UK Finance

UK Finance response to the BCBS Consultation on *"Principles for the sound management of third-party risk"*

9 October 2024

Introduction

UK Finance appreciate the opportunity to respond to the Basel Committee on Banking Supervision's (BCBS) consultation on the proposed "*Principles for the Sound Management of Third-Party Risk"*. We recognise the critical importance of effective third-party risk management (TPRM) in maintaining the operational resilience and stability of banks and the broader financial system.

Our response aims to provide constructive feedback on the proposed Principles, highlighting areas where clarity and alignment with existing frameworks, such as the BCBS Principles for Operational Resilience (POR) and the Principles for the Sound Management of Operational Risk (PSMOR), could enhance their effectiveness. We have structured our comments according to the 12 Principles outlined in the consultation, ensuring a comprehensive review that addresses both overarching concerns and specific recommendations.

Overall Feedback

Alignment with Existing Principles and Definitions

In UK Finance's view It is crucial that the TPRM Principles align closely with the overarching objectives of the BCBS POR and PSMOR. Creating global expectations based on jurisdictions whose regulations may dilute or confuse these objectives should be avoided. Specifically, definitions such as "critical service" and "key nth party" should be revised to better align with the operational resilience framework or, at a minimum, with the definitional language set out in the Financial Stability Board's (FSB) TPRM Toolkit.

Holistic Risk Management Approach

Effective management of third-party risk is vital for a bank's operational resilience. Within this framework, certain third-party arrangements should be considered "critical" due to their potential impact on resilience and should be subject to enhanced controls and oversight. However, we have identified two overarching issues that may undermine this approach:

1. Overly Broad Definition of "Critical": The Principles adopt an expansive definition of what constitutes "critical," which could lead banks to allocate limited resources to third-party arrangements that do not pose a genuine threat to operational resilience.
2. Disproportionate Emphasis on Operational Resilience Risk: The Principles place significant emphasis on operational resilience risk, often neglecting broader risk management concerns that banks should consider when managing third-party risk and tailoring controls accordingly.

These issues may result in the application of complex and resource-intensive resilience-related controls to an excessively wide range of third-party arrangements.

Recommendations:

- Clarify the Intention of the Principles: The BCBS should clarify that the Principles provide standalone guidance on holistic TPRM approaches, including the risk-based methodology where operational resilience is one of many risks considered.
- Acknowledge Holistic Risk Assessment: The Principles should recognise that banks perform holistic risk assessments covering the full range of risks presented by third-party arrangements, assigning risk ratings or categorisations, and tailoring oversight accordingly.
- Refine the Definition of "Critical": Explicitly state that the term "critical" is narrowly focused on resilience considerations, aligned with the definition of critical operations in the BCBS POR. Amend the definition of "critical service" to better reflect its focus on resilience risks and impacts.

- Tailor Control Requirements: Amend control requirements for critical third-party service provider (TPSP) arrangements to ensure they address risks to the continued provision of critical services, rather than other risks a TPSP arrangement could present.
- Encouragement of Efficiency : We encourage the inclusion of a principle for supervisors encouraging the implementation of measures designed to lessen the reporting burden on banks. These would include greater consideration data minimisation and the format of TPSP registers.

Specific Feedback on the Principles:

Governance Risk Management and Strategy

Principle 1: Board Responsibility

Current Principle: 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.

Issue:

The current drafting suggests that the board is expected to provide governance and oversight of all TPSP arrangements directly, which is impractical and inconsistent with governance best practices.

Recommendation:

- **Clarify the Board's Role:** Amend Principle 1 to reflect the board's proper role in overseeing TPRM frameworks rather than directly managing TPSP arrangements.

Suggested Revision:

"Principle 1: The board of directors (or equivalent body) has ultimate responsibility for overseeing the management of the bank's third-party risks and should approve (or appropriately delegate approval of) a clear strategy for TPRM within the bank's risk appetite and tolerance for disruption."

- **Clarity:** UK Finance recommends that the BCBS append their final document with a footnote or other suitable reference clarifying that "board" refers to the board of directors or equivalent governance body, similar to the approach in the Basel Committee's *Corporate Governance Principles for Banks (2015).*

Principle 2: Senior Management Responsibility

Current Principle: Senior management should ensure that effective policies and processes of the TPRM framework are in place and in line with the bank's third-party strategy, including reporting of TPSP performance, related risks, and mitigating actions.

Issue(s):

Principle 2 should emphasise that senior management is responsible for implementing the TPRM framework in line with the bank's third-party strategy.

UK Finance request acknowledgement that banks should not be constrained to a single Third-Party Risk Management policy when existing internal and external TPRM policies, and others such as operational resilience, complement each other. Similarly, UK Finance believes that banks should not be constrained to a single third-party strategy as intra-group and external strategies can be different but complementary.

Recommendation:

- **Clarify Senior Management's Role:** Amend Principle 2 to accurately reflect senior management's responsibilities.
- **Recognition of complimentary and interlocking strategies**: The BCBS should include text in their final document highlighting the importance of complimentary approaches to TPRM including operational resilience. The BCBS should avoid text indicating that the adherence to a single TPRM policy is required for all circumstances including intragroup arrangements.

Suggested Revision:

"Principle 2: Senior management should ensure that effective policies and processes of the TPRM framework are in place and in line with the bank's third-party strategy, including reporting of TPSP performance, related risks, and mitigating actions."

Risk Assessment and Due Diligence

Principle 3: Risk Assessment

Current Principle: Banks should identify and assess risks associated with TPSP arrangements before entering into, and throughout the lifecycle of, the arrangement.

Issue:

The criteria for determining "*criticality*" include factors such as "*tolerance for disruption*" and "*nature of data or information shared*," which are more appropriately considered during inherent risk assessments.

Recommendation:

- **Revise Criticality Criteria:** UK Finance would like the BCBS to remove these factors from the criticality assessment and consider them within the broader inherent risk evaluation.

Additional Comments:

- A bank's tolerance for disruption should not influence the importance of a service to its operations. Similarly, the nature of data shared is a factor in inherent risk assessment, not criticality.

Principle 4: Due Diligence

Current Principle: Banks should conduct appropriate due diligence on TPSPs before entering into arrangements and on an ongoing basis.

Issue:

Due diligence processes are often integrated into broader business initiatives, and over-specification could reduce flexibility.

Specifically relating to para 37, point 5 of the consultation document, UK Finance request clarity on what is meant by “complaints” and “investigations” in practical terms. We request recognition of proportionality, as not all complaints will be relevant nor will TPSPs be willing or contractually obliged to disclose them. Any requirement to examine all complaints would be overly onerous and unnecessary.

Recommendation:

- **Maintain High-Level Principles:** UK Finance recommends that the BCBS keep the guidance at a high level to allow institutions flexibility in integrating due diligence within existing governance frameworks.
- **Acknowledge Embedded Processes:** Recognise that due diligence may be part of sourcing strategies and change management programs.
- **Complaints and investigations:** Amendment of current wording to: *“Relevant, (whether recent or pending) complaints or investigations…”* leaving the determination of what is relevant to the bank.

Contracting and Monitoring

Principle 5: Contracting

Current Principle: Banks should ensure that contracts governing TPSP arrangements are clear, written, and enforceable.

Issue:

While we agree with the importance of clear and enforceable contracts, the Principles should acknowledge that negotiation power with TPSPs, especially large or systemic ones, may be limited.

Recommendation:

- **Recognise Practical Limitations:** Acknowledge that banks may not always be able to negotiate all desired terms, particularly with critical or systemic TPSPs, and may accept the attendant risk if it is within the bank's risk appetite.

Principle 6: Ongoing Monitoring

Current Principle: Banks should regularly monitor and assess the performance and risk profile of TPSPs.

Issue:

The requirement to maintain a register of all TPSP arrangements, including nth parties, could lead to an overwhelming administrative burden.

Recommendation:

- **Focus on Key Nth Parties:** Specify that registers should include only "key nth parties" that materially support critical services or have access to sensitive information.
- **Apply Risk-Based Approach:** Encourage banks to use materiality and proportionality principles in subcontractor oversight.

Additional Comments:

- Banks should use the information in the registers to map dependencies and interconnections related to arrangements, particularly those associated with high inherent risks or deemed critical services.
- We strongly call upon the Basel Committee to recognise the substantial administrative and operational burdens that the current and proposed reporting requirements impose on banks. The obligation to maintain exhaustive registers of TPSP arrangements, including detailed information on nth parties, demands significant resources, both in terms of personnel and technological infrastructure. This requirement not only diverts critical resources away from proactive risk management activities but also introduces complexities that can hinder a bank's ability to respond swiftly to emerging risks.

The lack of standardized register formats and objectives across different jurisdictions exacerbates these challenges. Banks operating internationally are often confronted with a patchwork of reporting requirements, each with its own unique specifications and expectations. This fragmentation leads to duplicative efforts, inefficiencies, and the potential for inconsistencies . Such disparities can undermine the very objectives of third-party risk management by overwhelming both banks and supervisors with data that may not be directly relevant to assessing and mitigating risks, either at the bank or system level. UK Finance support common approaches and requirements for register formats where appropriate.

Principle 7: Confidentiality and Security of Information

Current Principle: Banks should ensure that TPSPs protect confidential and sensitive information.

Issue:

The Principles should recognise that unless contractually agreed in advance, TPSPs may not provide certain assurances or allow specific controls.

UK Finance seek acknowledgement of proportionality, and proportional language, (specifically as it relates to para 48) as only relevant TPSPs and TPSP arrangements should be reviewed when there are changes to the TPSP, or the external or internal bank environment.

Recommendation:

- **Acknowledge Contractual Limitations:** Clarify that banks should make best efforts to ensure confidentiality and security through contractual agreements.
- **Proportional Language:** UK Finance requests the wording to be amended to the para 48:

> *"All TPSP arrangements should be reviewed and assessed on a regular basis and relevant TPSP arrangements should be reviewed whenever there are major changes in a bank's internal environment (e.g. organisation, conflict of interest etc), the TPSP (e.g. organisation, location of services, introduction of new or advanced technologies) or the external environment (e.g. political, economic, social, legal and financial landscape, any potential impediments to the delivery of activities). Critical TPSP arrangements should be assessed more frequently."*

Business Continuity and Termination

Principle 8: Business Continuity and Contingency Plans

Current Principle: Banks should integrate TPSP dependencies into their business continuity and contingency planning.

Issue:

While integrating TPSP dependencies is important, practical limitations exist where joint testing with TPSPs is not feasible unless contractually agreed upon.

Recommendation:

- **Acknowledge Practical Limitations:** Recognise that unless contractually agreed, TPSPs may not participate in joint testing, and banks should make best efforts within these constraints.

Principle 9: Termination

Current Principle: Banks should have exit strategies and termination plans for TPSP arrangements.

Issue:

To minimise the possibility of confusion, the concepts of “plans”, “strategies” for "planned" and "unplanned", “stressed” and “unstressed” exits and TPSP termination scenarios needs further clarification by the BCBS. UK Finance request the BCBS to use descriptive examples when utilising these terms in their final text.

While UK Finance accept the BCBS’s inclusion of intragroup arrangements within their definition of TPSP arrangement however, we determine that policies such as operational resilience and operational continuity may mitigate the impact and disruption caused as result of a stressed exit scenarios when it is involving an intragroup arrangement.

Recommendation:

- **Provide Descriptive Language:** Offer additional context and examples to differentiate between planned (i.e. anticipated or intentional) and unplanned (i.e. unexpected or sudden) exits.
- **Distinguish Exit Plan vs. Exit Strategy:** Further describe the overall approach to be taken to an exit plan for a planned exit and an exit strategy for unplanned exit
- **Exit planning for Intragroup arrangements:** UK Finance would like the BCBS to specify a proportionate, risk-based approach to the expectation to maintain stressed exit plans when related to intragroup arrangements.

+ Additional Comments:

- UK Finance would welcome further collaboration with the BCBS to develop a common understanding of the scope of planned and unplanned terminations.

Principle 10: Group-Wide and Cross-Border Considerations

Current Principle: Banks should manage third-party risks across the group and consider cross-border implications.

Issue:

No specific feedback at this time.

Principle 11: Supervisory Oversight

Current Principle: Supervisors should review banks' TPRM frameworks and require improvements where necessary.

Issue:

To effectively manage systemic risks, coordination is needed to prevent duplicative efforts and conflicting requirements across jurisdictions.

Recommendation:

- **Harmonise Regulatory Requirements:** Promote alignment of regulatory requirements and reporting formats to facilitate compliance and reduce the burden on global institutions.
- **Clarify Roles:** Distinguish between supervisory oversight of systemic risks and banks' management of entity-level risks.

Additional Comments:

- UK Finance would welcome supervisors sharing aggregated or anonymised data on systemic concentration risks to better understand and manage these risks.

Principle 12: Supervisory Cooperation

Current Principle: Supervisors should cooperate and coordinate to manage third-party risks that span multiple jurisdictions.

Issue:

International regulatory cooperation is essential, but there should also be recognition of home regulator engagement to prevent overlapping regulations.

Recommendation:

- **Foster International Dialogue:** Support initiatives enhancing cross-border resilience through information sharing and coordinated responses.
- **Encourage Deference to Home Regulators:** Where appropriate, regulators should seek to coordinate with the firm’s home regulator on enterprise-wide third-party risks.

Additional Comments:

- We welcome the intention of Principle 12. Regulatory cooperation is important to avoid diverging standards or duplicative requirements. In particular, alignment on the specific format of reporting would be a valuable outcome.

Definitions

“Critical Services”

Issue:

The Principles define "critical service" as "a service provided to a bank, the failure or disruption of which could significantly impair a bank’s viability, critical operations, or ability to meet legal and regulatory compliance obligations." Including "ability to meet legal and regulatory compliance obligations" expands the scope beyond what is covered in the BCBS POR.

Detail:

The BCBS POR defines operational resilience as the ability to deliver critical operations through disruption. Critical operations are defined as critical functions and the activities, processes, services, and supporting assets whose *disruption would be material to the continued operation of the bank or its role in the financial system.*

The Principles define ‘**critical service**’ as ‘*a service provided to a bank, the failure or disruption of which could significantly impair a bank’s viability, critical operations, or ability to meet legal and regulatory compliance obligations*’. The inclusion of the ‘legal and regulatory compliance obligations’ criteria, whilst necessary for consideration as one of the risks that banks consider when assessing TPSP arrangements, will inappropriately expand the scope of what is considered ‘critical’ beyond what is covered in the BCBS POR. Failure to comply with legal and regulatory compliance obligations will rarely, if ever, case a disruption that would materially impact a bank’s continued operation or its role in the financial system. Its inclusion means that an expansive scope of services would be captured by this definition, including services that are not critical from a resilience perspective, and significantly expand the scope of banks’ operational resilience programs.

Whilst recognizing that some jurisdictions already have similar requirements, we recommend that the BCBS definition of ‘critical service’ is revised as follows in order to remain practical and effective, and to ensure it remains aligned to the BSBC POR in its intended objective and focus on significant impairment to a bank’s viability or critical operations:

Recommendation:

- **Refine the Definition:** Revise the definition to focus on resilience risk and impacts.

Suggested Revision:

"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 its ability to meet legal and regulatory compliance obligations such that failure to meet those obligations could significantly impair the bank's viability or critical operations."

“Critical TPSP Arrangement”

Issue:

The definition of "critical TPSP arrangement" is unnecessary and may cause confusion.

Detail:

The Principles define a ‘**critical TPSP arrangement**’ as ‘*a TPSP arrangement which supports or impacts one or more critical services provided to a bank*.’ This definition is unnecessary and risks additional confusion surrounding the classification of third-party services that are assessed as ‘critical’ and how it differs from ‘critical services’ and related definitions in the Principles. Banks assess the risks associated with each third-party arrangement, including as to whether those arrangements are critical to a bank’s resilience reasons, irrespective of how they are captured in framework agreements or contracts that may apply to more than one contracted third-party service. We therefore recommend that the BCBS removes this definition and leverages the ‘critical services’ definition (as amended above), ensuring it is applied consistently and appropriately throughout.

Recommendation:

- **Remove the Definition:** Eliminate this definition and consistently apply the refined "critical service" definition throughout the Principles.

“Key Nth Party”

Issue:

The current definition does not differentiate between service providers based on their actual impact on critical services.

Detail:

The definition of ‘**key nth party**’ should also be amended to more appropriately apply a risk-based approach. The current language does not differentiate between service providers which are linked in any way to a critical service, without considering the actual role they play in service delivery and therefore the potential impact if they were disrupted. To better reflect the importance of a service provider to the critical service, the definition should be amended.

Recommendation:

- **Amend the Definition:** Focus on service providers that materially support critical services or have access to sensitive information.

Suggested Revision:

"Key nth party: A service provider that is part of a TPSP's supply chain and materially supports the ultimate delivery of a critical service by a TPSP to a bank or has the ability to access sensitive or confidential bank information (e.g., consumer data)."

"Concentration Risk"

Issue:

The definition references "critical operations," which should be consistent with the term "critical services" used elsewhere.

Detail:

The definition of '**concentration risk**' references "critical operations". A citation should be included referencing the definition of critical operations in the BCBS POR. Further, we note that the reference to critical operations is not consistent with the use of the critical services term used elsewhere in the draft principles. As noted above in connection with the definition of critical TPSP arrangements, we are concerned that a proliferating list of different definitions for the concept of 'criticality' creates confusion amongst market participants and financial authorities and will challenge banks' ability to maintain a single internal framework.

Additionally, the reference in example (ii) to the "*concentration of services from one or multiple TPSPs in a single geographic region*" should be nuanced. A single geographic region meaning a single legal/political jurisdiction may create risk related to policy/law. However, a single legal geographic region could still be physically larger than several other legal geographies combined, meaning it is exposed to less physical risk from e.g. fire, flooding, severe drought or pandemic.

Recommendation:

- **Ensure Consistency:** Use consistent terminology and include citations referencing definitions in the BCBS POR.

Additional Comments:

- The reference to the concentration of services in a single geographic region should consider nuances. A single legal jurisdiction may be less exposed to certain physical risks despite being a single region.

“Systemic third-party dependency”

Issue:

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.[1]

Recommendation:

UK Finance request 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:

> “**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.”[2]

---

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

[2] Financial authorities in some jurisdictions may use a different term in a similar context, taking into account the different approaches used in the jurisdictions . + See footnote 13 on page 6 of the FSB TPRM Toolkit which also references certain related sections of the FSB TPRM Toolkit.

Summary and Conclusion

We support the Basel Committee's initiative to enhance the sound management of third-party risk. By refining certain definitions, clarifying roles and responsibilities, and promoting international regulatory alignment, the Principles can more effectively guide banks in managing third-party risks holistically. We appreciate the opportunity to provide feedback and look forward to continued dialogue on this important topic.