October 9, 2024

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

INSTITUTE OF INTERNATIONAL FINANCE

Submitted via electronic mail

Re: IIF feedback on Basel Committee Consultation on Principles for the Sound Management of Third-party Risk

Dear Mr. Esho,

The Institute of International Finance (IIF)[1] appreciates the opportunity to provide public comments to the Basel Committee on Banking Supervision's (BCBS) consultative document on "*Principles for the sound management of third-party risk*" ("the consultation").[2]

The IIF welcomes the Basel Committee's efforts to develop global principles for third-party risk management (TPRM) in the banking sector, building on and updating its 2005 Joint Forum paper on "Outsourcing in Financial Services." As financial institutions increasingly leverage third party service providers (TPSPs) to support their operations, and as part of the digital transformation of their businesses, having a consistent global approach to managing the associated risks is essential. IIF members also appreciate and endorse the Basel Committee's commitment to a technology-agnostic approach. As the financial industry and the associated tools and technologies continue to evolve rapidly, it is essential that regulatory principles remain flexible enough to accommodate technological innovations without inadvertently favoring or discouraging specific solutions.

The IIF and its members have consistently advocated for a principles-based, outcomes-focused approach to risk management, including TPRM, which can be applied across jurisdictions and banks. The IIF has previously submitted its views in detail on these topics, including in response to the Financial Stability Board (FSB) consultation, "*Enhancing Third-Party Risk Management and Oversight,*"[3] and the UK regulatory Authorities' consultation, "*Operational resilience: Critical third parties to the UK financial sector*."[4]

The remainder of this letter is organized into Overarching Comments, which include four proposed priorities for the BCBS to consider as it finalizes the Principles, and Specific Comments on the definitions and draft principles.

---

[1] The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, professional services firms, exchanges, sovereign wealth funds, hedge funds, central banks and development banks

[2] BCBS, "Principles for the sound management of third-party risk," July 2024.

[3] IIF, "IIF Submits Response to FSB Consultation on Third-party Risk Management," August 2023.

[4] IIF, "IIF response to UK Operational Resilience CTPs consultation," March 2024.

Overarching Comments

IIF members support the Basel Committee taking a principles-based approach to TPRM. However, we believe it is important that the Committee reflect in the final Principles that TPRM approaches are an integrated part of banks' broader risk management frameworks. Banks monitor a wide spectrum of risk drivers when managing third-party relationships, including but not limited to data and security, regulatory compliance, operational, financial, and reputational risks. While the potential disruption to critical operations due to a third-party outage or failure – as outlined in the BCBS Principles for Operational Resilience (POR)[5] – could be significant, it represents just one aspect of the multifaceted risk landscape that banks evaluate as part of their approaches to TPRM. A holistic risk assessment of third parties should encompass a broad range of risk categories, ensuring a thorough understanding of the full risk profile associated with each third-party relationship which, for many banks, results in the assignment of a risk rating or categorization of a TPSP and TPSP relationship. We think the current draft Principles could benefit from a more holistic approach, and suggest that in the final Principles the BCBS recognize that TPRM methodologies, including those a bank may use to assess a TPSP's risk rating, are designed to capture a diverse set of risks, *including but not limited to* those aligned to operational resilience.

As part of this effort to maintain a clear distinction between TPRM and operational resilience, there are areas where regulatory principles should reasonably take a narrower focus on resilience considerations within the context of third-party relationships. This appears to be the Committee's intention in parts of the draft Principles, [6] although this is not reflected consistently and is missing in foundational areas such as the definitions (see comments on definitions such as "critical services", below).

As such, IIF members recommend that the BCBS consider four overarching priorities when developing the final Principles, which are set out below.

1. *Incorporate a holistic approach to TPRM and avoid conflation with operational resilience concepts.*

Our understanding is that the proposed Principles aim to guide banks in the overall management of third-party risk – not just in incorporating resilience objectives. That said, the sound management of third-party risk is generally a driver of a bank's operational resilience. There are certain third-party relationships that should be considered "critical" to the firm due to the potential material impact of the third-party on the bank's critical operations. These third parties should be subject to specific enhanced controls and oversight that best address risks to *resilience*.

However, the draft Principles currently have two overarching issues which could endanger this approach. First, the Principles apply an overly expansive scope to what should be considered 'critical,' which would result in finite bank resources being dedicated to third-party arrangements that do not pose material risk to a bank's resilience. Second, the Principles' primary emphasis on operational resilience risk above all generally overlooks broader risk management concerns and drivers that banks should (and do) consider when managing third-party risk and tailoring their controls and oversight. The combination of these two issues could

---

[5] Principle 5 in BCBS, "Principles for Operational Resilience," March 2021.

[6] The consultation, page 1: "Through the publication of this document, the Committee seeks to promote a principles-based approach to improving banks' operational risk management and operational resilience through effective third-party risk management (TPRM)."

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

Banks' TPRM frameworks are designed to address various risks, including data and security risks, regulatory compliance, financial viability, and reputational risks. Principle 3, specifically Para. 30, reflects this by stating that banks should consider *all* types of risks related to TPSP arrangements. The outcome of such a risk assessment will, for many banks, lead to a risk rating for the third-party (i.e., a determination of the level of risk inherent in the arrangement) or similar, which in turn will dictate the level of oversight and specific controls the bank will deploy. This reflects a holistic risk-based approach, which is fundamental to TPRM.

It is important to acknowledge that there may be third-party engagements that do not pose significant risks to a bank's resilience, but may still require enhanced due diligence and specific controls due to a range of other risk drivers and the bank's assessment of the risks. One issue is that the draft Principles combine these differing considerations and impacts into just the operational resilience scoping and oversight expectations. The result is a dichotomy between third parties deemed critical from a resilience perspective, and all others. A direct impact of that dichotomy is that the Principles prescribe controls that may not align with the actual risks posed by the third-party, i.e., applying resilience-related controls to third-party arrangements that do not present resilience risk.

2. Adequately reflect operational resilience concepts and considerations in TPRM, without rescoping TPRM as operational resilience – which itself is an outcome of risk management.

The potential impact of a third-party outage that could significantly impair a bank's critical operations, as defined by the BCBS POR, is one of the many risks that banks should consider when tailoring their oversight. This risk should be assessed alongside a broader set of risks, which in turn dictate a risk assessment or risk rating for the third-party arrangement as part of the bank's holistic risk assessment of its third-party relationships. Therefore, the objective should be to integrate operational resilience as a risk consideration into broader TPRM frameworks without overlooking or confusing the full range of risk drivers that determine a third-party's risk assessment or rating.

Ultimately, the BCBS should ensure that the revised Principles maintain a holistic approach to TPRM which recognize that operational resilience is one of the key outcomes for a bank's TPRM. The Principles should therefore appropriately reflect operational resilience concepts and considerations within the broader context of TPRM, rather than inadvertently redefining all of TPRM solely in terms of operational resilience. Specific suggestions for how to do this are provided below, specifically in terms of the definition of "Critical Service".

3. Ensure that expectations for banks and supervisors are practicable and reflect actual relationships and interactions between banks, TPSPs, and TPSP supply chains.

This priority relates to a variety of examples across the Principles, including the expectations around monitoring supply chains/nth parties, due diligence, contracting, and concentration risks.

IIF members appreciate efforts to address supply chain risk, including nth parties. However, we request that the BCBS further acknowledge the practical limitations in effectively monitoring supply chain risks (as has been recognized by the FSB).[7] Banks often have little to no visibility

[7] FSB, "Final report on enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities," December 2023. Pages 22-23.

into the operations of nth parties, and typically lack the contractual relationship to be able to legally monitor or audit nth parties. There is exponential complexity and cost of monitoring risks arising from higher nth party subcontractors within the network of entities that materially underpin a critical service. Given these factors, it would be helpful for the BCBS to take a more risk-based and targeted approach in the Principles when defining expectations for banks' supply chain monitoring, recognizing the legal and practical challenges faced by banks in the oversight of a TPSP's extended chain of nth parties and that the focus should be on those entities that are material to a critical service.

In relation to system-wide concentration risk, supervisory authorities are uniquely positioned to understand the potential system-wide risks posed by arrangements with certain TPSPs and can leverage their broad perspective and authority to address potential systemic risks, promote standardization of requirements across jurisdictions, and foster a more cohesive global approach to TPRM. In some jurisdictions, supervisors have a mandate for direct oversight of certain TPSPs. In other jurisdictions, supervisors could consider alternative approaches to monitoring and supporting the resilience of TPSPs which are most important from a banking system perspective. For instance, the Basel Committee could consider establishing a forum for regular dialogue between banks, supervisors, and the TPSP community to address evolving challenges and foster a more balanced ecosystem (further discussed in the Specific Comments on the Principles related to the role of supervisors). This collaborative approach would help in developing solutions that enhance the overall stability and security of the financial system while recognizing the realities of the current regulatory framework and market dynamics.

4. Simplify and improve consistency throughout the Principles in relation to key definitions, and application of a proportionate, risk-based approach.

Specifically, we recommend that the BCBS:

- Clarify the Committee's intention to provide standalone guidance on holistic TPRM approaches, including referencing the risk-based methodology described above, of which operational resilience is just one of many risks considered.
- Acknowledge the practice of a holistic risk assessment that covers the full range of risks presented by entering into a third-party relationship, such as assigning a risk rating or categorization, and tailoring oversight in a way that fundamentally reflects a risk-based approach to banks' third-party risk management programs.
- Explicitly state that the term "critical" in the Principles for TPRM is narrowly focused on resilience considerations, linked with the definition of critical operations in the BCBS POR. Additionally, the BCBS should amend the definition of "critical service" to better reflect the term's focus on critical operations as defined by BCBS. Full comments on definitions are included in the Specific Comments section below.
- Amend the control requirements for critical TPSP arrangements to ensure they address the risks to the continued provision of critical services, rather than other risks a TPSP arrangement could present to a bank.

In terms of proportionality, the consultative document states that the concept of proportionality applies to all the Principles and recognizes that "a service or arrangement for one bank might not reflect the same risks or same level of risk as compared to another bank."[8] However, IIF members recommend that the Principles more clearly outline a proportionate, risk-based approach particularly in relation to distinguishing between critical and non-critical third-party services. At present, it is not always clear if expectations apply to all third-party services or only to critical third-party services, for example in the requirements related to the register tracking

[8] Para. 15 – Proportionality.

nth parties (Para. 22),[9] or those related to joint design and testing of business continuity plans (BCPs) with TPSPs (Para. 60).

There should be scope for all the requirements set out under the Principles to be implemented by banks on a proportionate basis based on the risks associated with the service provided by the TPSP. Further, we caution against an overly broad definition of criticality that would deviate from the intended scope and impacts considered under the POR (as explained in the *Definitions* section below), as this would have the unintended consequence of inappropriately expanding the scope of banks' resilience programs and resilience-related activities.

Specific Comments

Where we are proposing specific text edits to the draft Principles in this letter, we have summarized these in a table included in the **Appendix** to this letter for easy reference.

Definitions

As described above, consistent with our understanding of the Basel Committee's intention to appropriately reflect operational resilience considerations in banks' TPRM programs, we propose making the following refinements to certain definitions to maintain crucial alignment with related BCBS principles.

Critical service:

As currently drafted, this definition would expand the scope of resilience-related criteria beyond what is established in the foundational BCBS POR. This expansion could potentially create misalignment between these two sets of Principles, leading to inconsistencies in implementation and understanding. IIF members therefore propose amending the definition of a Critical Service to the following (below and throughout this letter, proposed new text is shown in bold and proposed deleted text has been struck through):

> *A service provided to a bank, the failure or disruption of which could significantly impair a bank's viability~~,~~* ***or*** *critical operation~~s, or the ability to meet legal and regulatory obligations~~.*

This alternative definition would address a key issue with the current one, which includes the consideration of a bank's ability to meet legal and regulatory compliance obligations and as such would significantly expand the scope of a critical service beyond what is appropriate or likely intended by the BCBS under its operational resilience framework. For many regulatory requirements, a temporary delay in being able to fulfill them (e.g., failure to submit a tax form on time due to a temporary disruption) would have a very limited impact on the bank, its customers, or wider markets. While these requirements are important in general, they do not justify the same degree of resilience required for services which, if disrupted, could be material to the continued operation of the bank or its role in the financial system.

At a minimum, if deemed necessary to include regulatory and legal compliance in the definition, we would propose amending the definition to more closely align with potential resilience impact. For example, the definition could be modified to:

[9] In Para. 20, although there is a reference to "as appropriate to the criticality of the service and associated risks", the text first refers to maintaining a "complete and up-to-date register of all TPSP arrangements (and nth parties, … ".

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 ***in a manner that affects the bank's viability and/or broader financial stability****.*

Critical TPSP arrangement:

The introduction of this definition may not be necessary and will not, in our view, significantly enhance a bank's ability to identify relevant third-party critical services or improve the application of enhanced controls, due diligence, and oversight. The BCBS could consider whether the existing guidance sufficiently addresses these aspects without the need for this additional definition.

If the BCBS is considering introducing this definition to capture contracts that cover multiple services provided by a TPSP (e.g., framework agreements), we would argue that it is unnecessary to differentiate such arrangements/agreements. Banks tailor their risk management of TPSP arrangements based on the inherent risks of a specific contracted service, as well as the potential impact to the bank and its critical operations (i.e., the criticality of the third-party service to the bank). The introduction of a term which looks to define a specific type of contract/agreement consequently adds no additional value and may lead to unhelpful interpretive differences across jurisdictions, which leads us to recommend removal of this definition in the final Principles.

If, however, the BCBS is intent on retaining this definition, we note that as currently drafted the definition is overly broad, especially with its inclusion of TPSPs which "impact" critical services, and could lead to a disproportionate number of TPSP arrangements being considered "critical". We would propose to include "materiality" in the definition to ensure that the scope is narrowed to those arrangements that could affect the viability of the bank's operations. For example, the definition could be modified to:

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

Critical TPSP:

We question whether a specific definition of "Critical TPSP" is required in the final Principles. As described above, IIF member banks assess the criticality of TPSP arrangements with reference to a range of risk factors considering the importance of the TPSP's support and the importance of the bank's operations which rely on the TPSP's services. In the context of a bank's own TPRM framework, this is a more discerning and globally applicable approach than seeking to define TPSPs which are "critical" in a broader sense.

Key nth party:

We note that, as per above, data protection is only one of many risks that a firm should consider. Naming one specific risk implies that all other risk categories that could be present with an nth party do not warrant enhanced controls or oversight. Data risks, as well as other risks, are already considered as part of a bank's risk assessment of the TPSP arrangement, and will flow through to the role an nth party plays in the service provision. Therefore, access to confidential data should not be explicitly included in the key nth party definition as this may create further confusion.

Furthermore, basing the definition of a key nth party on its "support" for the delivery of a critical service is extremely broad, and is likely to lead to the inclusion of nth parties with minimal

impact on the continuity of critical services. The current definition lacks proportionality, which has been embedded in the risk-based approach set out by the FSB with respect to key nth parties, i.e., "Focusing on those nth-party service providers that are knowingly essential to the delivery of critical services to financial institutions can be more consistent with a proportionate, risk-based approach." (Emphasis added.)[10]

We therefore recommend the BCBS amend its definition of "key nth party" to take a more explicitly proportionate, risk-based approach which is also aligned with the approach in the FSB's toolkit:

> *A service provider that is part of a TPSP's supply chain and ~~supports~~* ***that is knowingly essential to*** *the ultimate delivery of a critical service by a TPSP to a bank ~~or that has the ability to access sensitive or confidential bank information (eg consumer data)~~.*

As has also been recognized by the FSB,[11] we note the limited ability of financial institutions to directly monitor nth parties, and their very limited ability to control or impose requirements on them. Banks are therefore reliant on their TPSPs to provide clear, complete, and timely information, and to implement their own appropriate supply chain risk management approaches. Banks are best able to address supply chain risks where they have leverage, which would typically be with the contracted TPSP, and by requiring and validating that the TPSP maintains a robust TPRM program of their own.

Intragroup TPSP:

IIF members recognize that the use of intragroup relationships may not, in all cases, be inherently less risky than external TPSP relationships, and appreciate the BCBS's recognition that a bank's risk management process should be proportionate to the unique characteristics of intragroup arrangements. However, it should be recognized by the BCBS that these relationships may present a different risk profile than those with non-affiliated parties and, in certain cases, the risk profile may be inherently lower than service provision through an external third party due to differences in control, amongst other factors.

Banks often use intragroup providers to deliver common services such as general IT services (e.g., server/network/desktop support), risk (e.g., cyber, third party), finance, legal/compliance, and audit. Common services are sometimes referred to as shared services as these services are delivered centrally to numerous legal entities.[12] This shared services model results in banks establishing a consistent set of minimum control requirements across the organization through its corporate policies and standards. Whereas, if an external third party were contracted to provide such services, they may have different risk frameworks and risk appetite resulting in potential disparities in risk management.

Therefore, the IIF stresses the importance of supervisors applying a proportionate approach to intragroup TPSPs that recognizes that the appropriate level of oversight and controls a bank applies to an intragroup TPSP should reflect a considered approach reflecting the specific nature of the intragroup model.

---

[10] FSB, "Final report on enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities," December 2023.
[11] Ibid. See pages 22-23.
[12] The FSB has set out guidance on identification of critical shared services: FSB, "Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services," July 2013.

Further, it would be helpful for the BCBS to consider and explicitly address application of the Principles in complex group outsourcing structures, such as when an entity within a group structure leverages services provided via an intragroup affiliate but those services originate from a non-intragroup third party. Given that the BCBS Principles are intended to apply at an entity level, it is important to clearly define which entities should be considered TPSPs and which should be considered nth parties in such circumstances.

Comments on proposed Third Party Risk Management Principles 1 to 12

As currently drafted, Para 15. and its sub-bullet points appear to redefine TPRM frameworks in a way that solely prioritizes and bases the tailoring of controls and oversight on resilience risk, i.e., criticality. As banks' TPRM programs address a broad range of risks – not only resilience – that may necessitate enhanced controls and oversight, we recommend the BCBS revise Para. 15 as follows:

- "Not all TPSP arrangements present the same level **or types** of risk and therefore not all arrangements require the same level or type of oversight or risk management."
- Add a bullet point preceding the "Criticality" bullet point, titled "**Risk Assessment**" which sets out the above herein detailed holistic approach to TPRM. Importantly, we encourage the BCBS to note that the risk assessment encompasses the inherent risks of the potential TPSP arrangement. Complementing this is the assessment of criticality, which is just one consideration included in a bank's risk assessment, and primarily reflects the importance of the TPSP arrangement to the bank from a resilience perspective as set out in the BCBS POR.
- Nth parties and supply chain: We suggest adding the new text in bold here: "… Banks should have appropriate risk management processes to identify and manage the supply chain risks, proportionate to the **inherent risks and** criticality of the services being provided. …"

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 board's proper role is to oversee the bank's business strategy and financial soundness, internal organization, governance, and risk management, while senior management is responsible for executing the risk management strategies. As the BCBS has previously emphasized, the board should focus on core oversight functions and top-tier strategy, which are fundamental to the safe and sound operation of the banking organization.[13]

With respect to proposed Principle 1, the current drafting seemingly deviates from this intended approach and creates misaligned expectations for the banking sector. The proposed principle could be read to suggest that the Board should have direct oversight of every single TPSP arrangement, rather than the Board's typical role of ensuring that an appropriate third-party risk management framework is in place and providing strategic oversight of senior management. The IIF does not believe this was the Committee's intention and therefore we suggest refining Principle 1 to appropriately distinguish between the board's role of oversight vs. management's

[13] As set out in detail in the BCBS "Guidelines: Corporate Governance Principles for Banks," July 2015. Similar expectations for the board and senior management's roles and responsibilities were set out by the BCBS in Principles 3 to 5 of its "Revisions to the principles for the sound management of operational risk," March 2021.

responsibility for daily operations and implementation of the strategic framework by amending the drafting as follows:

> *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.*

Further 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. The Principles should instead refer to the most senior management or governance body in a given jurisdiction, rather than referring specifically to boards throughout.

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

> ***Senior management, who is responsible for a firm's day to day operations,*** ~~*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.*

We suggest amending Para. 18 to clarify that banks should have flexibility in how they structure their governance frameworks, including whether they use central or federated functions for monitoring TPSP arrangements.

The requirements under Para. 22, namely, to include nth parties in the register as appropriate to the criticality of service and associated risks, could benefit from further refinement and clarification. The inclusion of all nth parties in registers deviates from a risk-based approach and presents a potentially unworkable requirement. Banks would, as a result, deploy resources in an attempt to secure this additional information rather than focusing on enhancing risk management or oversight of service providers, which could result in material risk to their firms. To promote consistency of application and clarity, we suggest narrowing the scope to "key nth parties", with a clear definition of this term as outlined above.

With respect to the assessment of bank-level concentration risk, this presents significant challenges, beginning with a lack of a common understanding of what constitutes concentration risk in this context. The mapping of interdependencies and interconnections of TPSPs is a complex and resource-intensive process, and assessing concentration risks associated with nth parties presents significant challenges. The BCBS should therefore also consider limiting the mapping expectations (e.g., in Para. 23) to those nth parties identified as key nth parties, according to the proposed definition above, which could provide a more risk-based and proportionate approach.

Furthermore, information from a dependencies and interconnections mapping is highly sensitive and could represent a critical risk to operational and information security of not only an individual bank but the entire industry should it be accessed by bad actors. The concentration of information on dependencies and interconnections of TPSPs from multiple banks within a given supervisory authority could pose a significant risk to all those entities, and by extension, to financial stability. Furthermore, this information, by its nature, is not specific to one jurisdiction and therefore the security practices of any one authority could have outsize impacts

on the security of the wider financial system. Commensurate with these potential risks, it is important for supervisors across the world to establish clear guidelines to protect the confidentiality and integrity of data related to TPSP arrangements, and careful consideration should be given to how sensitive information will be handled and protected by supervisory authorities. To the extent that authorities need to collect this sort of sensitive information from banks, it would be better done on an exceptional and limited basis to allow banks and supervisors to more carefully manage the security risks at that point in time on a case-by-case basis.

With respect to the mitigants of concentration risk outlined in Para. 23, while we appreciate the BCBS's intention to provide guidance, we would suggest a more flexible approach that encourages firms to develop tailored solutions that best fit their unique circumstances. While IIF members recognize the importance of considering bank-level concentration risks, a balanced approach needs to be taken of weighing (and subsequently managing) any risks of TPSP concentration against any gains in resilience, efficiency, or effectiveness of using a TPSP to deliver services to its users or clients. The examples currently used in Para. 23 could be interpreted as prescriptive solutions, which may not always be feasible or appropriate in all circumstances. They also appear to be tailored to a particular technology rather than applicable across all third parties, which goes against the principle of technology-agnosticism. Additionally, given the rapid pace of change in the industry, these examples may become outdated quickly. We would also note that authorities and groups in some jurisdictions are working on definitions and risk management approaches in relation to concentration risk with respect to TPSPs, which should not be preempted in the BCBS Principles.

Risk Assessment (Principle 3)

To reinforce the holistic nature of banks' TPRM programs, and in line with the proposed amendments to Para. 15, we recommend amending Para. 27 to:

> *The risk assessment stage of the life cycle is where banks identify and assess the* ***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 outcomes-focused approach based on the impact of failure or disruption. However, Para. 28 appears to expand beyond this outcomes-focused approach by introducing additional factors to consider when determining the "criticality" of potential services provided by a third party, 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." This expansion raises concerns, as some of these criteria seem to diverge from the primary resilience-related focus of criticality, potentially leading to inconsistencies in application and interpretation.

While "the financial, operational or strategic importance of the arrangement" could link back to the key resilience criteria in the definition of a critical service (i.e., bank viability, critical operations), the remaining criteria are not relevant for determining the criticality of the third-party service to the bank. For example, the tolerance for disruption is typically an output of the criticality determination performed by the bank, rather than a leading indicator. Furthermore, the additional criteria in Para. 28 related to data/information and substitutability, are characteristics that inform the inherent risks of the arrangement, rather than the criticality of the third-party service to the bank. These inherent risks could drive enhanced controls and oversight, tailored to the specific risk level and type, but should not be a standalone consideration for the importance or criticality of the third-party service to the bank.

To avoid conflating operational resilience concepts with existing holistic TPRM frameworks which are designed to address all risk types, we recommend removing Para. 28 from the final Principles, as the critical service definition with the suggested amendments in this letter adequately covers the key requirements for identifying resilience without introducing potentially confusing additional criteria.

Finally, to better support a proportionate, risk-based approach to TPRM, we recommend revising Para. 32 to read:

> *Risks may change throughout the life cycle of the TPSP arrangement. Therefore, banks should perform risk assessments on an ongoing basis**, at a frequency commensurate to the inherent risks of the arrangement and its criticality to the bank** (refer to Onboarding and ongoing monitoring below).*

Due Diligence (Principle 4)

Some of the due diligence requirements outlined under this Principle could create unrealistic expectations or have a disproportionate impact on both banks and TPSPs, especially as part of banks' due diligence given the limitations on pre-contractual information available to them. For instance, Para. 36 implies that banks should assess a TPSP's ability to maintain qualified staff for ongoing service delivery at the due diligence stage. Such an assessment would be extremely difficult for banks to conduct accurately during the initial due diligence process, and over time given the dynamic nature of staffing and skill requirements. We suggest refining the suggested approaches to due diligence to consider the practical limitations, especially during the pre-contractual phase. We recommend the BCBS also amend Para. 36, similar to the above recommended edits to Para. 32, to better support a proportionate, risk-based approach:

> *As part of the assessment of a TPSP's capacity and ability to deliver the services under the arrangement, **commensurate to the inherent risks of the arrangement and its criticality,** banks should consider the TPSP's: …*

Para. 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." The current language could be interpreted as limiting banks' options or prescribing specific actions during TPSP exits. 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 wider range of appropriate responses tailored to each unique situation. This adjustment would maintain the essential focus on risk management while providing banks with the necessary latitude to determine the most suitable exit strategy based on their specific circumstances.

Contracting (Principle 5)

While the suggestions in Paras. 41-42 are a useful reference and may also signal to TPSPs what banks expect in 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 contract terms.

Para. 42, in particular, sets out certain provisions which banks are unlikely to be able to secure as currently drafted. While it is important that banks and supervisors receive information regarding key nth parties, it is unlikely that this information can be secured directly from an nth party, which typically would not have a direct contractual relationship with the bank. As a bank's primary leverage stems from its contractual rights, information regarding key nth parties would typically be secured through the contracted third-party, which is also responsible for cascading

contractual obligations of the bank and applying its own robust TPRM program to its supply chain.

We therefore recommend amending the sub-bullet points under Para. 42 to better reflect the reality of this contractual relationship dynamic:

- *conditions governing key nth parties (e.g. prior notification of use or change **from the TPSP**, incident reporting **to the TPSP**); …*
- *…rights of banks to access, audit, and obtain relevant information from **the TPSP concerning** key nth parties; …*
- *rights of supervisory authorities to access, audit and obtain relevant information from **the TPSP related to** key nth parties as permitted under applicable laws and regulations within the respective jurisdictions or bi-/multilateral agreements amongst supervisors; …*

Lastly, we note that the final bullet point in Para. 42 on insuring against uninsurable risks could be interpreted broadly and without clarity on policy limits or minimums. We suggest changing this to be a consideration to ensure banks and TPSPs retain the flexibility to utilize insurance as a risk-transfer mechanism in a way that is most suitable to the risk being managed.

Onboarding and Ongoing Monitoring (Principles 6-7)

Para. 44 introduces requirements related to maintaining staff and competency levels. However, the scope and long-term applicability of these requirements are unclear. While the requirement is specified under the "Onboarding" section, it is unclear whether such maintenance of staff and competency levels needs to be sustained beyond the onboarding phase.

Para. 45 repeats requirements to include TPSPs in the register and to map interdependencies from paragraph 22 under Principle 2. In line with our comments under Principle 2, we would recommend that these should only be required for key nth parties.

We suggest the removal of "key nth parties" as part of banks' ongoing monitoring in Para. 47. As discussed under the definition of key nth parties, banks often have little to no visibility into the operations of nth parties, and typically lack the contractual relationship to be able to legally monitor or audit nth parties. Further, expanding monitoring to include nth parties would substantially increase the scope and complexity of a bank's monitoring responsibilities. As noted above in the recommended edits to Para. 42, key nth party oversight is primarily conducted through the contracted TPSP due to practical and legal challenges involved in attempting to establish direct oversight and monitoring of a service provider that is not contracted by the bank (i.e. nth parties). Monitoring of the provision of the critical services themselves will intrinsically identify where issues are arising due to a "key nth party", which delivers the same risk management and resilience outcomes in a substantially more efficient way.

The triggers for review of TPSP arrangements listed under Para. 48 are extensive and may lead to excessive and unnecessary review processes regardless of whether the changes impact the TPSP's provision of services to the bank. For example, a TPSP's introduction of new or advanced technologies may not in any way impact the services used by a given bank. Such reviews should only be triggered when events directly impact the TPSP's ability to provide their services to the bank.

Finally, we note that Para. 53 states that banks should "consider" incorporating requirements for incident reporting into contracts for critical services. However, bullet point 3 in Para. 42 makes it mandatory through contractual provisions for banks to have the right to receive accurate, comprehensive and timely information including for incidents. If the BCBS intends

Para. 42 to refer to something other than incident reporting from the TPSP to the bank, we ask that this be clarified.

Business Continuity Management (Principle 8)

In Para. 58, the BCBS should clarify that banks will manage third-party dependencies through a variety of frameworks, such as their TPRM and business continuity management (BCM) frameworks. We do not believe it is the intention of the BCBS to imply sole ownership of this responsibility to BCM, but this clarification could help to avoid potential confusion.

We ask that the Committee provide greater clarity around the expectations of joint design and testing of BCPs with TPSPs, as referenced in Para. 60, and whether this 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 testing of BCPs apply specifically to TPSPs with which the bank has a critical relationship and, more specifically, when the bank might be particularly vulnerable to temporary disruptions of the third-party service, meaning the bank's operations would be significantly impacted even with the bank's own independent BCP in place. Such testing should be a "coordinated" or "cooperative" exercise. In general, it is important that testing does not exacerbate or create new vulnerabilities related the sharing of sensitive BCPs that could involve spillover effects for the banking sector. We also note that the proliferation of operational resilience regulations has led to a significant increase in the number of exercises and amount of testing conducted in the sector. These exercises remain highly manual and resource intensive. Authorities and the industry need to be careful to avoid a situation in which the frequency of required testing becomes such that banks are forced to shift to a compliance, rather than learning, approach to participation.

In the second bullet point under Para. 58, the BCBS provides a list of potential recovery strategies or compensating controls that can be considered part of banks' BCM. However, this could be interpreted by some institutions or supervisors as requirements for specific methods to be leveraged in all instances. Furthermore, many of the examples might not be relevant across different types of TPSPs. For instance, banks will not be able to bring services in-house when these services pertain to, as one example, software license providers for word processing software. We also note that the recommendations seem particularly focused on a limited set of TPSP relationships, namely cloud computing. We would welcome the removal of these examples to ensure that the Principles remain technology agnostic and refrain from setting unpractical expectations.

The requirements for assurance testing under Para. 59 do not reflect that it may not be practical in all cases to conduct assurance testing of a TPSP's BCP methodologies. Even for the largest banks, running the kind of testing listed in Para. 59 is not scalable to all critical TPSP arrangements over a short or medium-term period. It must remain up to the bank, using a risk-based approach, to determine which TPSP arrangements to test and what kind of test to use. In line with general risk management principles, for circumstances where assurance testing is not practical or other risk mitigation measures are appropriate, banks should be able to determine the most appropriate approach.[14] To supplement bank-led testing, the bank should also be able to rely on the resilience testing of the third party, provided the third party can evidence such testing meets the standards of the bank and includes the services which the bank consumes. It is important to consider that meeting the standard of the bank does not imply exact replication of testing types or methods, but should be focused on the outcome of achieving the same level of

[14] For example, when a bank is engaging with highly regulated entities and/or large global providers, interdependencies with critical infrastructure, or where the bank has implemented recovery solutions independent of the TPSP.

resilience and assurance. This would still fulfill the core requirement of these Principles by providing visibility to banks and supervisors on areas of potential risk.

Finally, we would like to highlight that, without changes to the definition of critical services, the additional requirements in Para. 59 would end up being applied to a broad range of third parties, an outcome that would be infeasible for banks to maintain. It would also result in a misalignment of risks and controls, as third parties providing services related to basic and non-urgent compliance activities would be placed in the same category as those third parties providing services connected to a bank's critical operations, which could be central to the sound functioning of markets.

Termination (Principle 9)

The Principles should take into account that there is no one-size-fits-all approach to exit planning, and that executing an exit plan may not always be appropriate or feasible during a crisis situation – for example, as it may make it harder to differentiate between the incident and the exit and therefore harder to manage both. Any guidance on exit planning for critical services should take into account the practical and contractual limitations that can impact a bank's ability to switch providers or bring services back in-house without undue consequences.[15] In general, we encourage the Committee to acknowledge the greater scope for BCP efforts, as opposed to exit planning efforts. The BCBS might also consider limiting detailed exit plan requirements to critical TPSP arrangements, as the current language appears to apply broadly to all service providers.

In order to promote consistent interpretation of the Principles, it would be helpful for the BCBS to provide examples elaborating on the proposed concepts of "planned" versus "unplanned" exits, as currently these terms and the distinction between them are not clear. The examples of "unplanned" termination include expiration or breach of contract, TPSP failure to comply with applicable laws or regulations, or a desire to seek an alternative TPSP, bring the activity back in-house or discontinue the activity. Each of these scenarios provided would appear to be consistent with an orderly, or planned, exit from a TPSP relationship. For example, in each of the first and last scenarios, the bank would know that the relationship was coming to an end well in advance (in the former case, due to implementation of contract governance, and in the latter case, due to business strategy planning that sits within the bank itself). We ask that the BCBS provides further clarification as to what would be considered an unplanned exit, or else remove it as a category and term.

While the Principles expect banks to have processes for the transfer of logical assets in a timely manner and appropriate format (Para. 65), these transfer timelines will likely be prolonged under an unplanned termination scenario. Strict expectations for the transfer of logical assets in timelines that would allow banks to remain within their tolerance for disruption would effectively equate to a ban on the use of certain technologies. We therefore recommend that rather than requiring transfer in a timely manner, BCBS require banks to assess and understand the timelines required to transfer such assets and plan accordingly.

Role of Supervisors (Principles 10-12)

Supervisory authorities are uniquely positioned to understand the risks posed by arrangements with certain TPSPs, particularly potential risks arising from the concentration of services provided by certain TPSPs, and can leverage their broad perspective and authority to address

[15] For example: long-term contracts with significant early termination penalties; proprietary data formats or APIs that are incompatible with other systems; and technical dependencies that are difficult to replicate or replace.

potential systemic risks, promote standardization of requirements across jurisdictions, and foster a more cohesive global approach to TPRM.

- Global systemic risk monitoring: While financial institutions recognize the importance of monitoring concentration risks with respect to their TPSPs, it is incumbent upon supervisors to assess whether there are systemic risks posed by the concentration of certain TPSPs, as individual financial institutions do not have sufficient information about how these services are being deployed across the sector. This also applies to mapping interconnections and interdependencies across the financial system and across borders. As noted above, there is still a lack of a common understanding of what constitutes concentration risk in relation to TPSPs.

  As the IIF has previously advocated, there may also be a useful role the global standard-setting bodies such as the FSB and Basel Committee can undertake in overall systemic risk monitoring arising from concentration of TPSPs, similar to the studies of central counterparty interdependencies undertaken in the past by the FSB with the Basel Committee, Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO).[16] Any such work would of course need to be appropriately governed, and any output would need to be carefully de-identified to ensure that no business confidential information is inadvertently disclosed through sharing the analysis.

- Registers: We strongly urge the BCBS to promote interoperable third-party registers with common data fields, and to work with other standard setters, such as the FSB, to pursue alignment of third-party registers, including by standardizing the data fields and data formats required to deliver information that meets common supervisory objectives. Such interoperable registers would significantly streamline the process for cross-border financial institutions to provide information and provide financial sector authorities with comparable data to help identify aggregate risk across the financial system, including potential systemic risks. The Basel Committee should also encourage regulators to limit changes to the format of, and means and frequency of updates to, registers to those that are strictly necessary. This would help reduce the number of situations in which financial institutions would need to divert resources from value-adding risk management activities to more administrative tasks and manual updates to registers. The application of the principle of data minimization for register requirements is also strongly encouraged, given the significant bank resources necessary to operationalize and maintain these tools. Supervisors should therefore only require a data field if it directly supports specific supervisory objectives.

- Information sharing and handling: While the Principles call for increased information sharing and reporting, security is crucial when it comes to access, exchange, storage and transmission of information. For example, Para. 70 includes reference to supervisors leveraging TPSP registers and maps of interconnections and interdependencies. Information in registers and on this type of mapping is highly sensitive and could represent a critical risk to operational and information security should it be accessed by bad actors. The concentration of this sort of information from multiple banks within a given supervisor could pose a significant risk to all those entities and, by extension, to financial stability.

  IIF members, including banks and TPSPs alike, request that the BCBS consider how supervisory authorities will store and protect information gathered related to TPSP

[16] As the IIF has previously advocated in its letter to the FSB in August 2023.

arrangements, including having robust security measures for transferring data and centralized storage of sensitive information within supervisory authorities. It is important for supervisors across the world to establish clear guidelines to protect the confidentiality and integrity of data related to TPSP arrangements, and careful consideration should be given to how sensitive information in any register of TPSP arrangements will be handled and protected by supervisory authorities.

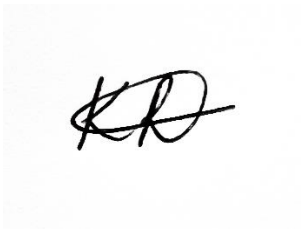
- International Coordination: Given the cross-border footprint of many financial institutions and TPSPs, the IIF strongly supports international coordination in relation to the treatment of TPRM and systemic TPSPs across the global financial industry. As recognized in the consultative document, many jurisdictions have already developed their own TPRM frameworks and standards and others are developing these at present. It is important to avoid regulatory fragmentation given the cross-border nature of many TPSP's business models, and for financial institutions that operate in multiple jurisdictions. Basel Committee members could consider developing a formal approach to recognizing equivalency of regulatory regimes for the resilience of TPSPs which are relevant from a systemic risk perspective.[17]

Conclusion

The IIF commends the Basel Committee for its proactive approach in refining its approach to TPRM in support of its broader objectives of supporting operational resilience and financial stability of the global banking system. We believe that with some modifications and consideration of the points raised in this letter, the proposed Principles can significantly enhance the resilience and stability of the banking sector in a forward-looking manner.

We thank you again for the opportunity to contribute to this important consultation. The IIF would be happy to discuss any aspects in more detail or provide additional perspectives, including by convening our global membership for a discussion. Please contact Martin Boer (mboer@iif.com), Katie Rismanchi (krismanchi@iif.com), or Melanie Idler (midler@iif.com) with any questions.

Respectfully submitted,



Katie Rismanchi
Deputy Director, Regulatory Affairs
Institute of International Finance

[17] Many TPSPs also achieve external certifications and validations from private-sector or public-sector entities, including the U.S. FedRAMP which is specifically for cloud products and services.

Appendix: Summary of specific text revisions proposed in the IIF comment letter

- Proposed new text is shown in **bold** and proposed deleted text has been struck through.
- Please note that this table is not an exhaustive summary of all the feedback and recommendations in the main IIF comment letter; it focuses on the specific drafting suggestions only for ease of reference.

BCBS Draft Para. Number (Linked to Corresponding IIF Comments)	BCBS Draft Text	IIF Proposed Revision
III. Definitions		
Critical TPSP arrangement	*A TPSP arrangement which supports or impacts one or more critical services provided to a bank.*	Suggest removing definition of Critical TPSP arrangement entirely. Alternatively, at a minimum, amend the definition to include "materially supports." For example: *A TPSP arrangement which **materially** supports ~~or impacts~~ one or more critical services provided to a bank.*
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.*	*A service provided to a bank, the failure or disruption of which could significantly impair a bank's viability~~,~~ **or** critical operations~~, or the ability to meet legal and regulatory obligations~~.* Alternatively, at a minimum, amend the definition to more closely align with potential resilience impact. For example: *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 **in a manner that affects the bank's viability and/or broader financial stability**.*

BCBS Draft Para. Number (Linked to Corresponding IIF Comments)	BCBS Draft Text	IIF Proposed Revision
Critical TPSP	*A TPSP that provides a critical service to a bank.*	Suggest removal of definition of Critical TPSP entirely.
Key nth party	*A service provider that is part of a TPSP's supply chain and supports the ultimate delivery of a critical service by a TPSP to a bank or that has the ability to access sensitive or confidential bank information (eg consumer data).*	*A service provider that is part of a TPSP's supply chain and ~~supports the~~* ***that is knowingly essential to*** *the ultimate delivery of a critical service by a TPSP to a bank ~~or that has the ability to access sensitive or confidential bank information (eg consumer data)~~.*
IV. Third-party risk management principles		
Paragraph 15	*Not all TPSP arrangements present the same level of risk and therefore not all arrangements require the same level or type of oversight or risk management.*	*Not all TPSP arrangements present the same level* ***or types*** *of risk and therefore not all arrangements require the same level or type of oversight or risk management.*
		Add a bullet point preceding the "Criticality" bullet point, titled "**Risk Assessment,**" setting out the holistic approach to TPRM which is detailed in the main IIF comment letter.
	Nth parties and supply chain: *…Banks should have appropriate risk management processes to identify and manage the supply chain risks, proportionate to the criticality of the services being provided…*	Nth parties and supply chain: *…Banks should have appropriate risk management processes to identify and manage the supply chain risks, proportionate to the* ***inherent risks and*** *criticality of the services being provided…*
Governance, risk management and strategy (Principles 1-2)		
Principle 1	*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.*	*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.*
Principle 2	*The board of directors should ensure that senior management implements the policies and processes of the third-party risk*	***Senior management, who is responsible for a firm's day to day operations,*** *~~The board of directors~~ should ensure that*

BCBS Draft Para. Number (Linked to Corresponding IIF Comments)	BCBS Draft Text	IIF Proposed Revision
	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.	***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.*
Paragraph 22	*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).*	*Banks should maintain a complete and up-to-date register of all TPSP arrangements (and* ***key*** *nth parties, as appropriate to the criticality of the service and associated risks).*
Risk Assessment (Principle 3)		
Paragraph 27	*The* risk assessment *stage of the life cycle is where banks identify and assess the criticality of potential services and the risks before entering into a proposed arrangement with a TPSP, in alignment with the bank's third-party strategy, policies and TPRMF.*	*The risk assessment stage of the life cycle is where banks identify and assess the* ***inherent risks and*** *criticality of potential services before entering into a proposed arrangement with a TPSP, in alignment with the bank's third-party strategy, policies and TPRMF.*
Paragraph 28	*When assessing criticality banks should consider factors such as 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.*	Recommend removing Para. 28 from the final Principles.
Paragraph 32	*Risks may change throughout the life cycle of the TPSP arrangement. Therefore, banks should perform risk assessments on an ongoing basis (refer to Onboarding and ongoing monitoring below).*	*Risks may change throughout the life cycle of the TPSP arrangement. Therefore, banks should perform risk assessments on an ongoing basis,* ***at a frequency commensurate to the inherent risks of the arrangement and its criticality to the bank*** *(refer to Onboarding and ongoing monitoring below).*
Due diligence (Principle 4)		

BCBS Draft Para. Number (Linked to Corresponding IIF Comments)	BCBS Draft Text	IIF Proposed Revision
Paragraph 36	*As part of the assessment of a TPSP's capacity and ability to deliver the services under the arrangement, banks should consider the TPSP's: …*	*As part of the assessment of a TPSP's capacity and ability to deliver the services under the arrangement,* ***commensurate to the inherent risks of the arrangement and its criticality****, banks should consider the TPSP's: …*
Paragraph 38	*As part of the assessment of relative benefits and costs associated with the TPSP arrangement, banks should consider:* *• the potential risks of not entering into a TPSP arrangement against the risks that the new TPSP arrangement may introduce or amplify known risks (eg replacing obsolete legacy system, difficulty in hiring and maintaining qualified staff);* *• the bank's ability (including cost, timing, contractual restrictions) to exit the TPSP arrangement and either transition to another TPSP or bring the activity back in-house; and* *• the bank's ability to adopt new and advanced technologies and the potential risks thereof.*	*As part of the assessment of relative benefits and costs associated with the TPSP arrangement, banks should consider:* *• the potential risks of not entering into a TPSP arrangement against the risks that the new TPSP arrangement may introduce or amplify known risks (eg replacing obsolete legacy system, difficulty in hiring and maintaining qualified staff);* *• the bank's ability ~~(including cost, timing, contractual restrictions)~~ to exit the TPSP arrangement* ***without undue disruption*** *~~and either transition to another TPSP or bring the activity back in-house~~; and* *• the bank's ability to adopt new and advanced technologies and the potential risks thereof.*
Contracting (Principle 5)		
Paragraph 42	*Banks' contracts governing critical TPSP arrangements should at a minimum include the provisions covered in paragraph 41 and those listed below:* *• conditions governing key nth parties (eg prior notification of use or change, incident reporting);* *…*	*Banks' contracts governing critical TPSP arrangements should at a minimum include the provisions covered in paragraph 41 and those listed below:* *• conditions governing key nth parties (e.g. prior notification of use or change* ***from the TPSP****, incident reporting* ***to the TPSP****)* *…*

BCBS Draft Para. Number (Linked to Corresponding IIF Comments)	BCBS Draft Text	IIF Proposed Revision
	• rights of banks to access, audit and obtain relevant information from key nth parties; *…* *• 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; …* *• TPSPs' obligation to take out insurance against insurable risks*	*• rights of banks to access, audit, and obtain relevant information from **the TPSP concerning** key nth parties;* *…* *• rights of supervisory authorities to access, audit and obtain relevant information from **the TPSP related to** key nth parties as permitted under applicable laws and regulations within the respective jurisdictions or bi-/multilateral agreements amongst supervisors; …* We suggest amending the final bullet point on insuring against uninsurable risks to be a consideration to ensure banks and TPSPs retain the flexibility to utilize insurance as a risk-transfer mechanism in a way that is most suitable to the risk being managed.
Onboarding and ongoing monitoring (Principles 6-8)		
Paragraph 47	*Ongoing monitoring should be aligned with banks' governance, risk management and strategy, the risks considered when the TPSP was selected, any new risks that have emerged since selection, and contractual obligations of the TPSPs. It should include key nth parties.*	*Ongoing monitoring should be aligned with banks' governance, risk management and strategy, the risks considered when the TPSP was selected, any new risks that have emerged since selection, and contractual obligations of the TPSPs. ~~It should include key nth parties.~~*
Paragraph 53	*…For critical services, banks should consider incorporating requirements related to incident reporting in the contracts, including minimum information to be reported. Contracts may require TPSPs to have clearly defined processes for identifying, investigating and remediating incidents related to contracted services and notifying banks in a timely manner of incidents that impact the TPSP's ability to meet contractual obligations…*	Resolve contradiction between optional "consider" language and Para. 42's mandatory requirement for TPSP incident reporting.

BCBS Draft Para. Number (Linked to Corresponding IIF Comments)	BCBS Draft Text	IIF Proposed Revision
Paragraph 58	*Banks should manage their dependencies on TPSP arrangements within their BCM. A bank's BCM should consider:* *• development, periodic review and updating of the bank's internal BCPs and DRPs with respect to TPSP arrangements;* *• periodic testing of the bank's BCPs and DRPs, considering a range of possible recovery strategies or compensating controls (eg switching to another TPSP, using multiple TPSPs, bringing the service in-house, employing a combination of on-premises and external data centres across different geographical regions) that can deliver a level of resilience consistent with the bank's risk appetite and tolerance for disruption;* *• lessons learned from incidents (if any) and result of the periodic testing; and* *• periodic updating of identified alternative providers.*	*Banks should manage their dependencies on TPSP arrangements within their BCM. A bank's BCM should consider:* *• development, periodic review and updating of the bank's internal BCPs and DRPs with respect to TPSP arrangements;* *• periodic testing of the bank's BCPs and DRPs, considering a range of possible recovery strategies or compensating controls ~~(eg switching to another TPSP, using multiple TPSPs, bringing the service in-house, employing a combination of on-premises and external data centres across different geographical regions)~~ that can deliver a level of resilience consistent with the bank's risk appetite and tolerance for disruption;* *• lessons learned from incidents (if any) and result of the periodic testing; and* *• periodic updating of identified alternative providers.*