FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

OFÍCIO Nº FB- 1102/2024

São Paulo, october 09, 2024.

Basel Committee on Banking Supervision
Bank for International Settlements
Centralbahnplatz 2, CH-4002 Basel, Switzerland

Ref: "Principles for the sound management of third-party risk"

The Brazilian Federation of Banks (FEBRABAN) appreciates the opportunity to comment on the Basel Committee's Public Consultation on the "Principles for the sound management of third-party risk - consultative document."

We support the Basel Committee in adopting a principles-based approach to the TPRM. However, we believe it is worth emphasizing that TPRM approaches are an integral part of banks' broader risk management frameworks.

Banks monitor a broad spectrum of risk factors when managing third-party relationships, including, without limitation, data and security, regulatory compliance, operational, financial and reputational risks.

While the potential disruption of critical operations due to a third-party disruption or failure, as described in the BCBS Principles for Operational Resilience (POR),[1] is significant, it represents just one aspect of the multifaceted risk landscape that banks assess as part of their TPRM approaches.

A holistic risk assessment should encompass several other risk categories, ensuring a full understanding of the risk profile associated with each third-party relationship, which results in the assignment of a risk rating or categorization of a TPSP arrangement for many banks.
In the comments below, we identified some opportunities to shape the final principles.

General comments

Criticality and proportionality

[1] https://www.bis.org/bcbs/publ/d516.htm, Principle 5.

Av. Brigadeiro Faria Lima / 4300, 4º andar
04538-132 / São Paulo SP / Brasil

55 11 32449800
febraban.org.br

The consultative document states that the criticality and proportionality concepts apply to all Principles and acknowledges that "a service or arrangement for one bank might not reflect the same risks or same level of risks as compared to another bank."[2]

However, **we recommend that the specific principles adopt a more clearly proportionate and risk-based approach, particularly in relation to the distinction between critical TPSP arrangements.**

The document does not clarify whether the expectations apply to all TPSP arrangements or only to critical TPSP arrangements, e.g., relating to N-party registration tracking (paragraph 22), relating to joint design and testing of business continuity plans (BCPs) with TPSPs (paragraph 60).

There should be space for all requirements set out under the principles to be applied by banks on a proportionate basis based on the risks associated with the service provided by the TPSP. Moreover, we caution against an overly broad definition of criticality that could impose undue burdens on the banking industry.

We also appreciate the Basel Committee's commitment to a technology-agnostic approach. As the financial industry and associated tools and technologies continue evolving rapidly, it is fundamental that regulatory principles remain flexible enough to accommodate technological innovations without inadvertently favoring or hindering specific solutions.

Supervisory authorities are in a unique position to understand the system-wide risks posed by arrangements with some TPSPs and can leverage their broad perspective and authority to address potential systemic risks, foster standardization and a more cohesive global approach to TPRM. Some concerns with definitions are presented below:

Definitions

As described above, assuming that the Basel Committee intends to focus on resilience considerations in defining criticality, we propose to make the following refinements to some of the definitions.

- Critical TPSP arrangement:
    - As currently drafted, this definition, especially with the inclusion of TPSPs that "impact" critical services, is too broad and may lead to a disproportionate number of TPSP arrangements considered "critical." **We propose to introduce the concept of materiality into the definition to restrict arrangements that may affect the viability of the bank's operations. Instead, a critical TPSP arrangement should be**

[2] Paragraph 15 – Proportionality

defined as *"A TPSP arrangement which supports or impacts one or more critical services provided to a bank."*

- Critical service:
  - **We propose to change the definition of Critical Services to what already exists in some jurisdictions: "A service provided to a bank, the failure or disruption of which could have an immediate and adverse impact on the bank's viability, critical operations or ability to meet legal and regulatory obligations in a manner that affects the bank's viability or financial stability."**
  - This definition focuses most clearly on the material services provided to a credit institution by a critical TPSP, i.e., those that could have an immediate and adverse impact if they were disrupted.
  - It also addresses an issue with the current definition, which includes consideration of a bank's ability to meet legal and regulatory compliance obligations, which would significantly expand the scope of a critical service beyond what is appropriate or likely intended by BCBS. For many regulatory requirements, a temporary disruption to meet them would have very limited impact on the bank or its regulators (e.g., transaction reporting). While said requirements are generally important, they do not justify the same degree of resilience that is required for services that, if disrupted, could have significant impacts on the viability of the bank or its customers.

- Critical TPSP:
  - **The question as to whether a specific definition of "critical TPSP" is necessary arises, in addition to the definition and reference in the principles to "critical TPSP arrangements."**

- Supply chain:
  - We appreciate efforts to address supply chain risk, including nth parties, but BCBS must recognize the practical limitations in effectively monitoring supply chain risks, specifically N-th subcontractors (such as 4th, 5th, or 6th party service providers) within the "entity network." **We recommend that the BCBS adopt a more risk-based and principles-driven approach when setting expectations for credit institutions as they monitor their supply chains.**

- Nth key:

- While the ability of an nth party to access sensitive or confidential banking information is an important consideration from a data protection and cybersecurity perspective, including it in the TPRM requirements could create duplication and conflict between these disparate sets of requirements. Moreover, basing the definition of a nth key on its support for the provision of a critical service is extremely broad and will likely lead to the inclusion of nth parties with minimal impact on the continuity of critical services.
- As recognized by the FSB[3], we believe in the limited legal and operational ability of financial institutions to directly monitor nth parties and very limited ability to control or impose requirements on them. Thus, credit institutions rely on their TPSPs to provide clear, complete and timely information and to implement their own appropriate supply chain risk management approaches. **We suggest that this requirement be removed so that said limitations are reflected in the nth party risk management principles and supervisory approaches.**

- Intragroup TPSP:

While not a direct comment on the proposed definition of an intragroup TPSP, we believe the Principles should recognize that intragroup TPSPs, in many cases, are subject to robust regulatory requirements and risk frameworks, including operational risk and operational resilience frameworks. Said frameworks can provide a prominent level of reliability and resilience to such services, which should be considered when assessing the risks associated with such intragroup TPSP arrangements and the answer of required controls. **We recommend that all controls imposed on affiliates also consider a risk-based approach.**

Observations on the proposed principles

Governance, Risk Management and Strategy (Principles 1-2)

As currently drafted, the proposed allocation of responsibilities between the board and senior management is misaligned with corporate governance principles. The proper role of the board is to oversee the bank's business strategy and financial strength, internal organization, governance and risk management, while senior management is responsible for executing risk management strategies. As the BCBS has previously stressed, the board should focus on core oversight functions and top-line strategy, which are fundamental to the safe and sound operation of the banking organization.[4]

[3] www.fsb.org/wp-content/uploads/P041223-1.pdf. See pages 22-23.

[4] As provided for in detail in the BCBS "Guidelines for Corporate Governance Principles for Banks", July 2015. Similar expectations about the roles and responsibilities of the board and senior management as provided for by BCBS in Principles 3 through 5 of its "Reviews of the principles for good operational risk management," March 2021.

Regarding proposed Principle 1, the current wording appears to deviate from this intended approach. It can be read as suggesting that the Board should have direct oversight of each TPSP arrangement. We suggest that the wording of Principle 1 be changed to:

In addition to the above, the Principles should also recognize that, from a governance perspective, not all parts of a business within a banking group may have a formal board structure. Instead, the principles should refer to the highest management or governance body of a given jurisdiction, rather than referring specifically to boards of directors.

We recommend amending Principle 2 to reflect that senior management has a responsibility to manage risk through the implementation of risk management policies and procedures. The board is expected to hold senior management accountable for the effective implementation of the bank's strategic objectives and governance frameworks. As such, we recommend reviewing Principle 2 to:

> ***Senior management, who are responsible for the daily operations of a business,*** *third party risk management framework (TPRMF) policies and processes* ***in place and*** *in line with the bank's third-party strategy, including reporting on TPSP performance and risks related to TPSP arrangements, and mitigating actions*.

The requirements in paragraph 22 to include nth parties in the register based solely on the criticality of the service and associated risk could benefit from further refinement. Including all nth parties in records deviates from a risk-based approach and presents a potentially unfeasible requirement. Thus, banks would deploy resources to secure this additional information, rather than focusing on improving risk management or oversight of service providers that could pose material risks to their businesses. **To foster consistency and clarity, we suggest narrowing the scope to "Major nth parties," with a clear definition of that term as described above.**

Regarding the concentration risk mitigators described in paragraph 23, while we appreciate the BCBS's intention to provide guidance, we suggest a more flexible approach that encourages companies to develop tailored solutions that best suit their specific circumstances.

The current examples in paragraph 23 may be interpreted as prescriptive solutions, which are not always feasible or appropriate in all circumstances. They also appear to be tailored to a specific technology rather than applicable to third parties, going against the principle of technology agnosticism. Moreover, considering the rapid pace of change in the industry, these examples can quickly become outdated. We also observed that several jurisdictions are working on definitions

and risk management approaches regarding concentration risk in relation to TPSPs, which should not be precluded by the BCBS principles.[5]

We also suggest at this point that it be clear in the text whether we are talking about service dependence (a single supplier providing a critical service), financial dependence or a combination of the two elements, in addition to what is expected in monitoring.
Risk Assessment (Principle 3)

To reinforce the holistic nature of banks' TPRM programs, which are covered by the Principles, and in line with the proposed amendments to paragraph 15, we recommend amending paragraph 27 as follows:

"The risk assessment stage of the life cycle is where banks identify and assess inherent risks and criticality of potential services before entering into a proposed arrangement with a TPSP."

The proposed definition of a critical service, as amended earlier in this letter, takes an outcome-focused approach based on the impact of the failure or disruption.
However, paragraph 28 appears to expand beyond this outcome-focused approach by introducing additional factors to be considered when determining the "criticality" of potential services provided from a third-party relationship, namely "the financial, operational or strategic importance of the arrangement; their tolerance for disruption; the nature of any data or information shared with the TPSP; or the substitutability of the service provide a framework for assessing the importance of a service. **This expansion raises concerns as some of these criteria appear to diverge from the primary focus of criticality related to resilience, potentially leading to inconsistencies in application and interpretation**.

Moreover, the additional criteria in paragraph 28 relating to data/information and substitutability are features that inform the risks inherent in the arrangement, rather than the criticality of the third-party service to the bank. Such inherent risks may drive enhanced controls and oversight, tailored to the specific level and type of risk, but should not be considered by the importance or criticality of the third-party service to the bank.

To avoid confusion of operational resilience concepts with existing holistic TPRM frameworks designed to address all types of risks, we recommend removing paragraph 28 from the Final Principles, as the definition of Critical Service, including the changes suggested in this letter, adequately covers the key requirements for identifying resilience without introducing additional, potentially confusing criteria.

[5] [To add specific examples, such as Article 29 of the EU DORA, "Preliminary assessment of ICT concentration risk at entity level."]

Finally, to better support a proportionate and risk-based approach to the MPPC, we recommend reviewing paragraph 32 to read:
Risks may change throughout the life cycle of the TPSP arrangement. Therefore, credit institutions should perform risk assessments on an ongoing basis, with a frequency commensurate with the risks inherent in the arrangement and its criticality for the credit institution (refer to Onboarding and ongoing monitoring below).

Due Diligence (Principle 4)

Paragraph 36 implies that banks should assess a TPSP's ability to retain qualified personnel for the ongoing provision of services at the due diligence stage. Said assessment would be extremely difficult for credit institutions to conduct accurately during the initial due diligence process and over time, considering the dynamic nature of staffing and skills requirements. **We suggest refining the suggested approaches to due diligence to consider practical limitations, especially during the pre-contractual phase.**

Paragraph 38 requires banks to consider their "ability (including cost, timing, contractual restrictions) to exit the TPSP arrangement and either transition to another TPSP or bring the activity back in-house." **We suggest that the BCBS amend this provision to refer to the "bank's ability to exit the TPSP arrangement without undue disruption," which would allow for a broader range of appropriate responses tailored to each specific situation**.

Contracting (Principle 5)

While the suggestions in paragraphs 41-42 are a useful reference and can indicate to TPSPs what banks expect from contracts governing TPSP relationships, it would be valuable for the BCBS to provide guidance on risk management and regulatory compliance expectations for banks when faced with potentially inflexible contractual terms.

Particularly, paragraph 42 sets out certain provisions that banks are unlikely to be able to guarantee as currently drafted. While it is important that credit institutions and supervisory authorities receive information about key nth entities, it is unlikely that said information can be obtained directly from entities that do not have a direct contractual relationship with the credit institution.

Therefore, we recommend that paragraph 42 be amended to better reflect the reality of this contractual relationship dynamic:

- **"conditions governing key nth parties (e.g. prior notification of use or change, incident reporting);**

- **"... rights of supervisory authorities to access, audit and obtain relevant information from key nth parties as permitted under applicable laws and regulations within the respective jurisdictions or bi-/multilateral agreements amongst supervisors;"**

Finally, we observed that the last item of paragraph 42 on insurance against non-insurable risks can be interpreted broadly and without clarity on the limits or minimum values of the policy. **We suggest changing this to a consideration to ensure that banks and TPSPs maintain the flexibility to use insurance as a risk transfer mechanism in a manner most appropriate to the risk being managed.**

Onboarding and ongoing monitoring (Principles 6-7)

Paragraph 44 introduces requirements relating to the maintenance of staffing levels and competence. However, the scope and long-term applicability of said requirements are unclear. Although the requirement is specified in the "Onboarding" section, **it is not clear whether this maintenance of staff and competency levels needs to be sustained beyond the onboarding phase.**

We suggest removing the "key nth parties" as part of the ongoing monitoring of banks in paragraph 47. As discussed in the definition of nth parties, banks often have little or no visibility into the operations of nth parties and typically do not have the contractual relationship to be able to legally monitor or audit the nth parties. Furthermore, expanding monitoring to include nth parties would substantially increase the scope and complexity of a bank's monitoring responsibilities.

The triggers for review of TPSP arrangements listed in paragraph 48 are extensive and may lead to excessive and unnecessary review processes, regardless of whether the changes affect the provision of TPSP services to the bank. For example, the introduction of new or advanced technologies by a TPSP may not affect the services used by a particular bank in any way. **We suggest that these reviews should only be triggered when events directly impact the TPSP ability to provide its services to the bank.**

Business Continuity Management (Principle 8)

We ask that the Committee provide greater clarity on the expectations for joint design and testing of BCPs with TPSPs, as mentioned in paragraph 60, and whether such BCP testing is expected for all TPSPs or only those deemed "critical."

Joint testing of BCPs with all TPSPs would be a time- and resource-intensive process with potentially limited utility. **We recommend that joint BCP testing apply specifically to TPSPs with which the bank has a critical TPSP relationship and, more specifically, where the bank may be particularly vulnerable to temporary third-party service disruptions, meaning that the bank's operations would be significantly impacted even with the bank's own independent BCP in place.**

Said tests should be a "coordinated" or "cooperative" exercise. **Overall, it is important that tests do not exacerbate or create new vulnerabilities related to the sharing of sensitive BCPs that could have indirect effects for the banking industry.**

We also note that the proliferation of operational resilience regulations has led to a significant increase in the number of exercises and the amount of testing carried out in the industry. Said exercises remain highly manual and resource intensive. Authorities and industry need to be careful to avoid a situation where the frequency of required testing becomes such that banks are forced to shift to a compliance, rather than learning, approach to participation.

We also observed that the recommendations appear particularly focused on a limited set of TPSP relationships, namely cloud computing. **We would like to see these examples removed to ensure the Principles remain technology agnostic and refrain from setting unrealistic expectations.**

The requirements for assurance testing under paragraph 59 do not reflect that it may not be practical in all cases to perform assurance testing of a TPSP's BCP methodologies. **In line with general risk management principles, in circumstances where collateral testing is not feasible or where other risk mitigation measures are appropriate, credit institutions should be able to determine the most appropriate approach.**

Finally, we would like to highlight that, without changes to the definition of critical services, the additional requirements of paragraph 59 would end up applying to a wide range of third parties, an outcome that would be unfeasible for banks to maintain.

Termination (Principle 9)

Guidance on planning for the exit of critical services should consider practical and contractual constraints that may limit the ability of institutions to change providers or reintroduce services in-house without undue consequences. **BCBS may consider limiting detailed exit plan requirements to critical TPSPs, as defined in many resolution frameworks.**

Examples of "unplanned" termination include expiration or breach of contract, failure of the TPSP to comply with applicable laws or regulations, the desire to seek an alternative TPSP, bringing the activity back in-house, or discontinuing the activity. Each of these scenarios provided would be consistent with an orderly or planned exit from a TPSP relationship. **We ask that BCBS provide further clarification on what would be considered an unplanned exit, or remove it as a category and term.**

While the Principles expect banks to have processes in place for the transfer of logical assets in a timely manner and appropriate format (paragraph 65), these transfer timeframes are likely to be extended in an unplanned termination scenario. Strict expectations for the transfer of logical assets within timeframes that would allow banks to remain within their disruption tolerance would be equivalent to a ban on the use of certain technologies. **Therefore, we recommend that, rather than requiring timely transfer, the BCBS require banks to assess and understand the timeframes required to transfer said assets and plan accordingly.**

Role of Supervisors (Principles 10-12)

Monitoring global systemic risk: While financial institutions recognize the importance of monitoring concentration risks in relation to their TPSPs, **supervisors undertake to assess whether there are overall risks arising from the concentration of certain TPSPs, as individual financial institutions do not have sufficient information about how these services are being deployed across the industry. This also applies to mapping interconnections and interdependencies across the financial system.**

- Records: Existing interoperable records across jurisdictions would significantly simplify the reporting process for cross-border financial institutions and provide financial industry authorities with comparable data to help identifying aggregate risk across the financial system, including potential systemic risks. **The Basel Committee should also encourage regulators to limit changes to the format, means and frequency of updates to what is strictly necessary.**

- Information sharing and processing: While the Principles call for greater information sharing and reporting, security is crucial when it comes to accessing, exchanging, storing and transmitting information.[6] **We request that BCBS consider how supervisory authorities**

[6] For example, paragraph 70 includes reference to supervisors using maps of interconnections and interdependencies. Information about this type of mapping is highly confidential and can pose a critical risk to operational and information security if accessed by malicious players. The concentration of this type of information relating to several credit institutions in a given supervisory authority may pose a significant

will store and protect information collected in connection with TPSP arrangements. Banks and TPSPs themselves emphasize the need for robust security measures in the handling and centralized storage of confidential information collected by supervisory authorities.

- International Coordination: Considering the cross-border presence of many financial institutions and TPSPs, we suggest international coordination regarding the handling of systemic TPRMs and TPSPs across the global financial industry. As acknowledged in the consultative document, many jurisdictions have already developed their own TPRM frameworks and standards, while others are currently developing them (e.g. DORA). It is important avoiding regulatory fragmentation given the cross-border nature of many TPSP business models and for financial institutions operating in multiple jurisdictions.

Once again, we appreciate the opportunity to comment on the revisions to the "Principles for the sound management of third-party risk - consultative document." If you have any questions about the topics addressed in this letter, please contact the undersigned at com.gestao.riscos@febraban.org.br.

Sincerely,

Rubens Sardenberg
Executive Director of Economics, Prudential Regulation and Risk

Jayme Soares Alves Neto
Deputy Risk Director

risk to all these entities and, subsequently, to financial stability.