CLIFFORD
CHANCE


9 October 2024

Consultation response

Basel Committee on Banking Supervision – Principles for the sound management of third-party risk, July 2024

The Global Financial Markets Association (the "GFMA") [1] appreciates the opportunity to respond to the Basel Committee on Banking Supervision's (the "BCBS") consultative document "Principles for the sound management of third-party risk" (the "Consultation").

The GFMA welcomes the BCBS's continued focus on designing and improving the risk management framework applying to interactions with third parties and supports the BCBS's technology-agnostic approach to the principles proposed in the Consultation (the "Principles"). We want to emphasize that a risk-based approach is foundational to the strength and dynamic nature of third-party risk management ("TPRM") frameworks as markets develop. We look forward to ongoing collaboration as the BCBS along with the Financial Stability Board ("FSB") and the International Organization of Securities Commissions ("IOSCO") continue to evaluate the role of third parties and necessary governance structures.

EXECUTIVE SUMMARY

Scope and relationship with existing BCBS guidance

The Principles are intended to create a holistic TPRM regime that aligns with the existing BCBS Principles for operational resilience[2] ("BCBS POR") and the Principles for the sound management of operational risk[3] ("BCBS PSMOR"), only integrating operational resilience objectives where appropriate. The Principles are also intended to complement the work of other international bodies addressing TPRM in the financial sector, including the FSB publication

[1] GFMA brings together three financial trade associations, including the Association for Financial Markets in Europe ("AFME"), the Asia Securities Industry & Financial Markets Association ("ASIFMA"), and the Securities Industry and Financial Markets Association ("SIFMA"). See Appendix 2 for further information.

[2] BCBS, *Principles for operational resilience*, March 2021, www.bis.org/bcbs/publ/d516.htm

[3] BCBS, *Revisions to the principles for the sound management of operational risk* - March 2021, www.bis.org/bcbs/publ/d515.htm

Enhancing Third-Party Risk Management and Oversight - A toolkit for financial institutions and financial authorities ("FSB TPRM Toolkit").[4] However, the current draft Principles do not adequately differentiate between operational resilience and broader TPRM considerations. The proposed approach prioritizes operational resilience, rather than recognizing it is only one risk assessment factor of a holistic TPRM framework that should address a much wider range of risks.

We urge the BCBS to reconsider the Principles with this in mind and have provided specific guidance on where individual Principles and guidance paragraphs should be expanded in line with a broader TPRM analysis and where an existing emphasis on operational resilience should be broadened to include non-resilience-related risks. Conversely, the Principles should also avoid conflating the concept of "criticality" which is tied to resilience with broader risk considerations. We recommend revisions to key definitions to ensure that the Principles' use of "critical" is narrowly focused, consistent with BCBS POR. Where we have suggested specific amendments to key definitions or Principles these are also set out in full in Appendix 1 for ease of reference.

Proportionality

While the Consultation states that proportionality should be embedded throughout the third-party lifecycle and all stages of the Principles, this is not always reflected in the drafting of individual Principles and related guidance where many requirements seem to apply universally to all third-party service providers (TPSPs) regardless of their criticality or risk level. We have provided examples of where this may be problematic and recommendations for how specific Principles and related guidance should be drafted more clearly.

Dependencies and interconnections mapping

Information resulting from mapping dependencies and interconnections is highly sensitive and would represent a risk to the operational and information security of individual banks, and potentially the wider market, if accessed by bad actors. As such, the Principles should be amended to reflect the importance of supervisors implementing appropriate security practices to better safeguard the sensitive data of individual banks and broader financial stability.

We suggest the BCBS considers whether the Principles go far enough in recognising the importance of security practices of supervisors and the risks arising from disclosures of sensitive information to them. These security practices should include limiting the collection of data to the minimum required to meet a specific supervisory objective, and ensuring that appropriate policies, processes and controls are in place regarding the usage, sharing and disposal of this data, in line with industry best practice and standards.

[4] 4 December 2023, https://www.fsb.org/wp-content/uploads/P041223-1.pdf

Additional Principles

We recommend that the BCBS considers incorporating several additional Principles to bolster the proposed TPRM framework. In particular, in order for supervisors to effectively monitor and manage risk at a systemic level, it is critical that they have sufficient mandates and tools for oversight and enforcement over critical third parties, supported by international cooperation and information sharing.

KEY ISSUES

1. **Scope and risk drivers**

Scope

1.1 While the Consultation makes clear that it is intended to supersede the 2005 Joint Forum Paper in respect of the banking sector[5] and be reflective of existing BCBS principles relevant to third-party risk management, such as BCBS POR and BCBS PSMOR, it is important for the document to articulate that operational resilience is only one of many risk types that fall under a TPRM regime. The Principles are intended to create a holistic TPRM regime that includes risk-based methodology and integrates operational resilience objectives where appropriate. We recommend that the Principles should explicitly state the wider focus on TPRM for implementation purposes. As stated above, resilience should only be one factor falling under TPRM.

Conflation of operational resilience and TPRM: a delineation of requirements applicable to operational resilience and to general TPRM should be drawn.

1.2 TPRM requires consideration of a broad spectrum of risk drivers. This is not fully reflected in the Principles, which currently conflate TPRM and operational resilience and overly emphasize operational resilience risks. While operational resilience can result from effective TPRM, it addresses different concerns and requires different mitigations. Central to this concern is the Consultation's focus on resilience considerations (and related concepts like "criticality") to determine the risk rating and categorization of third parties, as well as the inclusion of non-resilience-related considerations or impacts for the scoping of TPSP arrangements which, if disrupted, could impair the resilience of a bank or the broader financial system.

1.3 TPRM frameworks address a wide range of risks, such as data security, regulatory compliance, financial viability and reputational risks. Principle 3 and paragraph 30 of the Consultation reflect this and state that banks should consider all types of risks related to TPSP arrangements. The risk assessment outcome will determine the risk rating/categorization of a third party and dictate the oversight and controls required.

[5] The Joint Forum, *Outsourcing in financial services*, February 2005, www.bis.org/publ/joint12.pdf

This is complemented by a discrete assessment of the criticality of the arrangement to the bank and the broader financial system, i.e. whether disruption of the TPSP relationship would be material to the continued operation of the bank or its role in the financial system. This reflects the risk-based approach foundational to TPRM frameworks.

1.4 The potential impact of a third-party outage or failure on a bank's critical operations as defined by BCBS POR is therefore just one of many risks that banks should consider alongside a broader set of risks as part of a bank's holistic assessment of TPSP relationships. Given the potential impact on a bank's viability and operations, these relationships require specific resilience controls. Alongside this, TPSP relationships may still require enhanced due diligence and specific controls due to a range of other risk drivers and ratings. The categorization of the full range of risks presented by a particular TPSP relationship and tailoring of the level of oversight needed is fundamental to the risk-based approach that underpins TPRM frameworks.

1.5 However, the Principles combine these differing considerations and impacts into just the operational resilience scoping and oversight expectations. As a consequence, the Principles prescribe controls that may not be appropriately aligned to the actual risk posed by the third party. If measures designed to ensure operational resilience are required to be applied to general TPSP relationships this could result in a significant and disproportionate operational burden and related cost for banks that is not commercially sustainable. Conversely, some of the broader considerations required for a comprehensive TPRM assessment may be overlooked. **Accordingly, a delineation of requirements applicable to operational resilience and to general TPRM must be drawn.**

1.6 **Recommendation:** We request that the BCBS clarify its intention to provide standalone guidance on holistic TPRM approaches that include the risk-based methodology described above (i.e., that the inherent risk of a TPSP relationship and level of controls is informed by a range of risk drivers of which operational resilience is just one of many operational risks considered). The final Principles should acknowledge the holistic risk assessment that covers the full range of risks presented by a TPSP relationship, 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. While terminology may vary between firms, the Principles should not favor one nomenclature or methodology over another. However, the practice of assigning a risk rating is recognized as best practice.

2. Definitions of critical TPSP, critical service and critical TPSP arrangement

2.1 The Principles conflate resilience risk with other risks, creating an overly broad concept of "criticality," especially in the definition of "critical service," which deviates from the foundational objectives and criteria set out in BCBS POR.

2.2 In respect of the proposed definition of "critical service", removal of the reference to "ability to meet legal and regulatory compliance obligations" would be beneficial to avoid a potential significant extension of scope. For example, there are many forms of regulatory reporting which, if temporarily disrupted, would not impact a bank's viability or critical services but this would be captured within the current definition.

2.3 It is important that the Principles related to critical TPSPs are focused on ensuring the resilience of those services which **are** critical to the ongoing viability of the bank. There are many services provided to a bank, the temporary disruption of which would have extremely limited impact both on the bank's ability to do business and to its regulators. While these services may still be important, they do not justify the same level of requirements as for critical services.

2.4 In addition, the definition of "critical TPSP arrangement" is unnecessary to differentiate such arrangements or agreements in addition to "critical service" and "critical TPSP" - if a bank contracts with a third-party to manage a critical service the third party would already be considered a critical TPSP. As drafted, the definition is also too expansive and may capture relationships[6] that are not relevant to the operation of a bank, particularly because of the subjective and very wide reference to "supports or impacts" without any materiality qualifier. The concept adds no value to how banks tailor their risk management of such relationships based on inherent risks of a specific contracted service as well as the potential impact to the bank and its critical operations. It could also introduce confusion, for example as to whether services should be risk assessed individually or collectively. Finally, it may also lead to unhelpful interpretive differences across jurisdictions.

Recommendations:

2.5 The Principles and definitions should be revised to state that "critical" focuses narrowly on resilience considerations, aligned with the BCBS POR definition of critical operations.

2.6 The definition of "critical service" should reflect the narrow focus of "critical" outlined above at paragraph 2.1 and be amended to state:

---

[6] We note that the equivalent definition to "TPSP arrangement" referenced on page 6 of the FSB TPRM Toolkit is "Third-party service relationship" and that this may may refer to a third-party service dependency or third-party service arrangement. See further paragraph 6.1 of this response.

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

Our strong preference is for the component of the definition referencing legal and regulatory compliance obligations to be taken out for the reasons outlined above. If it remains then the requirement would need to be qualified. For example, "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 is a similar approach but provides greater clarity than the equivalent definition in the FSB TPRM Toolkit[7] which includes a qualification by reference to "ability to meet **key** legal and regulatory obligations".

2.7 The definition of "critical TPSP arrangement" should be removed.

3. Proportionality

3.1 We welcome the comment from BCBS in paragraph 15 of the Consultation that proportionality and taking a risk-based approach should be embedded in all stages of the third-party life cycle and apply to all Principles. However, the principle of proportionality does not seem to have been fully reflected in the Principles, as many of the requirements are proposed to apply to all TPSPs, regardless of the risk associated with those TPSPs or their criticality.

3.2 **Recommendation**: We therefore ask the BCBS to clearly provide that scope for all of the requirements set out under the Principles must be implemented proportionally based on the risks associated with the service provided by the TPSP, up to and including disapplying provisions where the risk associated with the TPSP relationship does not warrant the application of that provision.

3.3 An example of this can be seen in relation to intragroup TPSPs. In many cases intra-group TPSPs are subject to robust regulatory requirements and risk frameworks that apply to banks, which can provide a high level of reliability and resilience for those services. The Principles should take this into account and allow this to be part of the consideration when assessing the risks associated with those intragroup TPSP arrangements.

4. Requirements on "nth parties"

4.1 The proposed definition of "key nth party" is "A service provider that is part of a TPSP's supply chain and supports the ultimate delivery of a critical service by a TPSP

[7] See page 6 of the FSB TPRM Toolkit.

to a bank or that has the ability to access sensitive or confidential bank information (e.g. consumer data)."

4.2 While an nth party's ability to access sensitive or confidential bank information is an important consideration for data protection and cybersecurity, including it in TPRM requirements may create duplication and conflicts. It is also not appropriate for an nth party to become a "key" nth party simply because it "supports" a critical service, as arguably any nth party in the chain of a critical service would be "supporting" the delivery of such service. This may lead to nth parties which have minimal impact on the continuity of critical services being included as a critical nth party.

4.3 **Recommendation**: We consider that a more appropriate definition of "key nth party" is:

- Key nth party: A service provider that is part of a TPSP's supply chain and that is knowingly essential to the ultimate delivery of a critical service by a TPSP to a bank.

4.4 Clarification is also needed on the treatment of nth parties in a group structure, where services are provided via an intragroup affiliate which originate from a non-intragroup third party. Given the proposed application at an entity level, it is critical that the Principles clearly define which entities should be considered TPSPs and/or nth parties in such circumstances.

5. Additional Principles

To further strengthen the proposed TPRM framework, we **recommend** the BCBS include the following additional Principles.

Data minimization and standardization

5.1 In our view, a general principle of data minimization and standardization should be incorporated into the Principles in relation to the collection and retention of data in registers in relation to TPSP arrangements and under similar requirements. This would benefit all parties from a risk perspective, as well as an administrative and cost perspective. As jurisdictions have existing or are introducing new requirements for banks to maintain registers of third-party service providers, this could be supported by an initiative to create a harmonized global reporting template for such registers.

Supervisory oversight

5.2 An effective holistic TPRM and operational resilience regime must consider risk at both an individual bank and systemic level. However, in order to effectively monitor and manage risk at a systemic level, it is critical that supervisors have sufficient mandates and tools that give them the right level of oversight and allow them to enforce any new

third-party risk regime effectively. Where it is determined that this is best achieved through supervisors having direct oversight and responsibility over critical third parties, this should be supported with direct rights of enforcement for the supervisor over such third parties.

5.3 This will enable supervisors with oversight or responsibility for firms which act as TPSPs, critical TPSPs, or key nth parties to address any concerns they have regarding the resilience of these parties or their ability to ensure continuity of the services they provide with those parties directly. It also ensures that supervisors are effectively able to monitor and address potential systemic risk in relation to any critical TPSPs. The traditional approach where regulators only enforce against the bank, thus indirectly impacting TPSPs, could be ineffective in particular where the TPSP is a major industry-wide service provider. However, the use of such direct oversight regimes for critical third parties is in its infancy and it is not yet clear what challenges may arise in practice.

5.4 Where such direct oversight regimes do exist, it is critical that there is international cooperation and information sharing between supervisors to maximize effectiveness and avoid any potential conflicting approaches.

5.5 ***Additional principle for Supervisors***

Where local rules implementing the Principles may result in substantially new requirements for banks, it should be recommended for supervisors to introduce a transitional period or phased lead-in for these new frameworks so that financial institutions have sufficient time to implement the new requirements.

FEEDBACK ON DEFINITIONS AND DRAFT PRINCIPLES

6. Definition of "TPSP arrangement"

6.1 **Recommendation**: We note that the equivalent definition to "TPSP arrangement" under the existing FSB TPRM Toolkit is "Third-party service relationship"[8] and that this may may refer to a third-party service dependency or third-party service arrangement. We emphasize that the BCBS should weigh the strength in having consistency in terminology between the Principles and the existing FSB TPRM Toolkit to support best practices across the financial services ecosystem and mitigate the risk of market fragmentation. We have generally used the term TPSP arrangement when we reference suggested amendments to the Principles in this response to be consistent with the approach taken in the Consultation, however, our strong preference is that this definition is reconsidered in line with the FSB approach.

[8] See page 4 of the FSB TPRM Toolkit, including footnote 7.

6.2 The exclusion of financial service transactions from the definition of "TPSP arrangement" requires further clarification. A particular financial services transaction may be momentary but often takes place as part of an ongoing financial services arrangement. As drafted it is unclear how these broader ongoing services would be treated. The drafting should be clarified to ensure that ongoing services that qualify as financial services are also excluded.

6.3 There should also be an exclusion from the definition of "TPSP arrangement" for arrangements where the provider itself is also a bank that is subject to the same principles or equivalent rules under any relevant domestic framework given the same standards will already apply to that bank provider.

7. Definition of "supply chain"

7.1 Clarification of services considered part of the supply chain would be beneficial. We would expect this to relate to parties in the chain used to deliver all or part of the relevant services to the bank. This will better ensure consistent application when assessing supply chains.

7.2 **Recommendation**: For example, "Supply chain: Where a TPSP uses another provider to deliver all or part of the services being provided to a bank. This may include infrastructure, physical goods, services and other inputs directly or indirectly utilised for the delivery of the service."

8. Proposed new definition – Systemic third-party dependency

8.1 Although the draft Principles include systemic risk under the definition of 'concentration risk', there is no defined term for systemically-critical services. An additional definition is therefore requested to address a 'critical service' that recognises a major and prolonged outage causing severe disruption that poses systemic risks to market integrity and financial stability. This is crucial in order for supervisory authorities to accurately and proportionately assess systemic risk posed by certain TPSPs in line with the Principles for supervisors. This is also consistent with the approach taken by the FSB which included a definition of "systemic third-party dependency" in the FSB TPRM Toolkit.[9]

8.2 **Recommendation**: Please add the following new definition and accompanying footnote and include references where appropriate in the Principles, for example in Principles 11 and 12. This definition is consistent with the FSB TPRM Toolkit definition, with the addition of "critical" to ensure suitable focus.

[9] See page 6 of the FSB TPRM Toolkit.

- "**Systemic third-party dependency:** a dependency on one or more **critical** services provided by a service provider to financial institutions where their disruption or failure has been identified by a relevant financial authority as having potential implications for financial stability."

  Accompanying footnote: Financial authorities in some jurisdictions may use a different term in a similar context, taking into account the different approaches used in the jurisdictions.[10]

9. **Paragraph 15**

9.1 Paragraph 15 of the Consultation sets out some key concepts relevant to determination of risk that apply throughout the Principles.

9.2 **Recommendation**: We suggest amending paragraph 15 to reinforce the clear delineation between operational resilience and the broader spectrum of risk drivers relevant for holistic TPRM.

(a) The first line of paragraph 15 should be amended to state "Not all TPSP arrangements present the same level **or type** of risk…"

(b) We suggest a new leading bullet point is added above "Criticality" which details the nature of the initial risk assessment, for example, looking at all the inherent risks of an arrangement. This is then complemented by the criticality assessment that would follow, which reflects on the importance of the service to the bank.

10. **"*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*."**

10.1 The proper role of the board is to be responsible for overseeing the business and affairs of the banking organization, while senior management is responsible for day-to-day operations. The board should be expected to review, discuss, and approve overall risk management strategy for the banking organization and oversee the establishment of the most important policies. The approval of the vast majority of policies that address day-to-day operations such as TPRM policy should instead be within the purview of senior management, which has the subject matter expertise, experience, and time to perform this role effectively.

10.2 **Recommendation**: We therefore propose the guidance be revised to better reflect the important distinction between the roles of management and the board of directors and suggest Principle 1 is amended to state: "The board of directors has ultimate

[10] See footnote 13 on page 6 of the FSB TPRM Toolkit which also references certain related sections of the FSB TPRM Toolkit.

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."

10.3 The Principles should also recognize that from a governance perspective not all parts of a business will have a board structure. The Principles should look to whatever the most senior governance forum is in a given jurisdiction, rather than focusing specifically on boards. This approach would be consistent with the approach taken already in the BCBS POR and BCBS PSMOR.

11. **"*Principle 2: 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."***

11.1 The board can have responsibility for oversight of the TPRMF and can hold management accountable for the implementation of the policies and processes of the TPMRF in line with the bank's third-party strategy, including reporting of TPSP performance and risks related to TPSP relationships, and mitigating action, but is not directly responsible for this.

Recommendations:

11.2 This Principle should therefore be modified to state "Senior management, who are responsible for a firm's day-to-day operations, should ensure that effective 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."

11.3 It is also currently unclear how the requirements under Principle 2 on the responsibility of boards apply in a group scenario. In particular, we propose clarifying that a centralized management of arrangements with certain critical TPSPs at group level would not cause a breach of this Principle.

11.4 Paragraph 19 of the Consultation mentions cloud service providers specifically in the context of shared responsibility. It would be helpful if the Principles are amended to provide more specific guidance on how banks should manage shared responsibilities with cloud service providers and how this differs from other types of TPSP.

11.5 Paragraph 22 of the Consultation requires banks to include nth parties in the register, "as appropriate to the criticality of the service and associated risk." More clarity is needed here, as the current expression is vague and likely to lead to significant deviation between firms. We suggest this requirement is adjusted so that:

(a) only key nth parties' arrangements need to be reflected in the register (with the necessary limitation and certainty on the definition of key nth parties, as discussed above); and

(b) the principle of data minimization should be reflected in the requirement for banks to maintain a register of all TPSP arrangements, with supervisors working on standardization as discussed in paragraph 5.1 above.

11.6 Paragraphs 22 and 23 of the Consultation require banks to conduct mapping of interdependencies and interconnections of TPSPs. Whilst it is inferred that this requirement should be proportionate to the risk, and therefore that mapping requirements which are typically extremely costly, time consuming and complex should only be conducted for critical TPSPs, reinforcement of this would be useful to avoid unnecessarily onerous activity being required.

11.7 Furthermore, information from the mapping of dependencies and interconnections is highly sensitive and could represent a risk to operational and information security of not only an individual bank, but the broader industry, should it be accessed by bad actors. The concentration of information on dependencies/interconnections for every part of the chain of critical services across supervised banks, with any given supervisor, could represent a significant potential risk to all involved entities, and subsequently to financial stability. Security practices at regulators should reflect this level of risk and be communicated to the banks whose sensitive data is being held. See our comments in relation to Principle 11 below for our suggested amendments to limit the collection of such data to specific supervisory objectives and ensure appropriate security policies are in place within the collecting regulator.

11.8 Paragraph 23 of the Consultation requires banks to assess concentration risk at the time of due diligence and periodically throughout the life cycle of a TPSP. The requirement to assess concentration risks associated with nth parties is challenging. Further clarity is required as to whether the concentration risk is intended to also be assessed at nth parties' level. If this is the intention, it is important that such concentration risks should only be required to be considered for those nth parties identified by the TPSP as potential key nth parties.

11.9 Paragraph 23 of the Consultation also sets out examples of measures banks may take to manage concentration risk. These suggestions could be interpreted as proposing or requiring specific solutions to be deployed, which may not be feasible or appropriate in individual circumstances. Additionally, some of the examples cited may not be relevant for all forms of TPSP, in particular non-outsourcing TPSPs (e.g., software license providers). There is also a risk that such example mitigants may quickly become obsolete. We therefore propose that these example mitigants be removed from the final Principles.

12. **"*Principle 3: Banks should perform a comprehensive risk assessment under the TPRMF to evaluate and manage identified and potential risks both before entering into and throughout a TPSP arrangement.*"**

12.1 Banks consider both operational risk and operational resilience in the assessment of all third parties, for example during on-boarding. A third party can be providing a non-critical service but still give rise to operational risks that must be managed. The BCBS framework should encourage banks to consider both operational risks and the impact the service could have on a bank's operational resilience when assessing third parties. However, this should be balanced with an assessment of what is proportionate for any particular arrangement.

12.2 As currently drafted, it is not clear that the potentially onerous requirement for a comprehensive risk assessment described in the explanatory paragraphs for Principle 3 would be qualified by proportionality. This may result in a disproportionate cost and time impact for TPSP arrangements that do not relate to critical TPSPs or critical services.

12.3 Conversely, the current guidance in the paragraphs following Principle 3 may not go far enough from an operational risk management perspective. It focusses on the identification of critical services and does not cover the real continuum in relation to other risks that exist when categorizing and tailoring the level of oversight needed. For example, other levels of risk that might not lead to a service being deemed critical but that are also important and that would still require enhanced due diligence and specific controls to address the risk drivers could be more explicitly addressed by reference to existing principles and guidance under BCBS PSMOR.

12.4 **Recommendation**: This Principle and related guidance should be amended to expressly state that it should be applied proportionally and to expand its focus beyond critical services in line with a broader TPRM approach. In line with our recommendation above that the Principles should state that "critical" and the definition of "critical service" focus narrowly on resilience considerations, paragraph 28 of the Consultation should also be amended for consistency as it expands on the criteria for criticality. When looking at the listed factors in paragraph 28 to assess criticality, banks should consider these with a view to whether ultimately the TPSP arrangement could significantly impair a bank's viability or critical operations.

12.5 Paragraph 30 of the Consultation requires banks to consider known risks that may be reduced or better managed and potential risks that may arise from a proposed arrangement and document the process and results of the analysis. **Recommendation:** In line with the requests above, we propose that the drafting is clarified to reflect a proportional, risk-based approach where concentration and supply chain risks are only required to be assessed for critical TPSPs and their subcontractors.

13. ***"Principle 4: Banks should conduct appropriate due diligence on a prospective TPSP prior to entering into an arrangement."***

13.1 Paragraph 38 of the Consultation 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." This requirement does not seem to give sufficient consideration of all possible approaches should an exit be required and may not be appropriate in all circumstances. This may ultimately be interpreted as requiring specific courses of action for banks when they exit a TPSP arrangement.

13.2 **Recommendation**: Accordingly, we propose that the BCBS amend the second bullet point of paragraph 38 as below:

"As part of the assessment of relative benefits and costs associated with the TPSP arrangement, banks should consider:

- …
- 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 to exit the TPSP arrangement~~; and
- …"

14. **"*Principle 5: TPSP arrangements should be governed by legally binding written contracts that clearly describe rights and obligations, responsibilities and expectations of all parties in the arrangement.*"**

14.1 As this Principle and some of the following paragraphs (e.g., Paragraph 41) are not currently expressly qualified by reference to proportionality or criticality, they may unintentionally require banks to go beyond what is proportionate for TPSP arrangements that do not impact in any way on a bank's ability to continue its operations. For example, direct access and audit rights for banks and/or supervisors are not typical or generally appropriate outside of the context of critical services. Obligations and responsibilities relating to security, resilience and other technical configurations should again be limited to TPSP arrangements for critical services and not all TPSP arrangements. **Recommendation**: This Principle and related guidance should be amended to expressly state that it should be applied proportionally.

14.2 In addition, the requirement outlined in Paragraph 42 of the Consultation to include provisions for rights of banks to have access, audit and obtain relevant information from key nth parties is burdensome and will be difficult for banks to comply with in practice. **Recommendation**: At a minimum, this expectation should be revised to reflect the actual relationship dynamic between the bank, TPSP, and key nth party by stating the

information on key nth parties to be provided by the TPSP, i.e., the contracting service provider to the key nth party.

15. **"*Principle 6: Banks should dedicate sufficient resources to support a smooth transition of a new TPSP arrangement in order to prioritise the resolution of any issues identified during due diligence or interpretation of contractual provisions.*"**

15.1 This Principle is not currently expressly qualified by reference to proportionality or criticality and therefore may unintentionally require banks to go beyond what is proportionate for insignificant TPSP arrangements that do not impact in any way on a bank's ability to continue its operations. For example, as outlined at paragraph 11.6 above, mapping of interdependencies for TPSPs is typically extremely costly, time consuming and complex and therefore should only be required for critical TPSPs. **Recommendation**: This Principle and related guidance should be amended to expressly state thar it should be applied proportionally.

16. **"*Principle 7: Banks should, on an ongoing basis, assess and monitor the performance and changes in the risks and criticality of TPSP arrangements and report accordingly to board and senior management. Banks should respond to issues as appropriate.*"**

16.1 Again, given the application to all TPSP arrangements with no qualification by proportionality or criticality, this requirement is likely to require banks to take action that may be disproportionate for insignificant TPSP arrangements that do not impact in any way on a bank's ability to continue its operations. **Recommendation**: This Principle and related guidance should be amended to expressly state that it should be applied proportionally.

16.2 Paragraph 47 of the Consultation proposes the inclusion of key nth parties in ongoing monitoring. The direct monitoring of nth parties is challenging given there is no direct relationship between the bank and such nth parties. A proven and more proportionate approach to achieve the same outcome is for banks to monitor the service being provided. This approach would allow banks to identify material issues with the delivery of services without the need to establish monitoring of nth parties which the bank has no legal relationship with. **Recommendation:** Accordingly, we recommend deleting the last sentence (i.e., "It should include key nth parties.") from paragraph 47.

16.3 Paragraph 48 of the Consultation sets out the examples of triggers for review of TPSP arrangements, which are extensive and may lead to excessive and unnecessary review processes where these changes do not 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. **Recommendation:** Accordingly,

we propose to limit such reviews, so they are only triggered when events directly impact the TPSP's ability to provide their services to the bank.

17. **"*Principle 8: Banks should maintain robust business continuity management to ensure their ability to operate in case of a TPSP service disruption.*"**

17.1 Paragraph 58 of the Consultation in its second bullet point sets out a list of potential recovery strategies or compensating controls which banks should consider in their business continuity management ("BCM"). These measures could be interpreted by some institutions or supervisors as requiring these specific methods to be leveraged in all instances. Furthermore, some of the examples will not be relevant across different types of TPSPs, for instance banks will not be able to bring services in-house where these services pertain to, for example, software license providers for word processing software. **Recommendation**: As such, we suggest that the BCBS remove these specific examples to avoid misunderstanding or otherwise clarify that they are not intended to apply in all circumstances.

17.2 Paragraph 59 of the Consultation requires a bank's BCM to include "assurance testing (eg walkthroughs, tabletops and simulations) that the TPSP's BCP methodologies are robust." This may raise some practical challenges. For example, in respect of assurance testing of critical TPSPs with a high level of market concentration where sequencing a large number of individual assurance tests for a single provider may impact the useability of that service for other users. **Recommendation**: We propose that, in line with general risk management principles and the approach under existing frameworks such as BCBS PSMOR and BCBS POR, banks should be able to determine the most appropriate and proportionate approach taking into account both the bank's size and operations, as well as the service being provided. Where supervisors have adequate powers in respect of critical TPSPs it may be more appropriate that such testing is led by the relevant authority, so that the wider industry can rely on the supervisor-mandated testing. Alternatively, banks should be able to rely on the resilience testing conducted by the critical TPSP, provided that the TPSP can evidence the quality of the testing meets the expectations of the bank and that the services provided to the bank were included in the testing.

18. **"*Principle 9: Banks should maintain exit plans for planned termination and exit strategies for unplanned termination of TPSP arrangements.*"**

18.1 Principle 9 mandates the maintenance of exit plans and strategies for all TPSP arrangements with no qualification by proportionality or criticality. As a result, this requirement is likely to require banks to take action that may be disproportionate for insignificant TPSP arrangements that do not impact in any way on a bank's ability to continue its operations. **Recommendation**: We propose adopting a proportional, risk-

based approach, such that Principle 9 should only be applied to arrangements with critical TPSPs or for critical services.

18.2 Clarification on the way that exit plans and exit strategies are defined and being applied would also be helpful as the current drafting is very specific and differs from a more general understanding of the terms and market practice.

18.3 Paragraph 63 of the Consultation introduces requirements for regular testing of exit plans which can be very challenging from an operational perspective. We are concerned that the potential scope of "other factors" included in the list of factors for which exit plans need to be regularly updated and tested for is very broad. **Recommendation:** We suggest that the drafting is clarified so that extensive additional testing requirements could not be introduced on this basis, particularly to the extent that such requirements would necessitate involvement of the potential new service provider.

18.4 We also seek additional clarification from the BCBS on the concept of "unplanned" terminations. The examples provided 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. We note that each of these scenarios would result in an orderly (planned) exit from the TPSP and that exiting a TPSP during a material operational incident may negatively and significantly impact the bank's ability to recover from an incident. It also may be challenging to differentiate between issues from the exit and the incident. **Recommendation:** As a result, we recommend that the BCBS clarify the drafting and requirements here and further describe what an unplanned exit is or consider removing unplanned terminations as a category.

19. **"*Principle 10: Supervisors should consider third-party risk management as an integral part of ongoing assessment of banks.*"**

We have no specific comments on Principle 10.

20. **"*Principle 11: Supervisors should analyse the available information to identify potential systemic risks posed by the concentration of one or multiple TPSPs in the banking sector.*"**

20.1 Paragraph 70 of the Consultation includes a reference to supervisors leveraging maps of interconnections and interdependencies. In line with our comments in relation to Principle 2 above, information on this sort of mapping is highly sensitive and could represent a critical vulnerability and risk to operational and information security if obtained by bad actors. The concentration of this sort of information regarding multiple banks with any given supervisor therefore represents a risk to those entities individually and collectively and could ultimately impact financial stability.

20.2 **Recommendation**: To the extent that supervisory authorities need to collect this sort of sensitive information from banks, it should be done on a limited and secure basis to minimize potential security risks. The Principles should therefore be amended to reflect the importance of security practices of supervisors given the sensitivity of this information. These security practices should include limiting the collection of data to the minimum that is required to meet a specific supervisory objective, and ensuring that appropriate policies, processes and controls are in place regarding the usage, sharing and disposal of this data, in line with industry best practice and standards.

20.3 It should also be recognized that there is an inherent challenge for banks to source and validate information in relation to nth parties. Banks are reliant on the third parties to provide such information and in many cases will be unable to independently verify its accuracy.

21. ***"Principle 12: Supervisors should promote coordination and dialogue across sectors and borders to monitor systemic risks posed by critical TPSPs that provide services to banks."***

21.1 Given the cross-jurisdictional footprint of many critical TPSPs, regulatory interoperability is paramount. Consistent methods of identifying and directly overseeing systemic TPSPs and their management of risks will benefit both firms and supervisors. This would also strengthen and enforce the role TPSPs play in contributing to strengthened resilience, thus reducing the likelihood of disruption.

21.2 Adoption of common data standards for third-party and outsourcing registers is key to supporting collaboration between supervisors.

We appreciate your consideration of our comments and proposals and remain at your disposal to discuss any of these views in greater detail.

Respectfully submitted,

Allison Parent
Executive Director
Global Financial Markets Association

Appendix 1
Proposed Specific Amendments to Definitions and Principles

To aid review we have set out certain specific amendments to key definitions and Principles in full below. Further comments, including specific drafting suggestions for guidance paragraphs in the Principles, are detailed throughout the main body of this response.

DEFINED TERM/PRINCIPLE	**BCBS PROPOSED DRAFTING, AS AMENDED**	**GFMA PROPOSED DRAFTING**
Critical service: *For further details see paragraph 2 above.*	A service provided to a bank, the failure or disruption of which could significantly impair a bank's viability~~,~~ **or** 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.
Critical TPSP arrangement: *For further details see paragraph 2 above.*	~~A TPSP arrangement which supports or impacts one or more critical services provided to a bank.~~	*[We request definition to be deleted.]*
Key nth party: *For further details see paragraph 4 above.*	Key nth party: 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)~~.	A service provider that is part of a TPSP's supply chain and that is knowingly essential to the ultimate delivery of a critical service by a TPSP to a bank.
Supply chain: *For further details see paragraph 7 above.*	~~The network of entities that provide infrastructure, physical goods, services and other inputs directly or indirectly utilised for the delivery of a service to a bank, limited to the services under a TPSP arrangement.~~	Where a TPSP uses another provider to deliver all or part of the services being provided to a bank. This may include infrastructure, physical goods, services and other inputs directly

		or indirectly utilised for the delivery of the service.
Systemic third-party dependency: *For further details see paragraph 8 above.*	-	A dependency on one or more critical services provided by a service provider to financial institutions where their disruption or failure has been identified by a relevant financial authority as having potential implications for financial stability. Accompanying footnote: Financial authorities in some jurisdictions may use a different term in a similar context, taking into account the different approaches used in the jurisdictions.
Principle 1: *For further details see paragraph 10 above.*	The board of directors has ultimate responsibility for ~~the oversight of all TPSP arrangements~~ **overseeing the management of the bank's third-party risks** and should approve a clear strategy for ~~TPSP arrangements~~ **TPRM** 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 and should approve a clear strategy for TPRM within the bank's risk appetite and tolerance for disruption.
Principle 2: *For further details see paragraph 11 above.*	~~The board of directors~~ **Senior management, who are responsible for a firm's day-to-day operations,** should ensure that ~~senior management implements the~~ **effective** policies and processes of the third-party risk management framework (TPRMF) **are in place and** in line with the	Senior management, who are responsible for a firm's day-to-day operations, should ensure that effective 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

	bank's third-party strategy, including reporting of TPSP performance and risks related to TPSP arrangements, and mitigating actions.	related to TPSP arrangements, and mitigating actions.

Appendix 2

Overview of the GFMA

The **Global Financial Markets Association** ("GFMA") represents the common interests of the world's leading financial and capital market participants to provide a collective voice on matters that support global capital markets. We advocate on policies to address risks that have no borders, regional market developments that impact global capital markets and policies that promote efficient cross-border capital flows, benefiting broader global economic growth. The GFMA brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe ("AFME") in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association ("ASIFMA") in Hong Kong and the Securities Industry and Financial Markets Association ("SIFMA") in New York and Washington are, respectively, the European, Asian and North American members of GFMA.