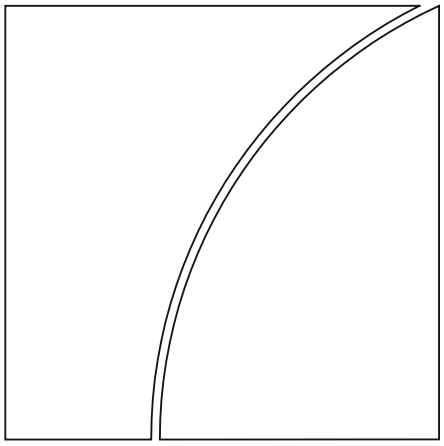
Basel Committee on Banking Supervision



Consultative Document

Principles for operational resilience

Issued for comment by 6 November 2020

August 2020

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-418-3 (online)

Contents

Principles for operational resilience

I. Introduction

1. In the years that followed the Great Financial Crisis (GFC) of 2007-2009, the Committee's reforms of its prudential framework have enhanced the supervision of the global banking system and resulted in a number of structural changes to strengthen banks' financial resilience. While significantly higher levels of capital and liquidity have improved banks' ability to absorb financial shocks, the Committee believes that further work is necessary to strengthen banks' ability to absorb operational risk-related events, such as pandemics, cyber incidents, technology failures or natural disasters, which could cause significant operational failures or wide-scale disruptions in financial markets. In light of the critical role that banks play in the operation of the global financial infrastructure, increasing their resilience would provide additional safeguards to the financial system.

2. Even prior to the Covid-19 pandemic, the Committee considered that significant operational disruptions would inevitably test improvements to the financial system's resilience made since the GFC. As the Covid-19 pandemic progressed, the Committee observed banks rapidly adapting their operational posture in response to new hazards or changes in existing hazards that occurred in different parts of their organisation. Recognising that a range of potential hazards cannot be prevented, 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 severe adverse impacts.

3. Through the publication of this consultative document, the Committee seeks to promote a principles-based approach to improving operational resilience. The approach builds on updates to the Committee's Principles for the Sound Management of Operational Risk (PSMOR),[1] and draws from previously issued principles on corporate governance for banks, as well as outsourcing-, business continuity- and relevant risk management-related guidance. The concurrent publication of the PSMOR and principles for operational resilience provides an opportunity to consider further streamliming of the Committee's set of related guidance in this area. The Committee also intends to use the consultation process to reflect any initial lessons learned from the impact of the Covid-19 pandemic.

4. Recognising the work undertaken by several jurisdictions and standard-setting bodies to bolster the operational resilience of the financial sector,[2] the Committee aims to strengthen operational resilience by furthering international engagement and seeks to promote greater cross-sectoral collaboration over this body of work.

[1] *Consultative Document: Revisions to the principles for sound management of operational risk,* 6 August 2020, https://www.bis.org/bcbs/publ/d508.htm

[2] Bank of England and Financial Conduct Authority, *Building the UK financial sector's operational resilience (December 2019);* The European Commission, *Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure* (December 2019); the Monetary Authority of Singapore, *Ensuring Safe Management and Operational Resilience of the Financial Sector* (April 2020), and the International Organization of Securities Commissions (IOSCO), Principles on Outsourcing (May 2020).

5. Comments on this consultative document should be submitted by 6 November 2020 via: www.bis.org/bcbs/commentupload.htm. All comments may be published on the website of the Bank for International Settlements unless a respondent specifically requests confidential treatment.

II. An evolving operational risk landscape

6. Until recently, some of the most predominant operational risks that banks faced resulted from vulnerabilities related to the rapid adoption of and increased dependency on technology infrastructure for the provision of financial services and intermediation, as well as the sector's growing reliance on technology-based services provided by third parties. The Covid-19 pandemic has exacerbated these operational risks and increased economic and business uncertainty.

7. Pandemic-related disruptions have affected information systems, personnel, facilities and relationships with third-party service providers and customers. In addition, cyber threats (ransomware attacks, phishing, etc) have spiked, and the potential for operational risk events caused by people, failed processes and systems has increased as a result of greater reliance on virtual working arrangements. The Committee's guidance on operational resilience will continue to be informed by its monitoring of the impact of the Covid-19 pandemic and any lessons learned.

III. Essential elements of operational resilience

8. Operational resilience is an outcome that benefits from the effective management of operational risk. [3] Activities such as risk identification and assessment, risk mitigation (including the implementation of controls) and ongoing monitoring work together to minimise operational disruptions and their effects. An operationally resilient bank is less prone to incur untimely lapses in its operations and losses from disruptions, thus lessening their impact on critical operations and their related services, functions and systems. While it may not be possible to avoid certain operational risks, such as a pandemic, it is possible to improve the resilience of a bank's operations to such events.

9. In addition, business continuity,outsourcing of services to third parties and the technology upon which they rely are important factors for banks to consider when strengthening their operational resilience. Previously issued guidance in these areas, whether issued solely by the Committee[4] [5] or jointly with other standard setting bodies (SSBs),[6, 7] does not adequately capture all essential

[3] See Basel Committee on Banking Supervision, *Consultative Document: Revisions to the principles for sound management of operational risk*, paragraph 5, 2020

[4] Basel Committee on Banking Supervision, *Risk management principles for electronic banking,* July 2003, www.bis.org/publ/bcbs98.pdf.

[5] Basel Committee on Banking Supervision, *Corporate governance principles for banks*, July 2015, www.bis.org/publ/bcbs.pdf.

[6] The Joint Forum (BCBS, IOSCO, IAIS), *Outsourcing in Financial Services,* February 2005, www.bis.org/publ/joint12.pdf.

[7] The Joint Forum (BCBS, IOSCO, IAIS), *High-level principles for business continuity,* August 2006, www.bis.org/publ/joint17.pdf.

elements when considered on a standalone basis, but does advance operational resilience when considered collectively.

10. It is essential for banks to ensure that existing risk management frameworks, business continuity plans and third-party dependency-management are implemented consistently within the organisation. Internationally active banks should consider whether their operational resilience efforts are appropriately harmonised with the stated actions, organisational mappings, and definitions of critical functions and critical shared services contained in their recovery and resolution plans as specified in the Financial Stability Board's (FSB) Recovery and Resolution Planning framework.[8]

11. The principles for operational resilience set forth in this consultative document are largely derived and adapted from existing guidance that has already been issued by the Committee or national supervisors over a number of years.[9] The Committee recognises that many banks have well-established risk management processes that are appropriate for their individual risk profile, operational structure,corporate governance and culture, and conform to the specific risk management requirements of their jurisdictions. By building upon existing guidance and current practices, the Committee is proposing a pragmatic, principles-based approach to operational resilience that will help to ensure proportional implementation across banks of various size, complexity and geographical location.

IV. Definition of operational resilience

12. The Committee 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. In considering its operational resilience, a bank should take into account its overall risk appetite, risk capacity and risk profile.[10]

[8] See FSB *Key Attributes of Effective Resolution Regimes for Financial Institutions (October 2014)* (http://www.fsb.org/wp-content/uploads/r_141015.pdf), relevant supporting guidance in *Identification of Critical Functions and Critical Shared Services (July 2013)* (http://www.fsb.org/wp-content/uploads/r_130716a.pdf), and *Guidance on Arrangements to Support Operational Continuity in Resolution (August 2016)* (https://www.fsb.org/wp-content/uploads/Guidance-on-Arrangements-to-Support-Operational-Continuity-in-Resolution1.pdf).

[9] See eg Bank of England and Financial Conduct Authority, *"Building the UK financial sector's operational resilience" (December 2019);* The European Commission, *Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure* (December 2019); the Monetary Authority of Singapore*, Ensuring Safe Management and Operational Resilience of the Financial Sector* (April 2020), and the International Organization of Securities Commissions (IOSCO), Principles on Outsourcing (May 2020).

[10] See the Committee's 2015 *Corporate governance guidelines*, which leverage the FSB's 2013 *Principles for an effective risk appetite framework* to define "Risk appetite" as the aggregate level and types of risk a bank is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan; "risk tolerance" to refer to the variation around the prescribed risk appetite that the bank is willing to tolerate, and "risk capacity" which is the maximum level of risk the financial institution can assume given its current level of resources before breaching constraints determined by regulatory capital and liquidity needs, the operational environment (e.g. technical infrastructure, risk management capabilities, expertise) and obligations, also from a conduct perspective, to depositors, policyholders, shareholders, fixed income investors, as well as other customers and stakeholders.

13. The term *critical operations* is based on the Joint Forum's 2006 high-level principles for business continuity. It encompasses *"critical functions"* as defined by the FSB[11] and is expanded to include, activities, processes, services and their relevant supporting assets[12] the disruption of which would be material to the continued operation of the bank or its role in the financial system. Whether a particular operation is "critical" depends on the nature of the bank and its role in the financial system.

14. The term *respective functions* used in this document explicitly refers to the appropriate function(s) within the bank's three lines of defence, as described in the PSMOR.[13] These consist of: (i) business unit management; (ii) an independent operational risk management function; and (iii) independent assurance. Depending on a bank's nature, such as its size, complexity and risk profile, how these three lines of defence are implemented may vary.

V. Operational resilience principles

15. This section presents the Committee's principles for operational resilience, which are organised across the following seven categories: 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.

16. These categories are based on the Committee's updated PSMOR, and previously issued principle-based guidance on corporate governance, business continuity, outsourcing and other relevant risk management frameworks. The practices described below, some of which reflect previously issued guidance, should not be viewed in isolation, but rather as integral parts of a bank's forward-looking operational resilience regime in line with its operational risk appetite, risk capacity and risk profile.

Governance

Principle 1: Banks should utilise their existing governance structure[14] to establish, oversee and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and

[11] FSB, *Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services,* 2013. According to the FSB, "critical functions" are defined as "activities performed for third parties where failure would lead to the disruption of services that are vital for the functioning of the real economy and for financial stability due to the banking group's size or market share, external and internal interconnectedness, complexity and cross-border activities. Examples include payments, custody, certain lending and deposit-taking activities in the commercial or retail sector, clearing and settling, limited segments of wholesale markets, market making in certain securities and highly concentrated specialist lending sectors."

[12] In this context, supporting assets are defined as people, technology, information, and facilities necessary for the delivery of critical operations.

[13] Basel Committee on Banking Supervision, *Consultative Document- Revisions to the Principles for the Sound Management of Operational Risk,* paragraph 5, 2020.

[14] Consistent with the PSMOR, this document refers to a governance structure composed of a board of directors and senior management. The Committee is aware that there are significant differences in legislative and regulatory frameworks across countries regarding the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) so as to ensure that

learn from, disruptive events in order to minimise their impact on delivering critical operations through disruption.

17. The board of directors should review and approve the bank's operational resilience expectations considering the bank's risk appetite, risk capacity and risk profile. In formulating the bank's risk tolerance for disruption to its critical operations, the board of directors should consider a broad range of severe but plausible scenarios (eg, lockdown due to pandemics, destructive cyber security incidents, catastrophic natural disasters, etc.).

18. Under the oversight of the board of directors, senior management should implement the bank's operational resilience approach and ensure that financial, technical and other resources are appropriately allocated in order to support the bank's overall operational resilience efforts.

19. Senior management should provide timely reports on the ongoing operational resilience of the bank's business units in support of the board's oversight, particularly when significant deficiencies could affect the delivery of the bank's critical operations.

20. The board of directors should take an active role in establishing a broad understanding of the bank's operational resilience approach, through clear communication of its objectives to all relevant parties, including bank personnel, third parties and intra-group entities.

Operational risk management

Principle 2: 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.

21. The bank's operational risk management function should work alongside other relevant functions to manage and address any risks that threaten the delivery of critical operations. For operational resilience purposes, appropriate coordination with business continuity planning, third-party dependency management, recovery and resolution planning and other relevant risk management frameworks may yield greater harmonisation in delivering a consistent approach to operational resilience across the enterprise.

22. Banks should have sufficient controls and procedures[15] to identify threats and vulnerabilities in a timely manner and, to the extent possible, prevent these threats from affecting critical operations. The *respective functions* should regularly assess the effectiveness of the implemented controls and procedures. These assessments should also be conducted in the event of changes to any underlying components of the critical operations, as well as after incidents in order to take into account lessons learned and new threats and vulnerabilities that caused the incident.

23. Banks should leverage change management capabilities in accordance with the change management processes under the overall management of operational risk as a way to assess

the latter fulfils its tasks. For this reason, in some cases it is known as a supervisory board. This means that the board has no executive functions. In other countries, the board has a broader competence in that it lays down the general framework for the management of the bank. Owing to these differences, the terms "board of directors" and "senior management" are used in this paper not to identify the segregated legal liability in corporate governance practices but rather to label two-tiered decision-making functions within a bank in general.

[15] These controls and procedures should be consistent with and conducted alongside the risk identification process as articulated in Principle 6 in the proposed revisions to the PSMOR.

potential effects on the delivery of critical operations and on their interconnections and interdependencies.

Business continuity planning and testing

Principle 3: 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.[16]

24. An effective business continuity plan should be forward-looking when assessing the impact of potential disruptions.Business continuity exercises[17] should be conducted and validated for a range of severe but plausible scenarios that incorporate disruptive events and incidents.

25. An effective business continuity plan should identify critical operations, key internal and external dependencies to assess the risks and potential impact of various disruption scenarios on operations and ensure appropriate resilience levels. These plans should incorporate business impact analyses, recovery strategies and business continuity plans as well as testing programmes, training and awareness programmes, and communication and crisis management programmes.

26. Business continuity plans should develop, implement and maintain a regular business continuity exercise encompassing critical operations and their interconnections and interdependencies, including those through relationships with, but not limited to, third parties and intra-group entities. Among other business continuity goals, business continuity exercises should support staff's operational resilience awareness including training of staff, so that they can effectively adapt and respond to incidents.

27. Business continuity plans should provide detailed guidance for implementing the bank's disaster recovery framework. These plans should establish the roles and responsibilities for managing operational disruptions and provide clear guidance regarding the succession of authority in the event of a disruption that impacts key personnel.

28. Business continuity plans should clearly set out the internal decision-making process and define the triggers for invoking the bank's business continuity plan. Internationally active banks should consider whether their operational resilience efforts are appropriately harmonised with the bank's business continuity plans for the delivery of critical operations and critical third-party services contained in their recovery and resolution plans.

Mapping interconnections and interdependencies

Principle 4: 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.

29. The respective functions should map (ie identify and document) the people, technology, processes, information, facilities, and the interconnections and interdependencies among them needed to deliver the bank's critical operations, including those dependent upon, but not limited to, third parties or intra-group arrangements.

[16] Further BCBS guidance on business continuity can be found in documents published through the Joint Forum (BCBS, IOSCO, IAIS), High-level principles for business continuity, August 2006, www.bis.org/publ/joint17.pdf.

[17] The business continuity planning and testing of critical operations should be consistent with and conducted alongside the business continuity planning articulated in Principle 11 in the proposed revisions to the PSMOR.

30. Internationally active banks may leverage their recovery and resolution plans for definitions of critical operations and should consider whether their operational resilience efforts are appropriately harmonised with the organisational mappings of critical operations and critical third-party services contained in their recovery and resolution plans.

31. The approach and level of granularity of mapping should be sufficient for banks to identify vulnerabilities and to support testing of their ability to stay within the bank's risk tolerance for disruption considering the bank's risk appetite, risk capacity and risk profile.

Third-party dependency management

Principle 5: 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.[18]

32. The *respective functions* should perform a risk assessment and due diligence before entering into arrangements including those of, but not limited to, third parties or intra-group entities, consistent with the bank's operational risk management framework,[19] outsourcing/third-party risk management policy and operational resilience expectations. Prior to the bank entering into such an arrangement, the bank should verify whether the third party, including, if relevant, the intra-group entity to these arrangements has at least equivalent operational resilience conditions to safeguard the bank's critical operations.

33. Banks should formalise their relationships with third parties and intra-group entities through written agreements which should cover how to maintain operational resilience in both normal circumstances and in the event of disruption. These written agreements should reflect: the *respective functions'* due diligence; banks' supervisory and resolution authorities access to third parties; and the bank's operational resilience expectations.

34. Banks should develop appropriate business continuity and contingency planning procedures and exit strategies to maintain their operational resilience in the event of a failure or disruption at a third party impacting the provision of critical operations. Scenarios under the bank's business continuity plans should assess the substitutability of third parties that provide services to the bank's critical operations, and other viable alternatives that may facilitate operational resilience in the event of an outage at a third party, such as bringing the service back in-house.

Incident management

Principle 6: Banks should develop and implement response and recovery plans to manage incidents[20] *that could disrupt the delivery of critical operations in line with the bank's risk tolerance for disruption considering*

[18] Further BCBS guidance on outsourcing of services can be found in documents published through the Joint Forum (BCBS, IOSCO, IAIS), Outsourcing in Financial Services, February 2005, www.bis.org/publ/joint12.pdf.

[19] The management of dependencies articulated in this principle should be consistent with and conducted alongside the control and risk mitigation policies as articulated in paragraph 51 of Principle 9 in the proposed revisions to the PSMOR.

[20] Incidents are current or past disruptive events the occurrence of which would have an adverse effect on critical operations of the bank. Incident management is the process of identifying, analysing, rectifying and learning from an incident and preventing recurrences or mitigating the severity thereof. The goal of incident management is to limit the disruption and restore critical operations in line with the bank's risk tolerance for disruption.

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.

35. Banks should maintain an inventory of incident response and recovery, internal and third-party resources to support the bank's response and recovery capabilities.

36. The scope of incident management should capture the life cycle of an incident,[21] typically including, but not limited to:

    a) the classification of an incident's severity based on pre-defined criteria (eg expected time to return to business-as-usual), enabling proper prioritisation of and assignment of resources to respond to an incident;

    b) the development, maintenance and testing of incident management procedures, including thresholds for triggering business continuity, disaster recovery and crisis management procedures; and

    c) the implementation of communication plans to report incidents to both internal and external stakeholders (eg, regulatory authorities), including performance metrics during, and analysis of lessons learned after an incident.

37. Incident response and recovery procedures should be periodically reviewed, tested and updated. Root causes should be identified and eliminated to prevent the serial recurrence of incidents.

38. Lessons learned from previous incidents including incidents experienced by others, should be duly reflected when updating the incident management programme. A bank's incident management programme should manage all incidents impacting the bank, including those attributable to dependencies on, but not limited to, third parties and intra-group entities.

ICT including cyber security[22]

Principle 7: Banks should ensure resilient ICT including cyber security 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.[23]

39. Banks should have a documented ICT policy, including cyber security, which stipulates governance and oversight requirements, risk ownership and accountability, information security measures (access controls, critical information asset protection, identity management, etc), periodic evaluation and monitoring of cyber security controls, and incident response, as well as business continuity and disaster recovery plans.

40. Banks should identify their critical information assets and the infrastructure upon which they depend. Banks should also prioritise their cyber security efforts based on the significance of the critical information assets to the bank's critical operations, while observing all pertinent legal and regulatory requirements relating to data protection and confidentiality. Banks should develop plans to maintain the integrity of critical information in the event of a cyber event. Banks should

[21] Recognising that the life cycle on an incident could span multiple measures of time that could range from hours to weeks to months.

[22] Financial Stability Board Cyberlexicon's definition of cybersecurity, November 2018 (https://www.fsb.org/wp-content/uploads/P121118-1.pdf).

[23] The management of ICT articulated in this principle should be consistent with and conducted alongside the ICT principle as articulated in paragraphs 55-57 of Principle 10 in the proposed revisions to the PSMOR.

regularly evaluate the threat profile of their critical information assets, test for vulnerabilities and ensure their resilience to ICT-related risks.

41. When facilitating the implementation of wide-scale remote-access, rapid deployment of physical assets and/or significant expansion of bandwidth to support remote user connections and customer data protection banks should ensure that:

    a) appropriate risk mitigation strategies are developed for potential risks associated with a disruption or compromise of technology systems and applications. Banks should evaluate whether the risks, taken together with these strategies, fall within the bank's risk appetite and risk tolerance for disruption;

    b) well defined processes for management of remote assets, privileged users and application development are in place; and

    c) regular updates are made to ICT including cyber security in order to maintain an appropriate security posture to accommodate remote access as a longer-term option.

VI. Questions on the proposed principles

42. The Committee welcomes comments on this document from all stakeholders. More specifically, regarding the operational resilience principles, the Committee requests feedback on the following questions:

Q1. 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?

Q2. Do you have any comments on the individual principles and supporting commentary?

Q3. Are there any specific lessons resulting from the Covid-19 pandemic, including relevant containment measures,that the proposed principles for operational resilience should reflect?

Q4. Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience?

VII. Measuring operational resilience

43. The Committee recognises that measuring a bank's operational resilience is in a nascent stage and further work is required to develop a reliable set of metrics that both banks and supervisors can use to assess whether resilience expectations are being met. The Committee seeks specific feedback on the following measurement-related question:

Q5. What kind of metrics does your organisation find useful for measuring operational resilience? What data are used to produce these metrics?