November 6, 2020

Secretariat of the Basel Committee on Banking Supervision
Bank for International Settlements
CH-4002 Basel, Switzerland

Japanese Bankers Association

JBA comments on the BCBS Consultative Document: "*Principles for operational resilience*"

Dear Basel Committee members:

The Japanese Bankers Association[1] (JBA) appreciates the opportunity to provide comments on the Basel Committee on Banking Supervision's (BCBS) Consultative Document: "*Principles for operational resilience*" (the Principles) on August 6, 2020.

General Comments

Use of principle-based and risk-based approach and maintaining flexibility

JBA supports the principle-based and risk-based approach that the Principles have taken, rather than a prescriptive or standardized approach, considering that the expected operational resilience of a bank could vary by its type of business. JBA recognizes that banks are inherently responsible for ensuring their important services be operationally resilient in view of the public nature of the banks' business and for maintaining the banks' credibility. In fact, Japanese banks have been improving the level of their operational resiliency through conducting regular exercises of the business continuity plan and assessing its effectiveness[2]. Given that there is no silver bullet to achieve the objective of operational resilience, the framework should provide flexibility to the bank's approach in terms of strategies, processes and systems as long as they achieve the same outcome.

As the Principles state, operational resilience is an outcome that benefits from the effective management of operational risk. Since the approach to achieving operational resilience shall differ between firms, regulators should ensure the transparency with respect to how it will measure the outcome of the framework that a bank has in place. Needless to say financial sector firms have different business models and organizational structures across the globe and therefore a principle-based, risk-based and outcome-focused approaches are crucial in order to ensure global consistency.

Nonetheless, if the Principles are implemented as prescriptive rules in jurisdictions, such rules would undermine the objective of operational resilience and impose undue compliance burdens on banks. This is because the bank's framework for ensuring operational resilience is highly tailored in nature to respective business and organization. A best practice of a bank assumed under the rule does not necessarily fit to all other banks. While JBA supports the BCBS's principle-based and risk-based approach, we are concerned that the Principles do not explicitly preclude prescriptive implementation in jurisdictions leaving room for each regulatory authority with such significant discretions.

With that said, JBA believes the Principles generally capture the requirements for effective operational resilience on a high-level approach and supports the fact that – it aligns with other regulatory approaches, by placing

[1] The Japanese Bankers Association is the leading trade association for banks, bank holding companies and bankers associations in Japan. As of November 6, 2020, JBA has 116 Full Members (banks), 3 Bank Holding Company Members (bank holding companies), 72 Associate Members (banks & bank holding companies), 58 Special Members (regionally-based bankers associations) and one Sub-Associate Member for a total of 250 members.

[2] In such practice, Japanese banks (i) assume a wide range of crisis events (natural disasters, terrorist attacks, pandemics, computer viruses, etc.), (ii) identify high-priority operations for each crisis event, and (iii) develop a business continuity plan with a target recovery period, commensurate with the level of importance of the services.

emphasis on good governance and by encouraging banks to leverage existing approaches- e.g. use of business continuity planning and testing. However, these high-level principles may not reflect the complexity of some organizations and their various delivery structures which makes it challenging to implement.

Considering the above, we recommend adding the following provisions to the Principles:

- "Backstop provision" that explicitly encourages regulators to avoid unreasonable prescriptive rules in their jurisdictions so that the Principles will be implemented as intended by BCBS.
- "Consistency provision" that requests regulators in each jurisdiction to respect the spirit and standards of the Principles in order to avoid deviation or detailed rules which may lead to fragmentation.

JBA requests continuous collaborative efforts and conversations between regulators and banks in order to establish appropriate framework and strengthen operational resilience.

Specific comments, answers to the questions from BCBS

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?

The consistency of definitions

JBA notes that BCBS provides some important definitions of operational resilience which can be the basis for future discussion and preparations by banks. To avoid the potential fragmentation due to divergences in interpretation and supervisory practices, JBA suggests setting the globally-consistent definitions. JBA found that there are some differences in definitions, such as between "Critical Services" and "risk tolerance" in the Principles and "Important Business Services" and "Impact Tolerance" defined by the UK regulators in their consultation documents[3].

The difference can also be found in the terms used in the existing framework such as "Recovery Time Objective". The Principles refer to the various existing documents. It will be beneficial for banks and regulators to have a consolidated common "Definitions" part in the Principles to avoid any misunderstandings.

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

Principle 3: Business continuity planning and testing

Severe but plausible scenarios

Principle 3 states that *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.* JBA requests to clarify the expected level of definition of "severe but plausible scenarios" and that if each bank is supposed to reasonably decide the level of "severe but plausible scenarios".

Principle 5: Third-party dependency management

Application to third parties located in third countries

Global financial institutions sometimes centralize their IT systems and middle/back office operations across jurisdictions into intra-group subsidiaries. In this case, we are concerned that such intra-group subsidiaries are required to meet all relevant jurisdictional requirements for operational resilience applied to the outsourcing operations in each jurisdiction, which will result in undue compliance burdens on such intra-group subsidiaries. JBA believes that such multinational application of requirements is neither effective nor efficient. In order to avoid such cumulative impacts, JBA suggests putting the following or similar wordings into the Principles:

[3] CP 29/19 "*Operational resilience: Impact for important business services*" by the Prudential Regulation Authority, CP 19/32"*Building operational resilience: impact tolerances for important business services*" by the Financial Conduct Authority (FCA) and the consultation document titled "*Operational Resilience: Central Counterparties/Central Securities Depositories and Recognized Payment System Operators and Specified Service Providers"* by Bank of England

“In applying the rules of a jurisdiction to shared service centers and third parties located in third countries, they should be treated as having satisfied the rules of such jurisdiction, as long as those entities are subject to and meet the rules in the home jurisdiction that is consistent with the Principles”

Written Agreement

Paragraph 33 of the Principles states that the written agreements with third parties should reflect the respective functions’ due diligence, banks’ supervisory and resolution authorities access to third parties, and the bank’s operational resilience expectations. However, it is difficult and burdensome for banks and third parties to include statement on third-party operational resilience frameworks in written agreements. In addition, given the current business practices, it is not general to do so. As it may hinder the appropriate outsourcing, JBA believes that such requirement should be deleted from the Principles.

Also, without common standards for written agreements, the expectations for the same third party or third parties providing the same services in the regions or sectors may diverse. This could result in operational challenge for third parties that perform the critical operations of multiple banks, leading that they will be required to adhere to various levels of operational resilience and risk capacity. Therefore, JBA believes that each jurisdiction should have the common standards regarding expectations on operational resilience for third parties.

Substitutability

Paragraph 34 of the Principles states that 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. JBA believes that expectations on operational resilience in such scenarios should be set considering impact analysis/identification of countermeasures taken for third party risk in business continuity plans. Current business practice should be taken into account for third party management, including the arrangements with third-country vendors.

Also, due to the nature of operations and disruption events, there may be cases where it is difficult for banks to transfer the outsourced operations to a different third party or internalize such operations. JBA believes that these should be addressed in contingency plans. The Principles should allow such absence of substitutability as long as sufficient levels of operational resilience are secured by alternative measures such as establishing/maintaining business continuity capabilities of the subject third party and signing relevant written agreements.

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?

COVID-19 pandemic highlighted the importance of operational resilience. The scale and impact of the pandemic, across different geographies and sectors, demonstrated that firms everywhere need to be prepared for disruption events.

Business continuity and contingency plans: The Principles emphasizes leveraging existing processes and business continuity and contingency plans which were the key features of the COVID-19 response. COVID-19 has highlighted the need to ensure that business continuity plans and response plans are reviewed regularly and brought up to date and that they cover the end to end delivery of critical operations. COVID-19 also emphasizes the need to consider a broad range of scenarios in planning and testing even when they appear to be low probability, as COVID-19 demonstrates they can crystallize. Also, we could reflect the impact from disruption of supply chains for the procurement of IT resources and longer-term effects of split operations and wide-scale remote-access to reflect the importance of mobility and flexibility in the working environment so that critical functions and services are not disrupted.

Governance: In dealing with the COVID-19 pandemic and market disruption, key management decisions and changes to the banks’ operational arrangements had to be made on a local basis, as “one size fits all” approach was not appropriate due to different measures taken by respective government. It is important to consider balance between global governance framework and local governance in operational resilience. The Principles relating to governance should provide flexibility so that banks can choose to put in place a governance structure (i.e. central vs. federated governance structure) that is “fit for purpose” given the global impact of the COVID-19 pandemic. As discussed earlier, whether operational resilience is achieved as an outcome or not must be the question, not the formality of the governance structure.

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

There may be a merit in unifying the common aspects of both principles for simplicity, but JBA is reluctant to say we can automatically consolidate the two, as we need more clarity on the linkage between the two principles. Also, we saw no need to consolidate the guidance further as consolidation might lead to the principles becoming less descriptive or detailed with regards to the items not mentioned in the principles of operational risk, such as third-party dependency management and consolidation might also lead to lack of flexibility for future review as each principle refers to various existing documents.

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

JBA considers that the use of metrics should focus on the objectives of operational resilience. Without the clear evidence and regular review, there is a concern that using metrics for supervisory and regulatory purpose may prevent banks from making necessary changes in the measures taken in during disruption events and may impede the flexibility in the operational resilience framework. Therefore, JBA agrees to the BCBS’ recognition in the Principles which states 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*.

Based on our understanding above, JBA would like to propose that the following empirical and system data would be useful for measuring operational resilience:

- Existing data already used as part of its BAU operations to inform its approach to defining “risk tolerances” for its “critical operations”. For example, peak and total transaction volumes, values, customer numbers for critical operation related to payments.
- In addition to operational metrics, data relating to the impact metrics e.g. financial loss data, regulatory breaches, percentage of customers impacted by an outage (and customer segmentation), error rate, reputational damage, increase in processing time, customer complaints, staff morale/turnover etc.
- To assess the adequacy of business continuity preparation, relative and qualitative approach should be used.

(End)