9 October 2024

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 the sound management of third-party risk"

Dear Basel Committee members:

The Japanese Bankers Association[1] (JBA) appreciates the opportunity to provide our comments on the Basel Committee on Banking Supervision's (BCBS) Consultative Document: "*Principles for the sound management of third-party risk*" (the "Consultative Document") released on 9 July 2024.

The JBA supports the BCBS's efforts to enhance third-party risk management. However, considering the difficulties in obtaining certain information regarding third-parties in supply chain management, it is not practical to require banks alone to address these challenges. Therefore, as detailed in our comments below, we believe that it is also necessary for national authorities to take supplementary measures.

We hope that our comments will contribute to further discussions at the BCBS.

Supply chain management

Supply chains may be lengthy and complex, and it is important to prioritise and address these challenges. We believe that the management of cloud services should be given the highest priority due to the increasing frequency of cyber-attacks in recent years. However, there are many cases where information is not disclosed by cloud service providers when requested by a bank. Regulatory authorities should encourage the businesses that will be third party service providers (TPSPs) to cooperate with the banks' due diligence and monitoring in order to ensure the effectiveness of supply chain management.

Concentration risk

In paragraph 15, banks are advised to understand concentration risk at a systemic level based on available information. However, the information accessible from public sources or directly from TPSPs is limited, making it difficult to fully comprehend systemic concentration risk. For instance, public or TPSP-provided information might only indicate that "XX bank uses YY Inc." without specifying that "XX bank uses YY Inc. in their ZZ business," which is critical to assessing concentration risk. We believe that regulators should consider measures to help banks better understand systemic concentration, such as periodically disclosing

[1] The Japanese Bankers Association is the leading trade association for banks, bank holding companies and bankers associations in Japan. As of October 1, 2024, JBA has 114 Full Members (banks), 3 Bank Holding Company Members (bank holding companies), 74 Associate Members (banks & bank holding companies), 49 Special Members (regionally-based bankers associations) and one Sub-Associate Member for a total of 241 members.

information about third parties with higher concentration risk. Specifically, if there are any issues identified by the authorities regarding major TPSPs or matters requiring improvement that are communicated with supervisors of other sectors, sharing such information with financial institutions would facilitate the consideration of effective countermeasures.

Furthermore, while the Consultative Document suggests enhancing monitoring and other measures (e.g., more frequent testing) when concentration risk is unavoidable, there are limits to how much monitoring can be strengthened from the perspective of a single user, especially for companies like major cloud service providers that pose high concentration risk but banks have few alternatives. In cases where banks conduct risk assessments on major cloud service providers, information is often not disclosed or handled individually. Contract management also faces challenges, as most requests to adjust individual contracts are rejected. The BCBS should encourage regulators in each jurisdiction to engage in dialogue to request sufficient responses and disclosures from entities where concentration risk cannot be avoided within the industry.

Intragroup TPSP arrangements

We understand that due diligence for intragroup arrangements should be conducted on a risk-based approach, similar to other arrangements. While thorough due diligence on intragroup TPSP arrangements itself (e.g., aspects such as the nature of the service provided or arrangement) is necessary, we would like to ask for consideration for simplified due diligence on the TPSP itself (e.g., substitution through the implementation of the risk management framework/rules of TPSP equivalent to those of the parent company) if conditions such as the implementation of a unified global risk management framework/rules within the group are met. In general, the risk management framework of the headquarters or parent company is implemented at its branches and subsidiaries, ensuring a relatively high level of risk management comparable to that of the headquarters or parent company. Therefore, it is considered excessive to conduct due diligence with the same depth as for non-intragroup TPSPs for which the effectiveness of internal controls cannot be assessed without any due diligence.

Additionally, considering that the headquarters or parent company is a financial institution supervised by the home country's authorities, we would like to ask for consideration of global regulatory coordination regarding the scope and depth of due diligence (such as substituted compliance). Without global regulatory coordination, the headquarters or parent company would need to comply with requirements in each jurisdiction where it operates, which could place an excessive burden. Therefore, we would like to ask for consideration of alternative certification frameworks or similar measures in line with other regulations.

Business continuity management

We understand that it is important to clarify the items that banks should manage by contracts with critical TPSPs and the required measures to be incorporated into the bank's business continuity management (BCM) to prepare for service disruptions by critical TPSPs. However, the assessment of the criticality of a TPSP is based on various factors such as the financial, operational, or strategic importance to the bank, the bank’s tolerance for disruption, and the nature of the data or information shared. From this point of view, these items should not be uniformly defined for all critical TPSPs. For example, the items related to BCM indicated in paragraphs 58 and 59 are suitable for TPSPs that are operationally critical from a perspective of the bank's

tolerance for disruption. However, for TPSPs that are critical from the perspective of the nature of the data or information shared, these items might be somewhat excessive. Instead, it would be more appropriate to strengthen the aspects related to security for such TPSPs. Therefore, considering and implementing them based on a risk-based approach, taking into account the background of criticality assessment of each TPSP, would lead to more effective TPSP management.

Exit plan and strategy

In paragraph 66, we understand that exit strategies and plans should be implemented based on a risk-based approach, and we strongly agree with this perspective. However, at the same time, exit strategies are being required for all TPSP arrangements, which we believe is burdensome and unnecessary for both banks and TPSPs. If exit strategies were implemented for all arrangements, it would be burdensome and unnecessary for both banks and TPSPs. For example, we consider that there is little need to make an "exit strategy" for one-off contracts with the contract period of less than one year, such as a consultation service provided by a consulting firm or a lawyer. Additionally, if a third-party arrangement does not involve customer or confidential information and does not impact the continuation of a bank's critical services, an exit strategy would have a minimal impact, and we believe it is unnecessary to develop an exit strategy. To ensure thorough assessment for more critical arrangements with limited resources, we would like to suggest requiring the implementation of exit plans and strategies based on a risk-based approach.

Use and definition of terminology

The Consultative Document states that exit plans need to be regularly updated and "tested," but these plans differ in nature from business continuity plans (BCPs) in terms of unexpected events. It would be better to use a different term than "test" because procedures for exit plans is to verify their validity. Additionally, it is difficult to distinguish between BCM, exit strategies, and exit plans because they have similar outlines and objectives. The terms, objectives, and content should be clarified to avoid confusion.

Implementation schedule

Banks need to develop a management system on a consolidated basis based on the requirements of the Consultative Document, and it takes time to implement the necessary measures. Therefore, we would like to request a sufficient implementation timeframe from the finalisation of the Consultative Document to the time of introduction in each jurisdiction.

* * *

We thank the BCBS again for the opportunity to comment on the Consultative Document and hope our comments will contribute to further consideration in the BCBS.

Yours faithfully,

Japanese Bankers Association