Basel Committee
on Banking Supervision

Consultative Document

Principles for the sound management of third-party risk

Issued for comment by 9 October 2024.

July 2024

BIS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-774-0 (online)

Contents

Principles for the sound management of third-party risk

I. Introduction

1. Banks have long relied on arrangements with third-party service providers (TPSPs) for reasons such as to access specialised expertise, reduce costs, improve scalability, efficiency and operational resilience, and focus on core activities. In the 2005 Joint Forum paper "Outsourcing in Financial Services"[1], the focus of supervisory authorities was on outsourcing, which is an important subset of banks' arrangements with TPSPs. Since the issuance of the Joint Forum paper, ongoing digitalisation has led to a rapid adoption of innovative approaches, which has increased banks' dependency on TPSPs for services that banks had not previously undertaken. This expansion of reliance on TPSPs requires an evolution of the traditional concept of outsourcing to the broader scope of TPSP arrangements.

2. The Basel Committee (the Committee) believes that appropriate risk management of banks' TPSP arrangements, supply chain (ie nth parties) and concentration risk arising therefrom can enhance banks' ability to withstand, adapt to and recover from operational disruption and thereby mitigate the impact of potentially severe disruptive events. Through the publication of this document, the Committee seeks to promote a principles-based approach to improving banks' operational risk management and operational resilience through effective third-party risk management (TPRM). The approach builds on the Principles for operational resilience (POR),[2] the revised Principles for the sound management of operational risk (PSMOR)[3] and other Committee publications[4] to reflect the life cycle of a TPSP arrangement, and draws from previously issued principles as well as TPSP initiatives undertaken by prudential supervisors and other international standard-setting bodies.

3. This document supersedes the 2005 Joint Forum paper in respect of the banking sector. While many of the principles set out in the Joint Forum paper remain relevant, the Committee has developed a new set of principles to reflect the evolution of a larger and more diverse TPSP environment in the banking sector. The document includes 12 high-level principles. Principles 1 through 9 provide banks with guidance on effective management of TPSP risks, while Principles 10 through 12 provide guidance for prudential supervisors. The Principles seek to achieve a balance in improving practices related to the management of third parties and providing a common baseline for banks and supervisors, while maintaining sufficient flexibility given the evolution of practices in this area.

4. The Principles focus on third-party risk management holistically and are technology-agnostic to keep pace with technological developments. They aim to promote international engagement, greater collaboration and consistency, with a view to reducing regulatory fragmentation and strengthening the overall operational resilience of the global banking system.

5. The Principles seek to accommodate a diverse range of bank risk management practices and approaches. They are intended to be applied on a proportionate basis depending on the size, complexity and risk profile of the bank as well as the nature and duration of the TPSP arrangements and their contribution to the delivery of critical services. The Principles are primarily directed to large internationally

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

[2] See Basel Committee on Banking Supervision, *Principles for operational resilience*, March 2021, www.bis.org/bcbs/publ/d516.htm.

[3] See Basel Committee on Banking Supervision, *Revisions to the principles for the sound management of operational risk,* March 2021, www.bis.org/bcbs/publ/d515.htm.

[4] See, for example, Basel Committee on Banking Supervision, *Newsletter on third- and fourth-party risk management and concentration risk*, March 2022, www.bis.org/publ/bcbs_nl28.htm.

active banks and their prudential supervisors in Basel Committee member jurisdictions. However, smaller banks, which may rely even more on TPSPs, and authorities in all jurisdictions can also benefit from these Principles.

6. The Committee welcomes feedback on all aspects of the proposals set out in this consultative document. Comments should be submitted by 9 October 2024. All comments will be published on the Bank for International Settlements website unless a respondent specifically requests confidential treatment.

II. Reference to other guidance

7. These Principles should be read in conjunction with other BCBS principles and guidance, including but not limited to the following:

- BCBS Core Principles for effective banking supervision (2024);[5]
- BCBS POR (2021);
- BCBS PSMOR (2021); and
- BCBS Corporate governance principles for banks (2015).[6]

8. These Principles also aim to complement work of other international standard-setting bodies which have released international guidance addressing TPRM in the financial sector, including but not limited to the following:

- Financial Stability Board (FSB) – Final report on enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities (2023);[7]
- International Association of Insurance Supervisors (IAIS) – Issues paper on insurance sector operational resilience (2023);[8]
- International Organization of Securities Commissions (IOSCO) – Principles on outsourcing (2021);[9] and
- Committee on Payments and Market Infrastructures (CPMI) and IOSCO – Principles for financial market infrastructures (2012).[10]

9. The Committee has designed these Principles to provide guidance to banks on TPRM. Financial institutions other than banks may find these Principles beneficial in addition to the international guidance applicable to their sector.

[5] See Basel Committee on Banking Supervision, *Core Principles for effective banking supervision,* April 2024, www.bis.org/bcbs/publ/d573.pdf.

[6] See Basel Committee on Banking Supervision, *Corporate governance principles for banks*, July 2015, www.bis.org/bcbs/publ/d328.htm.

[7] See Financial Stability Board, *Final report on enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities*, December 2023, www.fsb.org/wp-content/uploads/P041223-1.pdf.

[8] See International Association of Insurance Supervisors, *Issues paper on insurance sector operational resilience*, May 2023, www.iaisweb.org/uploads/2023/05/Issues-Paper-on-Insurance-Sector-Operational-Resilience.pdf.

[9] See International Organization of Securities Commissions, *Principles on outsourcing*, October 2021, www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf.

[10] See Committee on Payments and Market Infrastructures and IOSCO, *Principles for financial market infrastructures*, April 2012, www.bis.org/cpmi/publ/d101a.pdf.

10. While developing these Principles, it is noted that many jurisdictions have developed their own TPRM frameworks and standards, which are unique to each jurisdiction and are designed according to differing regulatory objectives and constraints.

III. Definitions

11. These Principles aim to make use of terms previously defined by the Committee and other international standard-setting bodies (refer to Section II above, *Reference to other guidance*) to the extent possible. Additionally, certain terms that are necessary and relevant from a banking perspective are specifically defined in this document. To ensure a common understanding, as well as clarity and consistency, definitions for terms used in this document are provided below.

- <u>Third-party service provider (TPSP)</u>: An entity or individual which performs services, activities, functions, processes or tasks directly for a bank.
- <u>TPSP arrangement</u>[11]: A formal arrangement between a bank and a TPSP for the provision of one or more services, activities, functions, processes or tasks to a bank (which includes but is not limited to "outsourcing").
  - The term TPSP arrangement includes arrangements for the provision of services to a bank by an intragroup service provider.
  - The term TPSP arrangement excludes financial services transactions between banks and their customers, employees or counterparties (eg taking deposits from or lending to consumers, providing insurance to policyholders, or provisioning to /receipt of services from financial market infrastructures (FMIs), such as clearing or settlement, to other banks), but includes services supporting these functions (eg compliance or back office activities relating to these transactions).
  - The term TPSP arrangement excludes arrangements between a TPSP and any party in the supply chain (ie an nth party to the bank).
- <u>Critical TPSP arrangement</u>: A TPSP arrangement which supports or impacts one or more critical services provided to a bank.
- <u>Critical service</u>:[12] A service provided to a bank, the failure or disruption of which could significantly impair a bank's viability, critical operations,[13] or ability to meet legal and regulatory compliance obligations.
- <u>Critical TPSP</u>: A TPSP that provides a critical service to a bank.
- <u>Intragroup TPSP</u>: A TPSP that is part of a banking group and provides services predominantly to entities within the same group. Intragroup TPSPs may include a bank's parent company, sister

11 The Principles exclude nth parties from "TPSP arrangement" and instead provide specific expectations for managing nth parties when necessary, given the lack of a direct relationship between banks and nth parties. This allows for a broader application to all TPSP arrangements and highlights the different risk management approaches for TPSPs compared with nth parties. Furthermore, it is worth noting that the Principles in this document could also provide value for other types of relationships that banks may have with third parties, including joint support for banking products.

12 Supervisors in some jurisdictions use terms such as "material services" and "important services" in a synonymous way. However, such concepts are often used to qualify services of a bank to its customers.

13 See definition in POR.

companies, subsidiaries, service companies or other entities that are under common ownership or control.[14]

- Supply chain: 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.
- Concentration risk:
  - Bank-level: Risk arising from a dependency of a bank on one or more services provided by a single TPSP (directly or indirectly through nth parties) or a limited number of TPSPs where the disruption or failure of such activities has potential implications for the bank's critical operations. Examples of situations in which concentration risk may arise include but are not limited to: (i) concentrations of multiple services provided by the same TPSP; (ii) concentration of services from one or multiple TPSPs in a single geographic region; or (iii) multiple TPSPs with a dependency on the same key nth party.
  - Systemic: Risk to the banking sector (and, in some cases, broader financial sector) overall arising from a dependency on one or more services provided by a single TPSP or a limited number of TPSPs (directly or indirectly through nth parties), the disruption or failure of which may have systemic implications.
- Nth party: A service provider that is part of a TPSP's supply chain and supports the ultimate delivery of services to one or more banks. This term includes, but is not limited to, subcontractors of the TPSP.
- Key nth party: A service provider that is part of a TPSP's supply chain and supports the ultimate delivery of a critical service by a TPSP to a bank or that has the ability to access sensitive or confidential bank information (eg consumer data).

IV. Third-party risk management principles

12. This section presents the Committee's proposed Principles for the sound management of risks emanating from TPSP arrangements, organised across the following categories: (i) governance, risk management and strategy; (ii) the life cycle of TPSP arrangements; and (iii) the role of supervisors. These Principles should be applied on a consolidated and on an individual bank basis. Whether activities are performed internally or by a TPSP, banks are required to operate in a safe and sound manner and in compliance with applicable laws and regulations. While the use of TPSPs can reduce banks' direct control over their activities and may introduce new risks or increase existing risks, the use of TPSPs should neither diminish banks' responsibility to fulfil their obligations to stakeholders (eg customers, supervisors, other legal authorities) nor impede regulatory oversight. As with all business processes, documentation evidencing key decisions (eg third-party strategy, board minutes reflecting decision to enter into a critical TPSP arrangement) should be maintained in banks' records.

13. Effective TPRM generally follows the stages of the life cycle for TPSP arrangements. Controls should be designed proportionally to the risks of each TPSP arrangement. A framework for monitoring and managing risks associated with TPSP arrangements benefits from identifying the criticality of bank operations supported by TPSP services at inception and periodically throughout the life cycle of a TPSP

[14] Branches are not considered intragroup providers, as they are not separate legal entities from their head offices. However, the provision of services from a head office of a bank to its overseas branches, or between branches, is not riskless. Therefore, in practice a proportionate risk-based approach to risk management and oversight of head office/branch relationships may be appropriate.

arrangement. The stages of the life cycle typically include *risk assessment, due diligence*, *contracting*, *onboarding and ongoing monitoring*, and *termination*. The bank's *governance, risk management* and *strategy* are integral to each stage of the life cycle. The stages of the life cycle are shown in Graph 1, with detailed descriptions given in the respective subsections.

Graph 1: Third-party life cycle

14. The stages of the life cycle do not necessarily reflect a linear progression. Rather, the output of each stage should serve as factors to consider in the subsequent and prior stages. For example, a bank may leverage information gained in response to an incident during the *onboarding and ongoing monitoring* stage for updating the *risk assessment* and *due diligence* processes.

15. Not all TPSP arrangements present the same level of risk and therefore not all arrangements require the same level or type of oversight or risk management. The following key concepts are embedded in all stages of the life cycle and apply to all Principles:

- Criticality: The Principles emphasise additional areas to focus on when TPSP arrangements cover critical services. Critical services typically warrant a greater level of risk management consideration. Banks' processes should enable services and TPSP arrangements which are designated as critical to receive more comprehensive oversight and more rigorous risk management (eg robust business continuity management (BCM)).
- Concentration: Concentration risk[15] in TPSP arrangements may emerge either at the individual bank level or at the systemic level. Monitoring and managing concentration at the individual bank level is the responsibility of the individual bank. While supervisors are best placed to monitor systemic concentrations, it is important for banks to understand the relative systemic importance of a TPSP, based on available information (eg from the public domain, directly from the TPSP), so that they may consider the implications of entering into an arrangement with the TPSP.
- Proportionality: Proportionality focuses primarily on how banks' management of risks related to TPSP arrangements might vary based on a bank's business model, complexity, cross-border presence, function, risk profile, scale, structure and size. When applying proportionality, a service or arrangement for one bank might not reflect the same risks or same level of risks as compared

15 See definition of concentration risk in Section III.

to another bank. For example, one bank with operations in one jurisdiction and another that operates in multiple jurisdictions may differ in their approach to applying these Principles regarding a service arrangement with the same TPSP. Application of proportionality does not mean that arrangements should be exempt from the application of appropriate risk management.

- Intragroup TPSP arrangements: Banks should not treat intragroup arrangements as if they are less risky than other arrangements. Banks' risk management processes should be proportionate to the unique characteristics of intragroup arrangements (eg the bank's level of control and influence on the intragroup entity, complexities from cross-border operations, prioritisation of the bank's requirements) and the criticality of the arrangements. Some of the important considerations include: carrying out due diligence to align with the bank's understanding of governance and risk management of the intragroup TPSP; having an appropriate formal, written arrangement with appropriate provisions and escalation mechanisms; managing risk of intragroup nth parties akin to external third parties; tailoring business continuity plans (BCPs) to maintain the bank's operations; and having exit strategies for planned and unplanned terminations of the intragroup TPSP arrangements reflecting the bank's position, while recognising that the possible range of exit options may be limited.

- Nth parties and supply chains: Banks' TPSP arrangements often involve dependencies on nth parties in the supply chain for delivery of services because of a variety of factors (eg specialisation, different types of innovation). Such chains may be lengthy and complex, resulting in additional or increased risks to banks. Banks should have appropriate risk management processes to identify and manage the supply chain risks, proportionate to the criticality of the services being provided. 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 (eg level of service, risk management, compliance, operational resilience standards). Further, contracts should reflect the right of banks to obtain information (including incident notifications) about key nth parties on an ongoing basis. As determined by the risk, such information should be captured in the registers and factored into ongoing risk assessments, including assessment of the bank-level concentration risk.

- New and advanced technologies: Rapid adoption of new and advanced technologies has increased banks' dependency on TPSPs. This has the potential to magnify existing risks (including intellectual property disputes) and introduce new risks to banks. In certain cases, because of a lack of staff experience, it may be more challenging for banks to identify or evaluate risks associated with a new technology that is provided through a TPSP arrangement.

- Audits and assurance: There are various types of audits and multiple sources of assurance that banks can use in their *due diligence* and *onboarding and ongoing monitoring* of TPSPs. Audits include those by independent parties engaged by either a single bank, a collection of banks working collaboratively (eg pooled audits), or the TPSPs themselves (to be provided to and critically reviewed by banks). Additional sources of assurance may include industry-recognised certifications or standards (eg ISO certification). These certifications and standards can help provide a comparable, baseline level of assurance about TPSPs' controls, but they may not, by themselves, provide all the assurance banks need with regard to the resilience of critical services. These certifications and standards should therefore not be seen as eliminating the need for audits and other forms of assurance where appropriate (refer to the sections on *Contracting* and *Onboarding and ongoing monitoring* below).

Governance, risk management and strategy

<u>Principle 1</u>: 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.

<u>Principle 2</u>: 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.

16. Banks should implement a TPRMF defined by a board-approved policy,[16] supported by a strong governance structure led by the board of directors and effective risk management, and aligned with the banks' business strategy (eg business needs, overall strategic goals and objectives), risk management strategy and third-party strategy (refer to section on *Strategy* below). Consistent with the Principles outlined in the PSMOR and POR, banks' TPRMF should align with their: (i) governance; (ii) risk management practices; and (iii) strategy.

Governance

17. The board of directors has ultimate responsibility for the oversight of all TPSP arrangements and for holding senior management accountable for the TPRMF's implementation. Senior management should ensure communication of the bank's third-party strategy and policy to all relevant stakeholders, including bank personnel and intragroup entities, and should establish policies and procedures that include clearly defined roles and responsibilities to manage TPSP arrangements throughout the third-party life cycle.

18. The bank's third-party life cycle and services under TPSP arrangements should be integrated into the three lines of defence[17]. Roles and responsibilities of all staff should be appropriately defined. Based on risk and complexity, banks may establish a central function to monitor all TPSP arrangements.

19. There are certain arrangements with TPSPs which entail "shared responsibility" between the bank and the TPSP (eg cloud services). The concept of "shared responsibility" does not abrogate the board of directors' ultimate responsibility for the oversight of risk management associated with TPSP arrangements and for banks to meet their legal and regulatory compliance obligations.

Risk management

20. Banks should establish a comprehensive TPRMF, integrated within their broader operational risk management framework (ORMF)[18] to manage TPSP arrangements.

21. A bank's TPRMF should consider the business model, nature, size, complexity, cross-border presence, scale, structure and risk profile of its TPSP portfolio. The TPRMF should clearly outline criteria, processes and frequency for: (i) risk identification and assessment; (ii) monitoring and reporting; and (iii) application of controls. Controls supported by competent personnel across all three lines of defence should be implemented in each stage of the third-party life cycle. Banks may engage external support to supplement the qualifications and technical expertise of in-house staff.

22. Banks should maintain a complete and up-to-date register of all TPSP arrangements (and nth parties, as appropriate to the criticality of the service and associated risks). Banks should include key elements of each arrangement in the register (eg criticality of the arrangement, substitutability of the TPSP's services, contingent providers, whether proprietary or confidential information is shared, location(s)

[16] See Basel Core Principle 25 (essential criterion 9).

[17] See PSMOR Section 3, paragraphs 6–7 for details on the three lines of defence.

[18] See PSMOR for a definition.

of service and data). Registers should be updated periodically or when there are relevant changes (eg entering into another arrangement with the TPSP, change in contractual terms, changes in criticality, changes to the service location, availability of an alternative service provider, a new subcontract, mergers and acquisitions). Banks should use the information in the registers to map dependencies and interconnections related to arrangements, particularly those associated with higher risks and those supporting critical services. Banks should be prepared to share the register with supervisors when requested (as per jurisdictional requirements).

23. Banks should assess the bank-level concentration risk initially at the time of due diligence, and periodically throughout the life cycle of the TPSP based on changes in the TPSP portfolio. Up-to-date third-party registers and mapping of dependencies and interconnections facilitate the identification of concentration risk of TPSPs. Where concentration risk is not avoidable, banks should enhance monitoring and other measures (eg testing at more frequent intervals) to mitigate the risk of critical TPSP arrangements, including concentrations in their supply chains. Banks should also explore multiple options (eg provision of critical services from multiple availability zones or geographic regions by a single provider, ensuring that TPSPs adequately manage the resilience of their supply chains, combining the use of banks' on-premises infrastructure with TPSPs' services, backup or alternative TPSPs, retaining capability to bring the service back in-house) to manage risk within their risk appetite and tolerance for disruption.

Strategy

24. The board of directors should approve a third-party strategy (which could also be part of the bank's overall risk management strategy). It should be consistent with the bank's overall business strategy, risk appetite and tolerance for disruption. It should cover the following:

- whether and to what extent the bank should enter into TPSP arrangements;
- which services should or should not be performed by a TPSP;
- standards for the ongoing evaluation of risks, costs and benefits associated with reliance on one or more TPSPs; and
- what conditions, if any, should trigger an exit from TPSP arrangements.

25. Banks' tolerances for disruption should reflect the risks from TPSP arrangements, be forward-looking and, where applicable, subject to scenario and stress testing to ensure that banks evaluate whether risks relating to TPSP arrangements remain within their risk appetites. This includes consideration of the risks and benefits posed by new and advanced technologies when developing their third-party strategy, and as part of the implementation of their TPRMF.

26. Banks should maintain adequate in-house knowledge, experience, and training and awareness programmes to identify, assess, manage and monitor the risks posed by TPSP arrangements.

Risk assessment

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.

27. The *risk assessment* stage of the life cycle is where banks identify and assess the criticality of potential services and the risks before entering into a proposed arrangement with a TPSP, in alignment with the bank's third-party strategy, policies and TPRMF. Moreover, risk assessment is an iterative process throughout the life cycle of a TPSP arrangement.

28. When assessing criticality banks should consider factors such as the financial, operational or strategic importance of the arrangement; their tolerance for disruption; the nature of any data or information shared with the TPSP; or the substitutability of the service.

29. Banks should assess the potential impacts of entering into any TPSP arrangement on their operations (eg activities, functions, systems, data), including the criticality of the operations, considering risks and assessment results in order to: (i) assess adequacy of the current control environment to incorporate the TPSP's activities; (ii) plan appropriate risk monitoring, reporting and escalation; (iii) plan mitigation measures; (iv) communicate expectations of the proposed TPSP arrangement to stakeholders;[19] and (v) develop related proposed contractual terms and conditions.

30. Banks should consider known risks that may be reduced or better managed and potential risks that may arise from the proposed arrangement, such as risks posed by new and advanced technologies. They should consider all types of risks related to TPSP arrangements, including but not limited to strategic risk, reputational risk, compliance risk, operational risk (eg information and communication technologies (ICT), cyber), concentration risk and the risk stemming from a long supply chain. Banks should document the process and results of the analysis performed.

31. In their risk assessments, banks should consider how any arrangement would align with their business strategy, third-party strategy, risk appetite and tolerance for disruption, and consider the expected benefits and costs of the proposed TPSP arrangement. The outcome of the initial risk assessment should enable a bank to make an informed decision on whether to engage a TPSP. This risk assessment would be complemented by a TPSP-specific risk assessment (eg TPSP's size, complexity) (refer to section on *Due diligence*).

32. Risks may change throughout the life cycle of the TPSP arrangement. Therefore, banks should perform risk assessments on an ongoing basis (refer to *Onboarding and ongoing monitoring* below).

Due diligence

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

33. The *due diligence* stage of the life cycle is where banks gather and analyse the information needed to determine how well an arrangement with a specific TPSP would support their third-party strategy. 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 TPSP.

34. Banks should have an appropriate and proportionate process for selecting and assessing the prospective TPSP before entering into a TPSP arrangement. The risk associated with a specific TPSP could affect the overall risk assessment of a bank's existing TPSP arrangements.

35. Banks should perform due diligence to mitigate risks as outlined in the *risk assessment* stage. Banks' due diligence, including inputs from monitoring of any prior arrangements, should support the analysis of: (i) the TPSP's capacity and ability to perform; (ii) known and potential risks related to the TPSP arrangement; and (iii) relative benefits and costs of the arrangement. Aspects that should be considered under each of these dimensions are outlined below.

Capacity and ability

36. As part of the assessment of a TPSP's capacity and ability to deliver the services under the arrangement, banks should consider the TPSP's:

- operational and technical capability;
- ability to support the bank's objectives for innovation, expansion and third-party strategy;

[19] See PSMOR Principle 7 and POR Principle 2.

- ability to support the bank's legal and regulatory compliance obligations;
- ability to maintain qualified and adequate staff for ongoing service delivery as well as during disruption;
- effectiveness of internal controls and risk management, including its ability to manage ICT,[20] cyber[21] and other operational risks;
- ability to manage supply chain risks; and
- ability to maintain BCPs, disaster recovery plans (DRPs) and other relevant plans (eg crisis communication plans) consistent with or benchmarked to the bank's tolerance for disruption of critical services.

Risks

37. As part of the assessment of known and potential risks associated with the TPSP arrangement, banks should consider:

- how the responsibility for security, resilience and other technical configurations (eg access management controls) will be allocated between banks and TPSPs with respect to the delivery of services, and the associated risks;
- financial soundness insofar as it can affect the delivery of the relevant services;
- geographic dependencies and management of related risks (eg risks related to the economic, financial, political, legal and regulatory environment in the jurisdiction(s) where the relevant service will be provided);
- potential conflicts of interest (including those from intragroup and nth parties);
- recent or pending relevant complaints, investigations or litigation including (if relevant) at TPSPs' nth parties;
- availability of potential alternative TPSPs and assessment of related risks; and
- whether the arrangement under consideration may result in unacceptable concentration risk (refer to *Definitions* and paragraph 15).

Relative benefits and costs

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

- the potential risks of not entering into a TPSP arrangement against the risks that the new TPSP arrangement may introduce or amplify known risks (eg replacing obsolete legacy system, difficulty in hiring and maintaining qualified staff);
- the bank's ability (including cost, timing, contractual restrictions) to exit the TPSP arrangement and either transition to another TPSP or bring the activity back in-house; and
- the bank's ability to adopt new and advanced technologies and the potential risks thereof.

[20] See PSMOR for definition.

[21] See POR Principle 7.

Contracting

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.

39. The *contracting* stage of the life cycle is when negotiations between a bank and a TPSP occur, and where terms 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.

40. TPSP arrangements should be governed by clearly written, legally binding contracts.[22] The nature and details of these contracts should be appropriate to the banks and to the criticality of the services provided by the TPSPs and should reflect legal and regulatory obligations of the jurisdictions where the banks and TPSPs operate.

41. Banks' contracts governing TPSP arrangements should consider:

- key performance benchmarks;
- rights for banks to receive accurate, comprehensive and timely information (including regarding incidents impacting the services they are receiving);
- rights of the TPSPs related to provision of the services outlined in the SLAs (eg technical requirements, facility access);
- rights of banks to access (including premises), audit and obtain relevant information from the TPSPs;
- rights of supervisory authorities to access (including premises), audit and obtain relevant information from TPSPs as permitted under applicable laws and regulations within the respective jurisdictions or bi-/multilateral agreements amongst supervisors;
- obligations and responsibilities relating to business continuity and disaster recovery for the services provided and to support banks' BCP and DRP testing as appropriate (refer to the section on *Business continuity management*);
- costs, including (if applicable) flexibility and scalability based on the banks' use of the service and the payment arrangements;
- ownership, access to and use of logical assets (eg data, applications, application programming interfaces (APIs), models, intellectual property rights) and physical assets (eg hardware, records, premises) as well as how easily these can be transferred in a timely manner and appropriate format, including in the case of termination;
- obligations and responsibilities relating to security, resilience and other technical configurations;
- the location(s) (ie regions or countries) where the activity will be performed and where relevant data will be processed and stored;
- confidentiality of banks' proprietary and strategic information and the use of non-disclosure agreements (NDAs);
- addressing the risk of co-mingling of banks' information with that of other clients of the TPSPs;

[22] In cases where a legally binding contract may not be possible, for example where the TPSP is a branch of the bank and thus not a legally distinct entity, it may be useful to have a service level agreement (SLA) to formally document the services required by the branch, the roles and responsibilities of the involved parties including service standards, and the consequences of not meeting these standards. This may be particularly useful in cases where the branch needs to meet local regulatory requirements, for instance with respect to operational resilience, for the services it provides locally.

- rights of banks to indemnification in specific circumstances (including any limitations on the TPSPs' liability);
- customer complaints handling and dispute resolution mechanisms;
- choice of law and jurisdiction in case of dispute (where possible, with a preference to apply the laws of the jurisdiction where the bank is incorporated or operating);
- default and termination, including conditions to terminate, roles and responsibilities, notification, and minimum periods to execute termination provisions;
- the framework to amend existing arrangements, including when there are changes in regulatory requirements in relation to the third-party activities; and
- provisions to support banks' exit strategies for eventual termination.

42. Banks' contracts governing critical TPSP arrangements should at a minimum include the provisions covered in paragraph 41 and those listed below:

- conditions governing key nth parties (eg prior notification of use or change, incident reporting);
- additional indicators and metrics for key performance benchmarks including the methodology for measurement (eg SLA and standards, BCM testing results, control effectiveness test results, customer complaint information);
- rights for banks to receive accurate, comprehensive and timely information as outlined in the SLA, including but not limited to information on incidents and material changes to the services of TPSPs or their supply chains;
- rights of banks to access, audit and obtain relevant information from key nth parties;
- rights of supervisory authorities to access, audit and obtain relevant information from key nth parties as permitted under applicable laws and regulations within the respective jurisdictions or bi-/multilateral agreements amongst supervisors;
- obligations and responsibilities for BCPs and DRPs should include minimum service uptime and/or maximum service downtime commitments, recovery time objectives (RTOs) and recovery point objectives (RPOs)[23]; and
- TPSPs' obligation to take out insurance against insurable risks.

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.

Onboarding and ongoing monitoring

Onboarding

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.

44. Banks should maintain levels of staffing and competency (including education, certifications or qualifications, skillsets, language proficiency, experience and training) to meet the needs of the TPSP arrangement within their TPSP portfolios.

[23] See PSMOR Principle 11.

45. When a TPSP is onboarded, banks need to ensure it has adequate understanding of the bank's policies, people, processes, technology, facilities and the interconnections that are needed to provide the contracted service, in compliance with laws and regulations. Each time banks onboard a new TPSP they should update their register and map interdependencies (refer to paragraph 22). Tools like an initial checklist may help banks in their onboarding process. Specific checklist items might vary depending on the type of arrangement, its associated risks and other context-dependent elements.

Ongoing monitoring

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.

46. The ongoing monitoring stage is where banks should: (i) confirm the quality and sustainability of a TPSP's controls and ability to meet contractual obligations; (ii) report the performance status of TPSPs and significant issues or concerns (eg material or repeat audit findings, deterioration in financial condition, security breaches, data loss, service interruptions, compliance lapses or other indicators of increased risk); (iii) escalate as specified in banks' policies and procedures; (iv) respond to issues; and (v) confirm the quality and sustainability of the banks' and TPSPs' BCM.

47. Ongoing monitoring should be aligned with banks' governance, risk management and strategy, the risks considered when the TPSP was selected, any new risks that have emerged since selection, and contractual obligations of the TPSPs. It should include key nth parties.

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

49. Monitoring should include performance-related metrics, such as ongoing key performance indicators and scorecards in line with banks' policies and procedures used to check compliance with SLAs, contractual provisions, regulatory expectations and legal requirements. Banks should keep an updated register of all TPSP arrangements, reflecting any changes in criticality (refer to paragraph 22). Banks should also maintain an up-to-date mapping of their interdependencies or interconnections for critical TPSP arrangements.[24] Banks should leverage this information to identify and monitor bank-level concentration risk at a frequency commensurate with the changes to the operating environment.

50. In arrangements involving shared responsibility, banks should monitor TPSP performance and operational implementation to ensure that obligations and responsibilities are clearly understood and fulfilled by the TPSP. Banks should also monitor their internal control environment and processes to meet their obligations and responsibilities.

51. Banks should review BCPs and DRPs of critical TPSPs and ensure that periodic testing is performed (refer to section on *Business continuity management*).

Reporting

52. The outcome of the risk assessments (eg portfolio level, critical services level) should be reported to senior management and boards of directors periodically and as needed according to banks' policies and procedures. Reporting should encompass: (i) reports on the results/performance of TPSPs; (ii) significant changes in the TPSP portfolio and its risk profile; (iii) breach of established triggers and

[24] See POR Principle 4.

thresholds; and (iv) items in need of prompt attention (eg a major disruption resulting from an incident at a TPSP, concentration risk).

53. Effective risk management includes monitoring, reporting and responding to incidents, including those originating from TPSPs contracted to provide services to banks. Where applicable, banks must comply with all reporting obligations to authorities regarding incidents and contract provisions should provide bank management with the ability to monitor incidents related to TPSPs (refer to section on *Contracting*). For critical services, banks should consider incorporating requirements related to incident reporting in the contracts, including minimum information to be reported. Contracts may require TPSPs to have clearly defined processes for identifying, investigating and remediating incidents related to contracted services and notifying banks in a timely manner of incidents that impact the TPSP's ability to meet contractual obligations. Banks' ongoing monitoring processes should include monitoring of incident response at TPSPs. Banks should integrate the remediation and reporting of incidents related to TPSPs into their broader risk management processes (eg cyber security, threat and intelligence gathering, BCM). Banks should also analyse updates on remediation of reported incidents and use this information to update their risk assessments of TPSPs.

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. Standardised assurances (eg ISO certificates) need to be critically assessed and fully understood to allow banks to identify their relevance compared to the banks' internal standards and requirements.

Response

55. In case of a disruption, banks' monitoring should provide: (i) oversight of remediation actions by TPSPs to restore service delivery to contractual levels; (ii) identification of risks associated with the continuation of the TPSP arrangement; and (iii) feedback to TPSPs' senior management of banks' expectations. When monitoring determines that a given TPSP is no longer a viable option, banks need to initiate steps for the least disruptive termination of the arrangement.

56. 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.

57. When banks decide to not renew a TPSP arrangement, they should ensure continuity of their operations and manage termination in the least disruptive manner (refer to section on *Termination*).

Business continuity management

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

58. Banks should manage their dependencies on TPSP arrangements within their BCM. A bank's BCM should consider:

- development, periodic review and updating of the bank's internal BCPs and DRPs with respect to TPSP arrangements;
- periodic testing of the bank's BCPs and DRPs, considering a range of possible recovery strategies or compensating controls (eg switching to another TPSP, using multiple TPSPs, bringing the service in-house, employing a combination of on-premises and external data centres across different geographical regions) that can deliver a level of resilience consistent with the bank's risk appetite and tolerance for disruption;
- lessons learned from incidents (if any) and result of the periodic testing; and

- periodic updating of identified alternative providers.

59. A bank's BCM governing critical TPSP arrangements should at a minimum include the provisions covered in paragraph 58 and those listed below:

- 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);[25] and
- assurance testing (eg walkthroughs, tabletops and simulations) that the TPSP's BCP methodologies are robust.

60. Banks should also consider joint design and testing of BCPs with TPSPs, or utilise independent parties to do the same.

61. In cases where alternative TPSPs do not exist for critical services, banks' BCM should address actions to be taken to ensure the continuity of the service.[26]

Termination

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

62. The *termination* stage is where banks manage planned or unplanned terminations of arrangements for reasons such as expiration or breach of the contract, the TPSP's failure to comply with applicable laws or regulations, or a desire to seek an alternate TPSP, bring the activity in-house or discontinue the activity. When this occurs, it is important for banks to terminate the arrangement in a safe and sound manner.

63. Banks should maintain appropriate and proportionate exit plans for planned terminations within their exit strategies. Exit plans need to be regularly updated and tested for availability of budget, human resources, technical infrastructure, transfer of knowledge, access to data and other factors. The level of detail in the plans should be commensurate with the criticality and substitutability of the services provided.

64. Banks' plans for the termination of TPSP arrangements should consider:

- transitional periods;
- perfection of rights contained in contract provisions (eg preservation and availability of audit trails, archiving and destruction of data, system access revocation);
- adequate budget allocation; and
- clear identification of responsibilities to coordinate and manage the exit.

65. Banks' exit plans for the termination of critical TPSP arrangements should at a minimum include the provisions covered in paragraph 64 and those listed below:

- processes for transferring logical assets (eg data, application, API, models, intellectual property rights) in an appropriate format, physical assets (eg hardware, records, premises) and human resources (eg consultants, contract employees) in a timely manner; and
- actions necessary to enable alignment between all internal (eg human resources, legal and compliance function, IT teams) and external stakeholders (eg new TPSP, supervisor).

25 See POR Principle 1.

26 See POR Principle 5.

66. Banks should maintain appropriate and proportionate exit strategies for unplanned terminations for all TPSP arrangements taking into consideration factors such as the size, complexity and risk profile of the bank and whether the TPSP arrangements cover critical services. Although unplanned terminations may occur less frequently than planned terminations, they potentially pose more risks and banks should prepare for such events.

67. Banks' exit strategies for the unplanned termination of critical TPSP arrangements should at a minimum include:

- processes for transferring logical and physical assets in a timely manner and an appropriate format;
- periodic updating of identified members of an escalation or emergency group (with appropriate control functions represented); and
- a process for budget approval to cover additional costs associated with the event and to source necessary expertise (eg consultants, temporary workers) to transition the services.

Role of supervisors

<u>Principle 10</u>: Supervisors should consider third-party risk management as an integral part of ongoing assessment of banks.

68. Supervisors recognise that banks' dependencies on TPSPs, if not managed appropriately, may impede their ability to fulfil their regulatory requirements. Supervisors should, therefore, assess banks' TPRMF and consider how they align to their ORMF to support their operational resilience. Supervisory evaluations should cover the entire third-party life cycle. Emphasis should be placed on how banks integrate TPSP arrangements within their overall risk management processes (eg incident management, cyber security controls, BCM).

69. As certain TPSP arrangements require highly technical skills, supervisors should periodically evaluate the knowledge and skills of supervisory staff.[27]

<u>Principle 11</u>: Supervisors should analyse the available information to identify potential systemic risks posed by the concentration of one or multiple TPSPs in the banking sector.

70. Concentration of services provided by TPSPs combined with lack of substitutability of TPSPs is relevant to the identification of systemic risks. To assess and monitor such risks across the banking sector, supervisors should be able to obtain from banks information reflecting their arrangements with TPSPs (including those involving shared responsibilities).[28] The types of information supervisors could leverage include registers of TPSP arrangements; maps of interconnections and interdependencies;[29] recovery and resolution plans; and reports on incidents involving TPSPs. To analyse systemic concentration risk, supervisors may assess banks' aggregate TPRM capabilities using common supervisory tools (eg scenario analysis, data analytics, other data-driven models).

<u>Principle 12</u>: Supervisors should promote coordination and dialogue across sectors and borders to monitor systemic risks posed by critical TPSPs that provide services to banks.

71. Bank supervisors should promote coordination and dialogue among themselves, supervisors of other sectors and relevant stakeholders to monitor systemic risk. Such collaboration may include a variety

[27] See Basel Core Principle 2 (essential criteria 5–7).

[28] See Basel Core Principle 25 (additional criteria 1–2).

[29] See POR Principle 4.

of efforts to support the resiliency of critical infrastructure (eg industry- and/or supervisory-led business continuity exercises).

72. Additionally, collaboration may comprise: (i) appropriate cross-border coordination and collaboration mechanisms (eg enhancement of bilateral and multilateral memoranda of understanding (MoUs), leveraging supervisory forums[30]) fostering direct collaboration with critical TPSPs providing services to banks in multiple jurisdictions (eg use of bilateral or multilateral platforms for promoting information-sharing and building collective competencies); and (ii) exploring efforts to enhance cross-border resilience of critical, internationally active service providers (eg information-sharing, tabletop exercises, coordinated responses and recovery exercises, joint examinations).

[30] See Basel Core Principle 3.