THE BANKING ASSOCIATION SOUTH AFRICA

Rosebank Link, 6th Floor
173 Oxford Road, Rosebank 2196
Tel +27 11 645 6700
www.banking.org.za

8 October 2024

Secretariat of the Basel Committee
on Banking Supervision
Bank for International Settlements
CH-4002 Basel
Switzerland

Our ref: 107411

Your ref:

Direct (071) 472 1250

E-mail: StephenL@banking.org.za

Dear Sir / Madam

Comments on the Principles for the Sound Management of Third-Party Risk

We thank you for allowing our members the opportunity to comment on matters relating to the Principles for the Sound Management of Third-Party Risk.

We have captured the South African banking industry's response as contained in the attached Annexure A.

We look forward to your consideration and any further engagement on the issues raised by our member banks.

Sincerely

DocuSigned by:
2A4C8CD2AD4A461...

Stephen Letsoenya
General Manager – Prudential

Registration Number : 1992/001350/08 A non-profit company under the Companies Act, No 71 of 2008
Directors : M Vilakazi (Chair), A Rautenbach (Deputy), BP Kunene (Managing Director), KG Bungane, GM Fourie, L Fuzile, HD Kallner, CJ Moodliar, JP Quinn, PW Taylor, C Zhang *(Chinese)*,
Company Secretary : AV Skosana

THE BANKING ASSOCIATION SOUTH AFRICA

Rosebank Link, 6th Floor
173 Oxford Road, Rosebank 2196
Tel +27 11 645 6700
www.banking.org.za

ANNEXURE A

NAME OF PERSON COMPILING SUBMISSION: **Stephen Letsoenya**

ORGANISATION: **The Banking Association South Africa**

SUBMISSION DESCRIPTION **BCBS Consultation on the Principles for the sound management of third-party risk**

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT	ADDITIONAL COMMENT
	Definitions			
1.	Third-party service provider (TPSP): An entity or individual which performs services, activities, functions, processes or tasks directly for a bank.			• It should specifically state that subcontractors and nth parties are excluded from this definition
2.	The term TPSP arrangement includes arrangements for the provision of services to a bank by an intragroup service provider	Intragroup arrangements do not pose the same level of risk as external TP arrangements, as ultimate management oversight of intragroup arrangements lies within an organisation. Intragroup arrangements should not be subject to the same requirements as stipulated in the Principles.	Distinction between intragroup and external third parties.	

Registration Number : 1992/001350/08 A non-profit company under the Companies Act, No 71 of 2008
Directors : M Vilakazi (Chair), A Rautenbach (Deputy), BP Kunene (Managing Director), KG Bungane, GM Fourie, L Fuzile, HD Kallner, CJ Moodliar, JP Quinn, PW Taylor, C Zhang *(Chinese)*,
Company Secretary : AV Skosana

3.	Third party service provider arrangement and concentration risk:	The definitions include and exclude nth parties. Clarity is needed regarding the requirements for nth parties. Also, under concentration risk- A firm would have to do assessments to understand nth parties to understand concentration risk. Up to how many levels would be sufficient e.g. 4^{th}, 5^{th}, n^{th} parties?	Clarity on the definition of third-party service provider arrangements, including types of third parties that are included and excluded in these principles. Clarity on the requirements specific to nth parties as well as critical nth parties.	
4.	Third party service provider arrangement	It is noted that FMIs are specifically excluded. However, disruption at an FMI can have a systemic impact. What is the proposed risk management treatment of FMIs.	Clarity on the risk treatment for FMIs is required.	
5.	TPSP arrangement: A formal arrangement between the bank and a TPSP for the provision of one of more services, activities, functions, processes, or tasks to a bank (which includes but is not limited to "outsourcing").	Does formal imply that only written agreement should be in place	Relationship means an agreement, arrangement, engagement and/or connection between a Third-Party and a SBG entity, irrespective of (i) the length of time for which such agreement, arrangement, engagement and/or connection exists, (ii) whether reduced to writing or not and (iii) whether for purposes of concluding a transaction or otherwise.	

6.	Critical TPSP arrangement: A TPSP arrangement which supports or impacts one or more critical services provided to the bank.	The definition is slightly ambiguous. A critical arrangement is a service, therefore is this not reiterating the critical service definition		
7.	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 regulatory compliance obligations	Reputational risk should be included in the definition	Critical Service: A service provided to a bank, the failure or disruption of which could significantly **impact banks reputation**, impair a bank's viability, critical operations, or ability to meet regulatory compliance obligations.	
8.	Definitions (11)	• TPSP is underpinned by critical services. There should be an expansion on the definition, to include critical systems and critical operations. • TPSP arrangement should be explicit on the use of words such as vendor management and outsourcing arrangement. Are they used interchangeably, or do they mean differently?		
9.	Definitions (11)	***Critical service:*** *A service provided to a bank, the failure or disruption of which could significantly impair a bank's viability, critical operations,*	A service provided to a bank, the failure or disruption of which could significantly impair a bank's viability, critical operations, systems, or ability to manage risk,	

		or ability to meet legal and regulatory compliance obligations. • Critical Service needs to consider not only Operations, but **Systems.** • Also, the impact needs to include FI's ability to manage **Risk.**	meet legal and regulatory compliance obligations.	
10.	Definitions	Consider adopting a more comprehensive definition of Intragroup TPSP.	Any internal entity, individual or function within a bank that provides specific services, products, or performs activities, to support business operations.	
11.	Definitions	Consider adopting a more comprehensive definition of Supply chain.	An entire network of entities, resources, activities, and technologies that provide infrastructure, physical goods, services, and other inputs directly or indirectly utilised for the delivery of a service to the financial services industry, organisation, and/or client, limited to the services agreed upon.	

12.	Definitions	Consider adopting a brief definition of TP concentration risk.	Third-party concentration risk refers to the potential risk that arises when the business relies heavily on a single third-party service provider or a small group of providers for critical services or products. This lack of diversification can lead to significant vulnerabilities if any of these providers fail or experience disruptions.	Additionally, concentration risk may arise from the following factors: • **Usage:** The extent to which the organisation utilises their services throughout the business. • **Spend:** The amount of money an organisation allocates to a third party. • **Reverse concentration:** The ratio of an organisation's expenditure to the total revenue of the third party.
	Third-party risk management principles			
13.	Graph 1: Third-party life cycle	Suggest that Strategy be on the outer circle, as this is the overarching element.	Suggest that Strategy be on the outer circle, as this is the overarching element.	
14.	Graph 1: Third-party life cycle	Third-party life cycle suggested updates: Start with a Planning phase before Risk Assessments.	The first phase could relate to 'Planning / Strategy' i.e. involves identifying the business needs, objectives, and risks of outsourcing a service or function to a third party. It also involves defining the scope, requirements, and expectations of	

			the service, as well as the roles and responsibilities of both parties.	
15.	Graph 1: Third-party life cycle	The stages seem to exclude the process of: • identifying the needs of the Bank, • identifying potential third parties • selecting appropriate third parties prior to conducting risk assessment, etc. and could also include renewal process as well.	The stages of the life cycle typically include needs analysis, identifying and selection, before the following activities, risk assessment, due diligence, contracting, onboarding, and ongoing monitoring renewal or termination.	
	Governance, risk management and strategy			
16.	Principle 1	Caution on "*The board of directors has ultimate responsibility for the oversight of all TPSP arrangements"* – The principle can emphasise criticality as opposed to all.	"*The board of directors has ultimate responsibility for the oversight of TPSP involved in* ***Critical Service*** *arrangements*	
17.	19. There are certain arrangements with TPSPs which entail "shared responsibility" between the bank and the TPSP (e.g. cloud services).	All arrangements involve Shared responsibility.	Provide clarity on which arrangements do not involve shared responsibility.	
18.	Pg 7 of 21 Third-party service provider (TPSP): An entity or individual which performs	What about Banking as a Service (Alliance Banking) where third parties may provide services to a		

	services, activities, functions, processes, or tasks directly for a bank.	bank and vice versa as part of a Banking as a Service, these relationships have a strong third-party element and introduce significant risk to a bank. However, it is not clear whether these type of third parties are included in the definition.		
19.	Governance (18)	*"Based on risk and complexity, banks may establish a central function to monitor all TPSP arrangements. "* The size of the bank also matters the bigger the bank the bigger the operations and potentially bigger reliance on service providers.	*"Based on their size, complexity and risk landscape, banks may establish a central function to monitor all TPSP arrangements. "*	
20.	Governance (19)	*"There are certain arrangements with TPSPs which entail "shared responsibility" between the bank and the TPSP (e.g. cloud services)."* *Is there an expectation for Banks to define responsibilities of these TPSPSs or can Regulators/Supervisors set these R&R? Alternatively, is the thinking that Banks are meant to outline these via contracts/MSA they sign?*		
	Risk Assessment			

21.	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"* – This principle needs to emphasise comprehensive risk here considers both areas that need to be assessed: **Service** (e.g. Cyber/Privacy/Legal/Operational) and **Relationship (**e.g. Reputation/association/sanction/EGR) related risks.	*…." under the TPRMF to evaluate and manage identified and potential risks that may arise as a consequence of the relationship and the service involved.,"*	
22.	Risk Management (22)	"Banks should maintain a complete and up-to-date register of all TPSP arrangements (and nth parties, as appropriate to the criticality of the service and associated risks)" Emphasis on **'Key Nth'** parties only on the registers, these have a greater impact to operations and data.	"Banks should maintain a complete and up-to-date register of all TPSP arrangements (and Key nth parties, as appropriate to the criticality of the service and associated risks)"	• Agreed for key nth parties, however, should note this Information is not always available or disclosed by TPSP, irrespective of criticality
23.	Risk Management (30)	"They should consider all types of risks related to TPSP arrangements, including but not limited to strategic risk, reputational risk, compliance risk, operational risk (e.g. information and	"They should consider all types of risks related to TPSP arrangements, including but not limited to strategic risk, reputational risk, compliance risk, step-in risk, operational risk (e.g. information	

		communication technologies (ICT), cyber), concentration risk and the risk stemming from a long supply chain." Consider 'Step-In Risk' from OCIR expectations, where a Bank might find it beneficial to save a **Critical Service TPSP** or a **Key Nth Party** to avoid a larger and much expensive impact.	and communication technologies (ICT), cyber), concentration risk and the risk stemming from a long supply chain."	
	Due diligence			
24.	Principle 4: Banks should conduct appropriate due diligence on a prospective TPSP prior to entering into an arrangement.	Will any guidance be provided on "appropriate due diligence"?	Will FSP's be left to adopt a risk-based approach or define the criteria to ensure appropriate due diligence is conducted?	
25.	33. Due Diligence Banks should **also** perform due diligence to evaluate whether they would be able to appropriately identify, monitor and manage risks associated with the specific arrangement with a prospective TPS	What does this mean compared to the due diligence that should be done? Does this entail something different and if yes, what is required.	Clarity regarding due diligence requirements.	

26.	Risks As part of the assessment of known and potential risks associated with the TPSP arrangement, banks should consider: • potential conflicts of interest (including those from intragroup and nth parties);	Please provide an example of what would constitute a potential conflict of interest for intragroup arrangements.		• Define the Conflict of interest for Intragroup. • Define the conflict of interest for nth party.
27.	Due diligence	Due diligence as a term for Banks may mean a lot of things. The document could include Due diligence definition to create understanding within Banks and across industry and geographies.		
28.	Due diligence (37)	To achieve comprehensive assessments, Supervisors ought to be required to periodically share **Industry view of concentration risk** to allow Banks to consider other players, this to limit and mitigate systemic shocks where possible.		
29.	Principle 4 Due Diligence	Criteria not clear before contracting any TPSP	Could be prescriptive not to deal with sanctioned entities.	
	Contracting			
30.	39. The *contracting* stage of the life cycle is when negotiations between a bank and a TPSP occur, and where terms	The use of service is too broad. Contracting can be for the delivery of goods or even for licensing.		

	and conditions of the delivery of services are agreed. Contract provisions should facilitate effective risk management and oversight and specify the expectations and obligations of both banks and TPSPs. The bank should negotiate a contract that meets its business goals and risk management needs.			
31.	41. rights for banks to receive accurate, comprehensive and timely information (including regarding incidents impacting the services they are receiving).	Include the right of remedy to non-delivery or ineffective performance of contractual duties impacting the service/function		
32.	41. Banks' contracts governing TPSP arrangements should consider: • Key performance benchmarks			Proposed wording for paragraph 41. Bullet point 1: • Key performance benchmarks and implications of breaches of obligations.
33.	42. Rights of supervisory authorities to access, audit and obtain relevant information from **key nth** parties as permitted under applicable laws and regulations within the respective jurisdictions or	This will have a massive implication, as Banks do not have direct relationships with nth parties. Implementation of this requirement will take years.	Reconsideration of contractual requirement for nth parties as the banks do not have direct relationships with these parties.	

	bi-/multilateral agreements amongst supervisors;			
34.	43. In exceptional cases where a legally binding contract does not exist, banks remain responsible for appropriate risk management and oversight of their TPSP arrangements as outlined in this document.	There are some third parties where it is challenging for banks to implement contracts. There is a case. to be made here for regulators to step in and assist with the due diligence E.G. FMIs.	Challenge in implement contracts across all third-party categories.	
35.	Principles for Sound Management of Third-Party Risk. P5 – Concentration:	The problem will be to identify the systemic importance of certain TPSP. Certain entities would be obvious, but there are many TPSP who could have a systemic impact, but will not disclose their customers due to contractual obligations etc. Limited information in the public domain. To what extend is the bank expected to mine the public domain for this type of data? It can be website, news etc. The information might be available but to what extend is the bank required to monitor the public domain. **Clarification needed:** The paragraph implies that it is prior to establishing the relationship, however the definition on P4	**Current Wording:** "it is important for banks to understand the relative systemic importance of a TPSP, **based on available information** (e.g. from the public domain, directly from the TPSP), so that they may consider the implications of entering into an arrangement with the TPSP." **The suggestion**: "based on **readily** available information."	

		implies that it is during the life cycle of the relationship with the entity.		
36.	42. Banks contracts governing critical TPSP – supervisory authorities to access	Supervisory access to data/information from a third party or nth party can only be accessed/obtained through the respective bank.	The wording must state banks involvement to provide the necessary information/data.	These rights are subject to applicable laws and regulations.
37.	43. Appropriate risk oversight & role of supervisors	Is there any impact or requirements to consider for operational risk capital calculation?	This is for the regulatory capital requirements.	Require further clarification
38.	Principle 5: Contracting	Perceived unfair practises over emerging SME in the context of supplier development in line with South Africa laws.	Firm could include special dispensation where necessary to support small TPSP without increased risk exposure.	Clarification on the perceived unfair practises
39.	Principle 5: Contracting	Upfront condition recommended to prevent bribery and corruption	Encourage employees are prohibited from conducting business directly or indirectly with firm, whether as directors of companies, members of a close corporation, a sole trader and/or independent contractor providing goods and services to the Group.	
	Onboarding and ongoing monitoring			
40.	Paragraph 45: Banks should keep an updated register of all TPSP	It should be clarified that a register can take different forms, e.g.	Clarify regarding register.	

	arrangements, reflecting any changes in criticality	service providers on a system can serve as a register. Also, the requirement should not be for a single register.		
41.	Paragraph 59: assurance that TPSPs develop and periodically review and update BCPs that set out clear and measurable RTOs and RPOs that support banks' tolerance for disruption (refer to paragraph 42); and • assurance testing (e.g. walkthroughs, tabletops, and simulations) that the TPSP's BCP methodologies are robust.	The level of audit and assurance expectations on third parties that is required, especially material relationships need to be carefully considered. This is practically difficult to execute with large third-party vendors/organisations.	Consideration of the level of assurance and testing required.	
42.	54. Banks may utilise the results of independent audits and other forms of assurance on the services contracted to TPSPs. **However, for critical services, they should use multiple forms of assurance and not rely solely on one.**	This has a huge implication. Clarity is needed regarding the multiple forms of assurance required.	Clarity is needed regarding the multiple forms of assurance required.	
43.	Principles for Sound Management of Third-Party Risk. P6 – Nth Parties	We can provide guidance and what we expect from the Third party to manage their nth parties.	**Current Wording:** Banks' risk assessment, due diligence, contracting and onboarding and ongoing monitoring processes should evaluate the TPSP's ability to manage its nth parties and meet equivalent contractual obligations	

			(e.g. level of service, risk management, compliance, operational resilience standards). **Suggestion:** Risk based approach; 'Bank should, where possible, provide the criteria and guidance and on the level of service, risk management, compliance and operational reliance standards.'	
	Ongoing Monitoring	Is there a requirement for how ongoing monitoring must be executed?	If there is no requirement then suggest that principles be expanded to allow banks to determine the way ongoing monitoring takes place.	
44.	Paragraph 55	Minimum period to reuse information when "break" in service occurs. E.g. same service a few months after contract expired. Can be seen as excessive repetition / barrier to do doing business.	When banks decide to renew a TPSP arrangement, they should leverage the information obtained from the *onboarding and ongoing monitoring* stage in performing *due diligence* prior to renewing the arrangement. The information should not be older than 12(x) months.	

	Termination			
45.	Principle 9: Banks should maintain exit plans for planned termination and exit strategies for unplanned termination of TPSP arrangements.	Noting that these are principles to ensure best practice, one would deem failure to comply as no contravention to law.	Reason is that in respect of terminations, there could be legal clauses that would bind both parties so failure to terminate must be considered with these clauses in mind. E.g. where an undesirable customer is exited from the Bank and they have a home loan, customer still has an obligation to pay back the home loan, noting no extension of credit or new products to be offered to this customer.	
46.	66. Unplanned terminations	Please define planned vs. unplanned terminations. How long before the exit the decision was taken would qualify as unplanned?	Clarity required on Planned vs unplanned terminations.	
47.	Principles for Sound Management of Third-Party Risk. P15 – Termination	It will not be practical to maintain exit plans for planned terminations for all Third-party service providers. The termination plan may also vary based on the point in the	**Current Wording: Principle 9:** Banks should maintain exit plans for planned termination and exit	

		relationship at which the parties terminate.	strategies for unplanned termination of TPSP arrangements. **Suggestion:** Risk based approach should be taken for developing and maintaining exit strategies for unplanned termination of TPSP – Critical TPSP with single supplier dependency. Banks should be able to initiate and determine a termination plan when the parties decide to terminate.		
	Role of supervisors				
48.	Principles 10-12:	The Banks require transparency regarding concentration on a TPSP. This is an important source of information.	**Suggestion on additional wording:** Supervisors should put measures in place to ensure the availability of the list of TPSP to the banks which pose a concentration risk.		
49.	Principle 12 Promoting collaboration	Systematic risk posed by TPSP used by all banks	Supervisor encouraged to facilitate collaboration between common critical TPSP's used by banks. This would assist with efficiency where each bank would want to engage common TPSP individually with similar requests.		

THE BANKING ASSOCIATION SOUTH AFRICA

Rosebank Link, 6th Floor
173 Oxford Road, Rosebank 2196
Tel +27 11 645 6700
www.banking.org.za

Registration Number : 1992/001350/08 A non-profit company under the Companies Act, No 71 of 2008
Directors : M Vilakazi (Chair), A Rautenbach (Deputy), BP Kunene (Managing Director), KG Bungane, GM Fourie, L Fuzile, HD Kallner, CJ Moodliar, JP Quinn, PW Taylor, C Zhang *(Chinese)*,
Company Secretary : AV Skosana