initiatives that are specifically aimed at helping address operational challenges and ensuring business continuity.

Business continuity and pandemics

Supervisory guidance on business continuity is typically aimed at restoring business processes after relatively short disruptions, such as those caused by natural disasters and infrastructure failures, or by cyber and terrorist attacks. Operational disruptions caused by pandemics, however, may pose different challenges. The duration of a pandemic could be weeks or even months and its impact is widespread, perhaps global. A pandemic could also occur in multiple waves and not just as a one-off incident. It may not directly harm physical or IT infrastructure but it could lead to staff shortages. Traditional business continuity measures such as backup locations for critical business processes may also prove ineffective.

[1] Rodrigo Coelho (Rodrigo.Coelho@bis.org) and Jermy Prenio (Jermy.Prenio@bis.org). The authors are grateful to Greg Sutton for helpful comments and insights and to Dmitrijs Randars for administrative support.

Incidents similar to Covid-19 have happened in the recent past, eg SARS in 2002–03 and swine flu in 2009–10, and the affected jurisdictions already have guidance in place on how financial institutions can maintain business continuity. These jurisdictions are now revisiting their guidance in the face of the Covid-19 pandemic and are making updates, as necessary.

At the international level, the Joint Forum's high-level principles for business continuity issued in 2006 were motivated partly by the SARS experience and included case studies on the experience of handling the outbreak in Canada and Hong Kong SAR.[2] The Basel Committee on Banking Supervision's *Principles for the sound management of operational risk* explicitly mention a pandemic as one of the scenarios to take account of in business continuity planning.

More recently, supervisory discussions have shifted towards achieving operational resilience more broadly, of which ensuring business continuity is one element. The Bank of England, for example, issued a December 2019 consultation paper describing its operational resilience expectations for financial institutions and financial market infrastructures. Similar discussions are also ongoing at the international level. However, these discussions are driven largely by the challenges and vulnerabilities brought about by technological change and an increasingly hostile cyber environment. While the scenarios to be taken into account for ensuring operational resilience are quite broad, at least in the case of the Bank of England consultation, the specific experience of dealing with a pandemic such as Covid-19 may have to be considered in any future supervisory guidance relating to operational resilience.

This paper focuses on (1) examples of business continuity guidance issued by authorities in response to Covid-19, including updates to existing guidance; and (2) how pandemic scenarios could be incorporated in testing operational resilience.

2. Business continuity guidance to address the Covid-19 pandemic

A number of authorities have issued business continuity guidance in response to Covid-19, including updates to their existing regulatory framework. These recommendations typically relate to the "preparing" and "responding" phases of a business continuity plan and fall under the following categories:

- ensuring customer and staff safety;
- reviewing the appropriateness of contingency plans to address a pandemic scenario;
- assessing telecommuting capabilities and increasing cyber resilience;
- identifying critical financial workers;
- coordinating with critical third-party service providers; and
- maintaining clear communication with internal and external parties.

Ensuring customer and staff safety

Several authorities have issued guidance to promote the safety of customers and staff. The Monetary Authority of Singapore (MAS (2020b)), for example, has requested financial institutions to implement safe distancing measures in all aspects of their business operations, especially customer touch points. Similarly,

[2] See Joint Forum (2006) for more information. The Joint Forum was established in 1996 under the aegis of the Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS) to deal with issues common to the banking, securities and insurance sectors, including the regulation of financial conglomerates

the Federal Financial Institutions Examination Council (FFIEC (2020)) recommends that banks consider providing employees with appropriate hygiene training and tools and implementing social distancing techniques to reduce face-to-face contact by using, for example, teleconference calls, flexible work hours and telecommuting. The European Central Bank (ECB (2020)) calls for banks to establish adequate measures of infection control in the workplace and highlights the importance of worker education. With the same objective, the Central Bank of the United Arab Emirates (CBUAE (2020)) directs banks to replenish automated teller machines (ATMs) with unused banknotes.[3]

A number of authorities have also recommended that financial institutions reduce traffic at bank branches and have encouraged customers to use alternative service options for access to financial services. The Federal Deposit Insurance Corporation (FDIC (2020)) and FFIEC (2020), for example, suggest that banks remind customers of the various channels for accessing banking services without physically coming to a branch, such as managing their accounts online, performing transactions at an ATM and using online and telephone banking. Similarly, MAS (2020b) recommends that banks encourage all customers to use electronic platforms for financial transactions and to take other measures to reduce traffic at branches such as limiting the number of people waiting at the premises and ensuring a minimum separation between customers.

Reviewing appropriateness of contingency plans to address a pandemic scenario

Some authorities have advised banks to review the appropriateness of their contingency plans to address risks arising from a pandemic scenario and to take relevant actions. Bank of Italy (2020), ECB (2020) and the Netherlands Bank (DNB)[4] have called upon financial institutions to assess to what extent contingency plans appropriately include a pandemic scenario, encouraging banks to take the necessary actions to minimise the potential adverse effects of the spread of Covid-19. ECB (2020) also urges banks to assess how quickly measures foreseen under the pandemic scenario could be implemented and how long operations could be sustained under such a scenario. The Bank of England has informed the public (BoE (2020)) that it was reviewing the contingency plans of banks, including assessments of operational risks and the ability of these firms to serve customers and markets with split teams and remote working.

Authorities recommend that the strategy to deal with the pandemic includes a range of actions that can be deployed depending on the severity of the various possible scenarios. ECB (2020) encourages banks to consider scenarios that provide for scaling measures commensurate with the institution's geographic footprint and business risk for the particular stages of a pandemic. Similarly, FFIEC (2020) requires banks to have a documented strategy that includes actions that are consistent with the effects of a particular stage of a pandemic, such as the six intervals described by the Centers for Disease Control and Prevention (2016). DNB recommends that banks consider various adverse scenarios, including the absence of 30% or more of staff.[5]

Assessing telecommuting capabilities and increasing cyber resilience

Several authorities have urged banks to test their IT and other critical capabilities to consider the additional strains resulting from the increased use of online banking and remote working arrangements. ECB (2020), for example, advises banks to assess and urgently test their existing IT infrastructure in the light of large-scale remote working arrangements and a potentially higher reliance on remote banking services. Similarly,

[3] See Auer et al (2020) for other guidance issued by central banks in relation to the provision and handling of banknotes.

[4] Please see De Koning (2020) for recent guidance issued by DNB.

[5] According to *The Implementation Plan for the National Strategy for Pandemic Influenza*, in a severe pandemic, absenteeism attributable to illness, the need to care for ill family members and fear of infection may reach 40% during the peak weeks of an outbreak. This number could be even higher if certain public health measures such as closing schools and quarantining household are taken.

DNB and MAS (2020a) call on financial institutions to anticipate and be prepared to manage any increase in demand for online financial services as a result of changes in the behaviour and preferences of customers and staff.

A number of authorities have also called on banks to enhance their cyber resilience efforts. ECB (2020) recommends that banks proactively assess and test the capacity of existing IT infrastructure, in the light of a potential increase of cyber attacks. In the same way, MAS (2020a) reminds financial institutions that they should remain vigilant on the cyber security front as there have been cases of cyber threat actors taking advantage of the current situation to conduct email scams, phishing and ransomware attacks. Dubai Financial Services Authority (2020) encourages banks to exercise vigilance with respect to cyber threats. It also calls on them to register to use the DFSA Cyber Threat Intelligence Platform (TIP) and make use of the cyber threat information available on TIP to enhance their cyber security.

Identifying critical financial workers

A key financial worker or a critical worker fulfils a role that is necessary for the bank to continue to provide essential financial services to consumers, or to ensure the continued functioning of payment systems and markets. In order for these individuals to be able to perform their roles, they might have to be exempted from some of the restrictions imposed by public authorities in response to the pandemic, such as access restrictions to workplaces.

At least two authorities have issued guidance to assist banks in identifying critical staff. The Prudential Regulation Authority (2020) suggests that financial institutions should first identify the activities, services or operations, which are likely to lead to the disruption of essential services to the real economy or financial stability. Banks would then identify the individuals that are essential to support these functions. Similarly, the Board of Governors of the Federal Reserve System (2020) issued a statement that referred to the Cybersecurity and Infrastructure Security Agency (CISA) guidance on this topic to inform banks that the CISA had identified a number of jobs in the financial services sector as essential, including, for example, workers who are needed to provide consumer access to banking and lending services.

Members of the Financial Stability Board (FSB) recently discussed[6] the critical nature of many financial services and the importance of ensuring access to the workplace for a limited number of essential personnel performing functions such as providing consumer access to cash, electronic payments and other banking and lending services; as appropriate, keeping branches and call centres open; processing claims under government support programmes; insurance services; risk management; supporting financial operations, such as staffing data and security operations centres; and supporting third-party providers of core services.

Coordinating with critical third-party service providers

Several authorities have highlighted the importance of successful coordination with critical suppliers and service providers. ECB (2020), for example, recommends that banks enter into a dialogue with critical service providers to understand how services continuity would be ensured in case of a pandemic. FFIEC (2020) highlights that management should monitor its service providers, identify potential weaknesses in the service and supply chains, and develop potential alternatives for obtaining critical services and supplies. In the same way, DNB recommends that banks verify that critical suppliers and service providers have taken adequate measures and are sufficiently prepared for a pandemic.

[6] See FSB (2020) for more details.

Maintaining clear communication with internal and external parties

A number of authorities have drawn attention to the need for banks to communicate clearly with internal and external parties. FFIEC (2020) asserts the role of senior management in disseminating the strategy in response to the pandemic to ensure that employees understand their role and responsibilities in responding to a pandemic event. FDIC (2020) advises banks to inform customers of the availability of services and operating hours, by, for example, posting this information on the institution's website, providing recorded information on its customer support lines and pushing notifications out to customers who have signed up for alerts.

3. Incorporating pandemic scenarios in testing operational resilience

Supervisory discussions at the international level have recently shifted towards achieving operational resilience more broadly. The Bank of England is the first national authority to issue a consultation on its operational resilience expectations. It defines operational resilience as the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover from and learn from operational disruptions. Its consultation paper requires that firms identify their important business services (ie services provided to users),[7] map the resources necessary to deliver these services and set and test its impact tolerances[8] to various potential disruption scenarios. It also requires that firms implement sound operational risk management, business continuity and outsourcing frameworks to ensure that they are able to remain within its operational resilience impact tolerances.

The objective of addressing financial institutions' operational resilience to IT outages and cyber attacks has clearly motivated the Bank of England consultation as well as international supervisory discussions. However, as seen in the disruption that Covid-19 has caused in recent weeks, financial institutions need to review and ensure that their operational resilience procedures are also fit for purpose during pandemics. As shown in the various supervisory guidance issued recently in relation to Covid-19, pandemics may have unique elements that financial institutions need to incorporate in the scenarios to test their operational resilience.

- **Critical/essential employees.** A pandemic could lead to significant absenteeism rates that may affect the critical functions necessary to deliver important business services. In this regard, it is important to identify the critical functions and employees who support important business services, as well as ensure employees' safety. Financial institutions should also ensure that employees can safely resume their duties (remotely, if necessary) so that business services can recover as quickly as possible.
- **IT infrastructure.** A pandemic could lead to pressure on a financial institution's IT infrastructure over an extended period due to work-from-home arrangements made necessary by quarantine or social distancing guidelines. In this regard, financial institutions should ensure that their IT infrastructure can support this sharp increase in usage and take steps to safeguard information security.
- **Third-party service providers.** A pandemic could lead to worldwide reliance on services provided by third parties (eg tele/video-conferencing services and internet providers for client-facing online services). In this regard, financial institutions should also ensure that their external

[7] Important business services are services that, if disrupted, would pose a risk to the stability of the UK financial sector, the firm's safety and soundness, or, in the case of insurance firms, the appropriate degree of policyholder protection.

[8] Impact tolerance is the maximum acceptable level of disruption to important business services (eg maximum tolerable duration for which the delivery of the important business service would be affected).

service providers and/or critical suppliers are taking adequate measures and are sufficiently prepared for such a scenario.

- **Cyber resilience.** A pandemic could lead to an increase in cyber attacks due to extensive use of financial institutions' IT infrastructure, third-party and client-facing online services. Threat actors might also take advantage of the general panic and confusion. In this regard, financial institutions' cyber resilience processes should remain vigilant in order to identify and protect vulnerable systems. These processes should also be able to detect and respond to cyber attacks and help the institution recover from them.

4. Concluding remarks

Experience in addressing the operational challenges faced by financial institutions in past outbreaks is a good starting point for addressing the challenges posed by the Covid-19 pandemic, especially for jurisdictions that have no experience with similar incidents. But a pandemic on this scale presents unique challenges given its global repercussions and potential duration. Authorities around the world are now coming to terms with these unique challenges. International efforts to come up with operational resilience standards should also take these challenges explicitly into account.

References

Auer, R, G Cornelli and J Frost (2020): "Covid-19, cash, and the future of payments", *BIS Bulletin*, no 3, April.

Bank of England (2019): *Consultation Paper 29/19: Operational resilience: Impact tolerances for important business services*, December.

——— (2020): *Governor statement to Treasury Select Committee, on behalf of the FPC, MPC and PRC*, March.

Bank of Italy (2020): *Extension of deadlines and other temporary measures to mitigate the impact of Covid-19 on the Italian banking and financial system*, March.

Basel Committee on Banking Supervision (2011): *Principles for the sound management of operational risk*, June.

Board of Governors of the Federal Reserve System (2020): *SR 20-6: Identification of essential critical infrastructure workers in the financial services sector during the Covid-19 response*, March.

Centers for Disease Control and Prevention (2016): *Pandemic intervals framework (PIF)*, November.

——— (2017): *National pandemic influenza plans*, June.

Central Bank of the United Arab Emirates (2020): *CBUAE directs banks to replenish ATMs with new banknotes*, March.

Cybersecurity and Infrastructure Security Agency (2020): *Advisory memorandum on identification of essential critical infrastructure workers during Covid-19 response*, March.

De Koning, N (2020): "DNB on business continuity plans for Coronavirus (Covid-19)", *Regulation tomorrow*, March.

Dubai Financial Services Authority (2020): *DFSA Supports the UAE government's measures to address the challenges of Covid-19*, March.

European Central Bank (2020): *Contingency preparedness in the context of Covid-19*, March.

Federal Deposit Insurance Corporation (2020): *Frequently asked questions for financial institutions affected by the Coronavirus disease 2019 (Referred to as Covid-19)*, March.

Federal Financial Institutions Examination Council (2020): *Interagency statement on pandemic planning*, March.

Financial Stability Board (2020): *FSB members take action to ensure continuity of critical financial services functions*, April.

Joint Forum (2006): *High-level principles for business continuity*, August.

Monetary Authority of Singapore (2020a): *MAS advises financial institutions to adopt recommended measures for DORSCON Orange*, February.

——— (2020b): *MAS tells financial institutions to adopt safe distancing measures*, March.

Prudential Regulation Authority (2020): *Statement by the PRA on key financial workers who are critical to the Covid-19 response*, March.