Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

October 9, 2024

Mr. Neil Esho
Secretary General
Basel Committee on Banking Supervision
Bank for International Settlements
Centralbahnplatz 2
4051 Basel, Switzerland

Via Electronic Mail to

Re: Feedback on Basel Committee consultation on principles for third-party risk

Dear Mr. Esho,

The Financial Service Sector Coordinating Council ('FSSCC')[1] welcomes the opportunity to comment on the Basel Committee for Banking Supervision ('BCBS' or 'Committee') *Principles for the Sound Management of Third-Party Risk* ('Principles')[2] and its efforts to increase consistency in regulatory approaches to bank's third-party risk management (TPRM) programs, which in turn should help strengthen the overall operational resilience of the global banking system.

Banks have a long history of using third-party service providers (TPSPs) to deliver products and services in a cost effective and efficient manner. The use of these providers has required banks to create frameworks to manage the risks that these providers may introduce to the bank's operations. In addition, financial authorities have had to develop oversight frameworks that set minimum control requirements on how these relationships are used and managed. In light of these changes, the FSSCC applauds the BCBS's efforts to update its 2005 Joint Forum paper, Outsourcing in Financial Services, to address changes in how banks use and integrate third party services into their operations and how banks address the increasingly diverse third-party service provider (TPSP) environment in the banking sector. The FSSCC also welcomes the additional principles that address certain approaches taken by financial authorities when conducting oversight of potential risks.

[1] The FSSCC was formed in 2002 as a public/private partnership with the support of the U.S. Department of Treasury (U.S. Treasury). FSSCC collaborates with the U.S. Treasury and the financial regulatory agencies at the federal and state levels through the Financial and Banking Information Infrastructure Committee (FBIIC), which was also formed in 2002 under the U.S. Treasury's leadership. FSSCC partners with the public sector on policy issues concerning the resilience of the sector. Our 70+ members consist of financial trade associations, financial utilities, and the most critical financial firms.

[2] The BCBS Principles for the Sound Management of Third-Party Risk (2024) can be found at: https://www.bis.org/bcbs/publ/d577.pdf

In addition, over the last decade, *operational resilience*[3] has increasingly become a focus of both financial institutions and financial authorities. A key driver of operational resilience is the ability of a bank to identify and manage risk in its third party and supply chain providers that support its critical operations. Several financial authorities, in an attempt to provide clarity to financial institutions on third party oversight of service providers supporting these critical operations, developed additional third-party guidance for the management of these providers. The result of these financial authorities' activities has been two-fold:

1. The emergence of financial authority guidance aimed at advancing general third-party risk management principles, and
2. The emergence of financial authority rulemaking aimed at defining oversight of third-party risks for third parties supporting a financial institution's critical business services or critical operations.

As a matter of clarity, the FSSCC requests that the BCBS clarifies throughout the Proposal that the drafted Principles represent an advancement of general third-party principles. Third parties which have a potential impact on a bank's operational resilience represent just a subset of the third-party inventory and may have additional requirements for the management of these risks.

While the FSSCC is supportive of the principles-based approach taken in the Proposal, there are areas where further refinement and clarification that would strengthen the draft principles and help avoid the creation of global expectations that dilute or confuse the intended scope of the Principles or create confusion with current operational resilience or third party risk management regulatory text.

Executive Summary

The FSSCC welcomes the Committee's efforts to strengthen the risk management of banks' TPSP arrangements. As the primary global standard setter for the prudential regulation of banks, the Committee's effort to provide TPRM principles that can be used globally will help drive consistency in financial authorities' expectations for banks in this area. The FSSCC recognizes that the goal of the Proposal is to guide firms in the overall management of third-party risk and that the sound management of third-party risk is a key driver of a bank's operational resilience. Therefore, as a general rule, the Proposal should more broadly cover general third-party risk management while highlighting how each principle should be considered in the context of a bank's operational resilience objectives. This approach will provide clarity to financial authorities and financial institutions on how the Proposal should be applied and strengthens the Proposal's alignment to the BCBS Principles for Operational Resilience (BCBS POR)[4] and the BCBS Principles for the Sound Management of Operational Risk (BCBS PSMOR)[5]. The FSSCC requests that the BCBS, to the greatest extent practical, keep the Proposal aligned with

[3] *Operational Resilience* is defined as *the ability of a bank to deliver critical operations through disruption*.
[4] The BCBS Principles for Operational Resilience (2021) can be found at: https://www.bis.org/bcbs/publ/d516.pdf
[5] The BCBS Revisions to the Sound Management of Operational Risk (2021) can be found at: https://www.bis.org/bcbs/publ/d515.pdf

general third-party risk management practices while drawing alignment to operational resilience practices where appropriate.

The FSSCC would like to offer the following comments for the BCBS' consideration, which are explained in greater detail in the Discussion of Specific Comments section.

Criticality. As currently drafted, the Principles' frame resilience risk as the primary driver of a bank's risk assessment of a TPSP arrangement, rather than ensuring that operational resilience is appropriately reflected in a bank's holistic TPRM programs. The difference between inherent risks and criticality for operational resilience purposes should be carefully considered.

Definitions. Several definitions contained in the Proposal require additional clarity for how these definitions translate to operational resilience and prior BCBS principles for operational risk and operational resilience.

Governance. As currently drafted, the lines between Board and Management responsibilities could be clearer. Further clarification is necessary to clearly delineate the roles of each function.

Third Party Register of Information. Third party registers provide key risk management and oversight capabilities for financial institutions and financial authorities. However, if not properly aligned with an actionable supervisory purpose, the number of data elements may expand and impact the resources necessary to maintain the register and the ability of financial authorities to maximize the value from it.

Exit Plans and Exit Strategies. The FSSCC looks to continue the dialogue with financial regulatory authorities to better understand the differences between unplanned and planned exits, including the expected differences in approaches to manage scenarios associated with each.

Role Of Supervisors. Third party risk management is a key part of the bank's risk management framework. However, TPSPs must also participate in the management of this risk which may be aided by the supervisors driving this expectation.

Discussion Of Specific Comments

Criticality

We recognize that the Principles aim to guide firms in the overall management of third-party risk – not just in incorporating resilience objectives – and that the sound management of third-party risk is a key driver of a bank's operational resilience. As part of this, there are certain third-party arrangements that should be considered 'critical' to the firm due to their potential resilience impact, and be subject to particular enhanced controls and oversight that best address resilience risk.

The Proposal however currently has two overarching issues which puts at risk this intended approach. First, the Principles apply an overly expansive scope to what should be considered 'critical'. This would result in finite bank resources being dedicated to third-party arrangements that do not pose real risk to a bank's resilience. Second, as drafted, the Principles' primary emphasis on operational resilience risk above all generally overlooks broader risk management concerns and drivers that banks should consider when managing third-party risk and tailoring its controls and oversight. The combination of these two

issues would lead to the application of resilience-related controls, which are generally complex and resource intensive, to be applied to an overly broad scope of third-party arrangements.

Third Party Risk Management (TPRM) frameworks are designed to cover risks that may be introduced through the use of TPSP arrangements. These risks include but are not limited to information, regulatory, financial and reputational risks. The Proposal lays out that banks should consider *'all types of risks related to TPSP arrangements including but not limited to strategic risk, reputational risk, operational risk…'*[6] The outcome of a bank's risk assessment of a planned TPSP arrangement is an inherent risk rating[7] for the arrangement which dictates the requisite level of oversight and controls throughout the lifecycle of the arrangement. An arrangement may present higher inherent risk for numerous reasons, including but not limited to the processing of a high volume of personal or highly confidential information, or a combination of various factors such as the arrangement's recovery time objective and the ability of the bank to find an alternate provider or bring the service back in house. Banks are required to consider a range of risk factors (e.g., financial, strategic) and impacts when determining the risk of a particular TPSP arrangement. Further, each of these arrangements may also require different confidentiality, integrity, or availability controls based on these different risk factors and potential business impacts.

The BCBS Principles for Operational Resilience define resilience as *'the ability to deliver critical operations through disruption.'*[8]where *'critical operations'* is based on the Joint Forum's 2006 high-level principles for business continuity. Further, the criticality of a third-party arrangement (in this operational resilience context) is defined by the support that a third party provides to the bank's critical operations. The potential impact of a third-party outage on a bank's critical operations, however, is just one of many risks that banks should consider when tailoring its oversight. This should be assessed alongside a broader set of risks as part of a bank's holistic risk assessment of third-party arrangements. Given its potential impact on a bank's viability and operations, these 'critical' arrangements require specific resilience controls. Therefore, the objective should be that operational resilience is appropriately reflected into broader TPRM frameworks without overlooking or confusing the full range of risk drivers that determine a third-party's risk rating.

The FSSCC stresses the importance of distinguishing the differences between inherent risk and criticality. A TPSP arrangement may be considered high risk due to numerous factors (e.g., the processing of personal information), however, a high-risk TPSP arrangement, by itself, does not make the arrangement critical in the context of operational resilience. Critical services for operational resilience must remain in the context of supporting a bank's critical operations.

To allow the Proposal to remain aligned with general third-party risk management principles, while keeping its alignment to the BCBS Principles for Operational Resilience and Principles for the Sound

[6] Proposal @ 13, paragraph 30
[7] Inherent risk is defined as the risk to a service or arrangement before any actions are taken to mitigate or control it.
[8] BCBS Principles for Operational Resilience (2021) @ paragraph 11

Management of Operational Risk, we recommend the BCBS make the following changes to the Principles:

- Clarify its intention to provide standalone guidance on holistic TPRM approaches, including the risk-based methodology described above, of which operational resilience is just one of many risks considered.
- Acknowledge the holistic risk assessment that covers the full range of risks presented by a third-party arrangement, assigns a risk rating or categorization, and tailors the necessary oversight fundamental to the risk-based approach that underpins banks' third-party risk management programs.
- Explicitly state that the term 'critical' is narrowly focused on resilience considerations, aligned with the definition of critical operations in the BCBS POR, as amended in the next section of this letter.
- Amend the control requirements for critical services to better address the risks to the continued provision of critical services, rather than other risks a TPSP arrangement could present to a bank.

Definitions

- Critical TPSP arrangement

The Proposal defines Critical TPSP arrangement as '*a TPSP arrangement which supports or impacts one or more critical services provided to a bank*'[9].

- Critical Service

The Proposal defines ***Critical Service*** as "*a service provided to a bank, the failure or disruption of which could significantly impair a bank's viability, critical operations, or ability to meet legal and regulatory compliance obligations.*"[10]

The FSSCC believes the current definition of critical service will inappropriately expand the scope of what is considered critical beyond what is covered in the BCBS POR, which will cause misalignment between the two sets of BCBS Principles. The BCBS POR defines operational resilience as the ability to deliver critical operations through disruption. Critical operations are defined as critical functions and the activities, processes, services, and supporting assets whose *disruption would be material to the continued operation of the bank or its role in the financial system.*

The proposed definition includes legal and regulatory compliance obligations. Banks, as a heavily regulated industry, must comply with many legal and regulatory obligations. While necessary for supervision of the sector, failure to comply in a timely manner will rarely, if ever, cause a disruption that would materially impact a bank's continued operation or its role in the financial system.

[9] Proposal @ 3
[10] Proposal @ 3

As written, the definition would require banks to apply the same resilience capabilities to submitting tax documents or responding to routine requests for information as they do to participating clearing major currencies. This significantly expands the scope of banks' operational resilience programs and misaligns its intended objective. The BCBS definition of 'critical service' would therefore require revision to remain practical. We believe legal and regulatory compliance should be one of the risks that banks consider when assessing TPSP arrangements, but not an automatic criterion for classification as critical, i.e., poses potential impact to a bank's resilience.

To address this, we recommend that the definition be amended as follows:

> "Critical service: A service provided to a bank, the failure or disruption of which could significantly impair a bank's viability, critical operations, or ability to meet legal and regulatory compliance obligations **such that the failure to meet those obligations could significantly impair a bank's viability or critical operations**".

This amended definition maintains the explicit recognition that failure to meet regulatory or legal obligations should be considered, while also remaining aligned to the BSBC POR in its focus on significant impairment to a bank's viability or critical operations.

Third Party Service Provider Governance

Principle 1 of the Proposal reads that '*The board of directors has ultimate responsibility for the oversight of all TPSP arrangements and should approve a clear strategy for TPSP arrangements within the bank's risk appetite and tolerance for disruption*'[11].

Principle 2 of the Proposal reads that '*The board of directors should ensure that senior management implements the policies and processes of the third-party risk management framework (TPRMF) in line with the bank's third-party strategy, including reporting of TPSP performance and risks related to TPSP arrangements, and mitigating actions*'[12].

Boards are accountable for managing a bank's third-party risk as part of its comprehensive risk management and corporate governance duties. Paragraph 54 of the Basel Principles for the Sound Management of Operational Risk (PSMOR) outlines Board and senior management's duties in managing operational risks from third-party service providers and ensuring effective risk management policies and practices are in place.

As currently drafted, Principle 1 could be interpreted as the Board is expected to have direct oversight into each TPSP arrangement. While the Board does have oversight responsibilities of the strategy used to manage the bank's risks, Board and Management responsibilities should be clearly delineated.[13] Therefore, Principle 1 should be clarified to reflect the board's proper role, which is to ensure an appropriate third-party risk management framework is in place and provide strategic oversight for the

[11] Proposal @ 7
[12] Proposal @ 7
[13] The BCBS Corporate Governance Principles for Banks (2015) provides guidance for the delineation of Board and Management responsibilities and can be found at: http://bis.org/bcbs/publ/d328.pdf

overall risk management strategy including the third-party risk management strategy. This oversight includes understanding the risks inherent to the bank, the bank's strategies for managing these risks, and reviewing performance measures that indicate how well the bank is executing these strategies.

The FSSCC proposes that the BCBS modify Principle 1 to read:

> *Principle 1: 'The board of directors has ultimate responsibility for* ***overseeing the management of the bank's third-party risks*** ~~*the oversight of all TPSP arrangements*~~ *and should approve a clear strategy for* ***TPRM*** ~~*TPSP arrangements*~~ *within the bank's risk appetite and tolerance for disruption'*[14].

The above suggested that these modifications provide a clearer delineation between Board and Management responsibilities while acknowledging that the Board is accountable for management oversight.

Separately, senior management is responsible for the day-to-day execution of risk-management strategies through the implementation of risk-management policies and procedures established under the third-party risk management framework (TPRMF). The Board should oversee the establishment of the overall strategy, framework, and policies. However, holding the Board accountable for *ensuring* implementation of these policies and processes—as suggested in Principle 2—does not reflect its proper role and could undermine the effectiveness of banks' governance and risk management.

The FSSCC proposes the following amendments to Principle 2, to appropriately reflect established principles of effective corporate governance and risk management and to better align with the BCBS PSMOR:

> *Principle 2*: '*The board of directors should ensure that* ***effective*** ~~*senior management implements the*~~ *policies and processes of the third-party risk management framework (TPRMF)* ***are in place and*** *in line with the bank's third-party strategy, including reporting of TPSP performance and risks related to TPSP arrangements, and mitigating actions*'.

By instituting these changes, it clarifies that the banking organization's Board of Directors is responsible for understanding and challenging the strategy used by the banking organization to oversee its third-party and supply-chain risks.

Third Party Register of Information

The Proposal sets the expectation that banks should maintain a complete and up-to-date register of all TPSP arrangements (and nth parties as appropriate to the criticality of the service and associated risks).[15] Further, the Proposal sets the expectation that banks should include key elements of each arrangement in the register.[16] The FSSCC agrees that third-party registers are an important and useful

[14] Proposal @ 7
[15] Proposal @ 7
[16] Proposal @ 7

tool in supporting effective risk management practices by banks and supervision by regulatory authorities. The Third-Party Register for Information also supports the identification of concentration risk at the entity and system level. More recently, the data submitted in these registers is informing and supporting the designation of critical third-party service providers in certain jurisdictions.

However, the expansion of reporting requirements for outsourcing and third-party registers under various global frameworks has resulted in expansive and divergent expectations on (i) the purpose or objectives of registers; (ii) the information that is required (i.e. data elements); (iii) the format of the required information and (iv) the timing and method of submission. The result is that banks are required to report on a substantial number of data elements and in different formats. Each data element and format require the bank to build the functionality and processes to ensure that the quality of the data element remains consistent. This requires diverting resources from other risk management functions to address these tasks. The FSSCC supports including data elements that provide an actionable purpose however, data elements that provide minimal or no immediate value creates undue effort on both the bank to collect and the financial authority to supervise. Further, the bank may be required to retain numerous different third- party registers by jurisdiction which further increases the susceptibility to error for these registers.

The FSSCC stresses the importance of a considered and risk-based approach to third-party register requirements that prioritizes the principle of data minimization which ensures the deliberate alignment of each data element with the specific objectives and purpose of the register.

Additionally, the FSCCC encourages regulatory authorities to seek to align to a common set of third-party register data elements. Similar to cyber incident reporting requirements[17], the more fractured the common data elements are between jurisdictions, the more fractured the management of these registers become for banking organizations. The lack of alignment enhances the reporting burden on banks who are required to create multiple processes and register templates to meet diverging regulatory requirements and impacts the ability of financial authorities to have a clear understanding of potential third-party impacts across jurisdictions.

Therefore, the FSSCC recommends that the BCBS clarify in its Proposal the importance of (i) alignment across register requirements and data minimization and (ii) ensuring purposeful data elements necessary to achieve core supervisory objectives. The FSSCC encourages the BCBS incorporate these considerations for supervisors in the Proposal. Such considerations may include:

[17] The FSB Cyber Incident Reporting working group was established to identify the current challenges facing financial institutions and authorities for cyber incident reporting. Disparate data elements, reporting formats, and timeframes between jurisdiction created an environment that made it difficult for financial institutions to understand all their reporting obligations and the information necessary to meet them and made it difficult for financial authorities to reconcile incident information across jurisdictions. The FSB Achieving Greater Convergence in Cyber Incident Reporting (2023) (https://www.fsb.org/uploads/P130423-1.pdf) provides insights into how the industry approached driving a solution.

- Clearly defined objectives for the register and ensuring that data fields are directly linked to those objectives;
- Providing transparency and clarity on the rationale for data elements and how the data will be used for supervisory objectives;
- Periodically reviewing (as a standards body function) the relevance and need of data elements, removing or refining as appropriate to align with the risk landscape or newly identified supervisory purposes and objectives;
- Ensuring the scope and level of data required is proportionate and that the benefit provided to supervisory oversight is balanced against the operational and reporting burden placed on banks;
- Seeking to align data requirements, elements and the format of registers across jurisdictions where reasonably practicable, particularly where there is commonality of register objectives (i.e. data collection for oversight of critical third parties).

The FSSCC also supports and encourages the creation of an international public/private working group to standardize a register template that can drive this consistency and purpose criteria for this register of information. The FSSCC believes these recommendations would drive collaboration, coordination, and outcomes supporting supervisory objectives.

Exit Plans and Exit Strategies

The Proposal introduces the concept of planned and unplanned terminations and supporting exit plans and strategies.[18] This distinction has led to confusion and mixed interpretations regarding what constitutes a planned versus an unplanned exit.

For instance:

> *Planned exits are those that are anticipated, or where a bank intentionally decides to end a third-party arrangement at a predetermined time or under expected circumstances. The exit plan for planned termination is therefore structured, proactive and can entail a more detailed roadmap for how the relationship will be wound down.*
>
> *Unplanned termination, on the other hand, could refer to an unexpected or sudden end to a third-party arrangement which could arise due to unforeseen circumstances or an event that prevents the third-party from continuing their services. The nature of these exits requires that banks focus on contingency measures that can be responsively deployed to mitigate the risks associated with unforeseen service disruptions.*

Public and private sectors should collaborate to define and develop scenarios for both planned and unplanned terminations to promote greater consistency in how banks understand exit planning expectations.

[18] Proposal @ 15

Role Of Supervisors

The Proposal rightly identifies the need for supervisors to prioritize third-party risk management as part of their ongoing assessments of financial institutions. In particular, Principle 11 notes that "supervisors should analyze the available information to identify potential systemic risks posed by the concentration of one or multiple TPSPs in the banking sector."[19] Among other things, the Proposal states information including registers of TPSP arrangements, recovery and resolution plans, and reports on incidents involving TPSPs can be used to assess these risks.[20]

Nevertheless, the availability of the materials listed above depends to some degree upon a TPSP's willingness to provide them to financial institution customers. To address these challenges, the FSSCC recommends that supervisors articulate clear expectations for TPSPs when providing services to financial sector partners. Moreover, supervisors should also review their own authorities, including those available in the U.S. under the Bank Service Company Act, to determine whether certain TPSPs could be subject to examination and regulation by financial supervisory authorities. Such an approach would increase transparency between TPSPs and financial institutions, reinforce the importance of security and resilience for TPSPs, and allow supervisory authorities to better identify and address concentration risk.

Conclusion

The FSSCC appreciates the opportunity to provide comments on the Consultative Document and your consideration of the views expressed in this letter. The FSSCC welcomes further discussion and engagement on the topics raised in this letter. If you have any questions or need further information, please contact Bridgette Walsh at +1 (703) 963-3399 or bwalsh@fsscc.org.

Sincerely,

Debbie Guild, PNC

Chair, Financial Services Sector Coordinating Council

[19] Proposal at 16.
[20] *Id.*