EBF Comments on the BCBS Consultative Document on Principles for the sound management of third party risk

General Remarks

In general, we appreciate the BCBS establishing harmonised principles on third-party risk management. However, we would like to underscore that in the EU context, there are already provisions on third parties, namely under the Digital Operational Resilience Act (DORA). Our position is therefore that it is desirable that the principles that will be defined by the BCBS do not exceed what already exists in the EU.

These principles are not intended to add further regulatory requirements to existing legislative frameworks the banks already operate under. Adherence to the principles must always happen in accordance with existing and future legislative frameworks and must not infringe these frameworks.

The objective of the proposed Principles is to guide firms in the holistic management of third-party risk, including but extending beyond incorporating resilience objectives and consideration from the BCBS Principles for Operational Resilience (POR) and the Sound Management of Operational Risk (PSMOR).

Effective management of third-party risk is crucial for a bank's operational resilience. Within this framework, certain third-party arrangements should be considered 'critical' due to their potential resilience impact and should be subject to certain enhanced controls and oversight to mitigate *resilience* risks effectively. However, the following two overarching issues appear to undermine this intended approach:

i. Firstly, the Principles adopt an overly broad definition of what constitutes 'critical,' which could lead to the allocation of limited bank resources to third-party arrangements that do not pose a genuine threat to a bank's resilience.

ii. Secondly, the Principles place a disproportionate emphasis on operational resilience risk, often neglecting broader risk management concerns that banks should consider when managing third-party risk and tailoring its controls and oversight accordingly.

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

Third-party risk management (TPRM) frameworks are designed to address various risks, including data and security risks, regulatory compliance, financial viability, and reputational risks. Principle three, particularly paragraph 30, underscores this by stating that banks should consider all types of risks associated with third-party service provider (TPSP) arrangements. The outcome of such a risk assessment will lead to a risk rating for the third-party, which will then dictate the level of oversight and specific controls required. This reflects a holistic and risk-based approach fundamental to TPRM.

The potential impact of a third-party outage on a bank's critical operations, as defined by the BCBS POR, is therefore just one of many risks that banks should assess alongside a broader set of risks and risk ratings as part of a bank's holistic risk assessment of third-party arrangements. Given the potential impact a bank's viability and operations, these arrangements will require specific resilience controls and oversight tailored to address resilience risk. It is important to note that there are also third-party arrangements which may not pose a resilience risk to a bank, but may still require enhanced oversight and specific controls due to a range of other risk drivers and ratings.

The integration of operational resilience into broader TPRM frameworks should therefore not overlook the full range of risk drivers that determine a third-party's risk rating. Yet the draft Principles seem to merge differing considerations and impacts related to operational resilience scoping and broader third-party risk oversight. The impact of this is that resilience concepts like 'criticality' become conflated with other risk considerations, although the objectives, risk drivers and impacts between TPRM and operational resilience differ. Consequently, the Principles prescribe controls that may not align with the actual risk posed by the third-party, i.e., applying resilience-related controls to third-party arrangements that do not present resilience risk.

To address these issues, we recommend the BCBS make the following changes to the Principles:

- Clarify its intention to provide standalone guidance on holistic TPRM approaches, including the risk-based methodology described above, of which operational resilience is just one of many risks considered.
- Acknowledge the holistic risk assessment that covers the full range of risks presented by a third-party arrangement, assigns a risk rating or categorization, and tailors the necessary oversight fundamental to the risk-based approach that underpins banks' third-party risk management programs.
- Explicitly state that the term 'critical' is narrowly focused on resilience considerations, aligned with the definition of critical operations in the BCBS POR. Additionally, the BCBS should amend the definition of 'critical service' in the Principles to better reflect the term's narrow focus on resilience risk and impacts (discussed further 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 (amendments to address this are suggested below).

Finally, there is a need to create a unique certification framework to be adopted by all TPSPs, leveraging third-party accredited institutes recognized by supervisors. This will help streamline and consolidate the monitoring and control activities that financial institutions are responsible for, minimizing the impact on both providers and applicant banks.

Specific Comments

Definitions

'Third-party service provider'
The definition of third-party service provider is too broad and will cover any type of service providers e.g. catering, cleaning, etc that wont materially impact the banks function and are easily replaceable. This scope is too broad, the definition should be limited to TPSP arrangements relevant to the operation of the bank. Therefore, there is a need to introduce the concept of "relevance" in order to not considered everything which is simply and indiscriminately" in support" as critical.

'Critical services'
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:

> "Critical service: A service provided to a bank, the failure or disruption of which could significantly impair a bank's viability, critical operations, or

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

'Critical TPSP arrangement'

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.
If a categorisation as a 'critical' TPSP arrangement and the associated application of extended requirements was to be retained, at least a certain materiality should be given. Please clarify this by amending the definition as follows:

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

'Key nth party'

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 as follows:

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

'Concentration risk'

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.

Section 11
Also ,the principles should take unto consideration existing definitions that are in place, in the case of EU regarding DORA and EBA Guidelines so that they can allow for equivalence with those, and therefore entities which are subject of these frameworks can be regarded as already compliant with the principles.

Section 15
It lists the requirements for IGAs including the need of Business Continuity Management (BCPs) and exit strategies etc. Proportionality should be allowed in certain IGA arrangements.

Principles 1, 2

Section 16, 17
The paper as drafted assumes a governance model based around a board of directors. This may not be the case for all parts of a business globally. The Principles should instead looks to whatever the most senior governance forum is in a given jurisdiction, rather than focusing specifically on boards.

As currently drafted, Principle 1 seems to suggest that the Board is expected to provide governance and oversight of TSPS arrangements directly. We understand this is likely not the BCBS's intention, in which case Principle 1 should be clarified to reflect the board's proper role as follows:

- Principle 1: 'The ~~board of directors~~ ***most senior governance forum*** 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'.

Boards are accountable for ensuring an appropriate third-party risk management framework is in place and for providing strategic oversight for the overall risk management strategy. The board should oversee the establishment of the overall strategy, framework, and policies. However, holding the Board accountable for ensuring implementation of these policies and processes—as suggested in Principle 2—does not reflect its proper role and would undermine the

effectiveness of banks' governance and risk management. Principle 2 should therefore be amended as follows.

- Principle 2: 'The ~~board of directors~~ ***most senior governance forum*** 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'.

Additionally, the application of Principle 2 in a group context is unclear, particularly when centralised management of critical TPSP arrangements could potentially conflict with the boards responsibilities outlined in this principle.

These amendments will clarify the role of the board and senior management and appropriately reflect established principles of effective corporate governance and risk management.

Section 17
The Principles should allow firms flexibility to rely on a global model and assessment of concentration risk or materiality rather than being required to do individual assessments per branch or jurisdiction. Where a branch assessment is required by a local regulator then the question of using the most senior governance forum arises (as above) but the aim should be to leverage global assessments over local where possible.

Risk management

Section 21
In this paragraph, it should be clarified whether (i) risk identification and assessment; (ii) monitoring and reporting; and (iii) application of Controls could be performed using a risk based approach or a criticality based approach across all three lines of defence.

Section 22
The reference in **paragraph 22** to maintaining a register of all TPSP arrangements and "*nth parties, as appropriate to the criticality of the service and associated risks*" does not sufficiently reflect a risk-based approach. To ensure an appropriate supply chain scope captured and reported in registers, we recommend that the BCBS specifies that only "***key*** *nth parties"* are captured in registers.

Additionally, we recommend the following be amended to clarify the correct use and application of terms such as "arrangements" and "critical services":

> "Banks should use the information in the registers to map dependencies and interconnections related to arrangements, particularly those associated with **high risk inherent risks and/or** ~~higher risks and~~ those **deemed to be** ~~supporting~~ critical services.

Finally, given the development of reporting requirements in various jurisdictions resulting in expansive and divergent expectations on nature of information required and format of this information, we would encourage and support the inclusion of a Principle for supervisors aimed at emphasising and ensuring data minimization and alignment of register formats and objectives as far as reasonably practicable. The collection and maintenance of information submitted in third-party registers is often manual and resource intensive and banks are currently already diverting important resources to administrative tasks in order to meet existing register requirements. This should not be necessary given the commonality of register objectives across jurisdictions. A Principle which ensures data requested is minimized to information necessary and proportionate to achieve register objectives would lessen the reporting burden on banks and would ensure effective and interoperable reporting to financial authorities.

Section 23
Principle 2 notes the importance of assessing concentration risk. Firms already have in place robust policies regarding concentration risk assessment including definitions of concentration risk appetite, tolerance definitions and senior management oversight. Firms also monitor processes including through annual reviews of the assessment approach. Recommendations regarding concentration risk assessments should avoid being overly prescriptive and enable firms to take advantage of well-established global processes that are subject to supervisory review as-is. It is suggested to adopt a proportional, risk based approach, where concentration risk is assessed only for critical or high risk TPSP and their subcontractors

Section 24
The Principles imply that a single strategy needs to be maintained at Group-level on third-party risk. Clarity would be welcomed here as to whether this does in fact need to be a single, separate document. Firms often leverage a number of global frameworks which collectively meet regulatory requirements. A single global policy could lead to overlap of existing frameworks.
Additionally, there are local regulatory nuances that firms would apply to risk assessments that may differ to Group-level assessments, and this also feeds into the difficulty of maintaining a single strategy.

Principle 3
Section 29
Banks should assess the potential impacts of entering into any TPSP arrangement on their operations (e.g. activities, functions, systems, data), including the criticality of the operations, considering risks and assessment results. It will be disproportionate to assess impact on all TPSP arrangements.

Principle 4
There is a need to refine the suggested methodological approach regarding the execution of due diligence to ensure its actual applicability, considering practical limitations due to limited pre-contractual information.

Principle 5

It is suggested to also take into account existing frameworks in different jurisdictions, such as the DORA provisions on key contractual provisions, so that equivalence is allowed and entities already subjected to such provisions can be considered as also following this principle.

Section 41

For the point 'obligations and responsibilities relating to security, resilience and other technical configurations' – the target should be critical TPSP arrangements and not all arrangements.

Section 42

The principles on contracting include requirements regarding key nth parties. These can hardly be fulfilled in practice, as banks often do not have direct contractual relationships with nth parties. Thus, they should be dropped. This has to be applied case-by-case as it may not be possible at all times.

Section 45

It is recommended to adopt a proportional, risk based approach, when mapping interconnections or dependencies.

Principle 7

Section 49

Outlined that firms will need to monitor all agreements for performance-related metrics. Again, it will be disproportionate to risk to implement these requirements for all contracts. A risk-based approach is needed.

Section 54

Reporting: The principles should elaborate and exemplify on different types of assurance regarding the statement "...they should use multiple forms of assurance and not rely solely on one".

Principle 9

We support the inclusion of an overarching principle of proportionality instead of grading the specific principles in a detailed manner. However, with regard to the principles on termination, more differentiation is needed. Generally requiring individual exit plans for each and every TPSP and adding additional requirements on exit plans for critical TPSPs is inappropriate. For the sake of risk-adequacy and efficiency, we suggest limiting the requirement to have exit plans to critical TPSPs in the first place.

Principle 9 should offer clear guidance, particularly on the distinction between planned and unplanned scenarios and how these should be addressed in exit plans.

Section 63

Clarification is needed on what is meant by testing'. It is not certain that this is realistic, and it is not clear what kind of tests are meant by this. Testing an exit plan, for instance under the EBA GL, is very challenging. Would the testing be done with the provider? Is it taken into account in the contractual provisions?

Principle 12

Section 71

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.

As alluded to in points 17 and 24 above, it should be emphasised that while regulatory cooperation is positive, regulators should also work towards a level of deference to home regulator engagement on enterprise-wide third-party risks – with regulators cooperating with each other.

Graph 1: Third-party life cycle

The graph could be expanded to include and connect with the wider Enterprise risk management framework as described in paragraph 16.