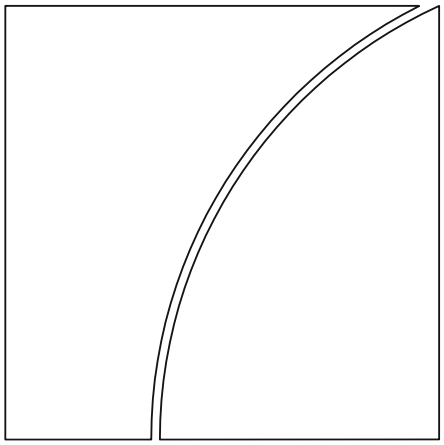
Basel Committee
on Banking Supervision



Principles for the sound management of third-party risk

December 2025

BIS

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

ISBN 978-92-9259-916-4 (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 to 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 on Banking Supervision (BCBS) believes that appropriate risk management of banks' TPSP arrangements, supply chain (ie nth parties), concentration risk and other risks 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 BCBS seeks to promote a principles-based approach to effective third-party risk management (TPRM), which should complement banks' operational risk management, and strengthen their operational resilience. The approach follows the life cycle of a TPSP arrangement, builds on the *Principles for operational resilience* (POR),[2] the revised *Principles for the sound management of operational risk* (PSMOR)[3] and other BCBS publications[4] and draws from previously issued principles as well as TPRM 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 BCBS 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 begins by laying out key concepts that apply to the 12 principles: Principles 1 to 9 provide banks with guidance on the effective management of TPSP risks, while Principles 10 to 12 provide guidance for prudential supervisors. The Principles seek to achieve a balance between 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 offer guidance on holistic third-party risk management for banks, allowing them the flexibility to tailor their TPRM practices based on the risks and the criticality of their TPSP arrangements. Further, the Principles outline additional expectations with regard to critical TPSP arrangements. The Principles are technology-agnostic to maintain relevance as technology

[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.

develops. They aim to promote international engagement, as well as greater collaboration and consistency, with a view to reducing regulatory fragmentation.

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, business model and risk profile of the bank, as well as the risks and criticality of the TPSP arrangements. The Principles are directed to large internationally active banks and their prudential supervisors in BCBS member jurisdictions.

II. Reference to other guidance

6. 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]

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

- Financial Stability Board (FSB) – 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]

8. The BCBS 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, *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.

9. While developing these Principles, it is noted that many jurisdictions have developed their own TPRM frameworks and standards, which are unique to jurisdiction(s) and are designed according to legal and regulatory obligations.

III. Definitions

10. These Principles aim to make use of terms previously defined by the BCBS and other international standard-setting bodies (see Section II above) 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.

- TPSP arrangement:[11,12] 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.[13]
  - 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 providing or receiving financial market infrastructure (FMI) services, such as clearing or settlement, to other banks),[14] 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).
- Third-party service provider (TPSP): An entity or individual which performs services, activities, functions, processes or tasks directly for a bank.

[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 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] The term "arrangement" was used to align with PSMOR terminology. It is synonymous with the term "relationship" as used in the FSB's report on *Enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities*.

[13] The Principles include intragroup entities in the definition of TPSPs when they function as third-party service providers. Although the POR differentiate between "third party" and "intragroup", the risk management requirements for third-party dependencies outlined in both documents apply equally to both categories.

[14] The exclusion of the FMIs is not intended to imply that banks should not take appropriate steps to manage risk in these arrangements. Rather, it is intended to avoid duplication and unintentional conflicts between the Principles and standards and guidance specific to FMIs.

- Critical service:[15] A service provided to a bank, the failure or disruption of which could significantly impair a bank's viability, critical operations,[16] or ability to meet key legal and regulatory compliance obligations.
- Critical TPSP arrangement: A TPSP arrangement which materially supports or impacts one or more critical services provided to a bank.
- Intragroup TPSP: A TPSP that is part of a banking group and provides services to entities within the same group. Intragroup TPSPs may include a bank's parent company, sister companies, subsidiaries, service companies or other entities that are under common ownership or control.[17]
- 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 (or, where relevant, on a group basis) 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 services 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.[18]
- Nth party: A service provider that is part of a TPSP's supply chain. This term includes, but is not limited to, subcontractors of the TPSP.
- Key nth party: An nth party that supports and is essential to the ultimate delivery of a critical service to a bank.

IV. Third-party risk management principles

11. This section presents the Basel Committee's Principles for the sound management of risks emanating from TPSP arrangements (organised across the life cycle of TPSP arrangements), and the role of supervisors. These Principles address risk management on a consolidated and on an

[15] 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 the nature of services provided by a bank to its customers.

[16] See definition in POR.

[17] 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. Additionally, in contrast to the FSB's toolkit this definition does not use the term "predominantly" to align with PSMOR.

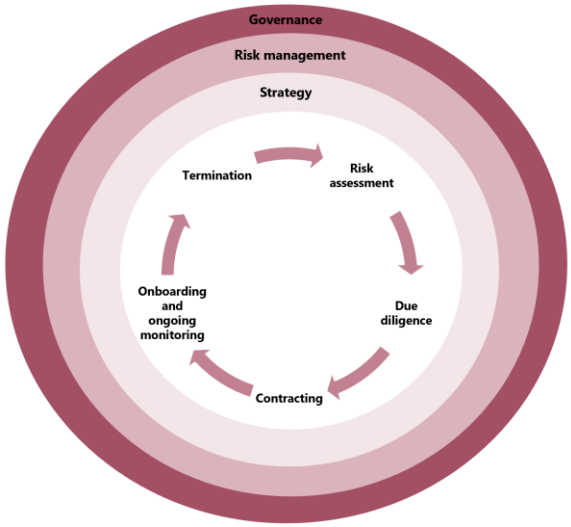
[18] For a definition of "systemic" see International Monetary Fund, Bank for International Settlements and Financial Stability Board, *Guidance to assess the systemic importance of financial institutions, markets and instruments: initial considerations*, October 2009, www.bis.org/publ/othp07.pdf.

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 assets (including data) 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 and other legal authorities) nor impede effective regulatory oversight. As with all business processes, documentation evidencing TPRM processes (eg risks assessment and due diligence results, selection of TPSPs, and monitoring and termination of TPSP arrangements) and decisions (eg third-party strategy and board minutes reflecting a decision to enter into a critical TPSP arrangement) should be maintained in banks' records.

Third-party arrangement life cycle

12. Effective TPRM generally follows the stages of the life cycle for TPSP arrangements. Controls should be designed proportionally to the risks and criticality of each TPSP arrangement. A framework for TPRM benefits from identifying the risks and criticality of bank operations supported by a TPSP arrangement at inception and periodically (eg renewals) throughout its life cycle. The stages of the life cycle typically include *risk assessment, due diligence,*[19] *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 arrangement life cycle



13. 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 its initial *risk assessment* and *due diligence* processes of that TPSP.

[19] Risk assessment focuses on the service arrangement, while due diligence concentrates on the specific prospective TPSP.

Key concepts of the life cycle

14. The following key concepts are embedded in all stages of the life cycle and apply to all Principles:

- Proportionality: TPRM processes should be commensurate with the bank's size, complexity, business model, risk profile and cross-border presence as well as the risks and criticality of the TPSP arrangements. Therefore, a TPSP arrangement for one bank might not reflect the same risks or same level of risks compared with another bank. As a result, banks may take a different approach when applying these Principles regarding a TPSP arrangement. Application of proportionality does not mean that arrangements should be exempt from the application of appropriate risk management.
- 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 apply more comprehensive oversight and more rigorous risk management (eg robust business continuity management (BCM)) to those TPSP arrangements and services which are designated as critical. Additionally, arrangements that contribute to bank-level concentration risks – where the simultaneous disruption of multiple non-critical services could severely affect the bank's viability, critical operations or ability to meet key legal and regulatory compliance obligations – should also be considered within this scope. Following the risk assessment (refer to section on *Risk assessment*), a bank may conclude that some TPSP arrangements pose higher levels of risk, which may be financial or non-financial. Banks should consider applying the Principles identified as relevant to critical TPSP arrangements to those TPSP arrangements that pose higher (but not necessarily critical) levels of risk.
- Concentration: Concentration risk[20] in TPSP arrangements may emerge either at the individual bank level or at the systemic level. Monitoring and managing concentration risk at the individual bank level is the responsibility of the individual bank. While supervisors have a role to play in monitoring systemic concentration risk, it is important for banks to understand the relative systemic importance of a TPSP, based on available reliable information (eg from the public domain and directly from the TPSP), so that they may consider the implications of entering into an arrangement with the TPSP.
- Intragroup TPSP arrangements: Banks should not treat intragroup TPSP arrangements as if they are inherently 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 and prioritisation of the bank's requirements) and the risks and 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 a 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 the delivery of services because of a variety of factors (eg specialisation and 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, monitor and manage the supply chain risks, proportionate to the risks and criticality of the services being provided. In addition, banks' *risk assessment, due diligence, contracting,* and

[20] See definition of concentration risk in Section III.

onboarding and ongoing monitoring processes should evaluate the TPSPs' ability to monitor and manage the risks related to nth parties essential for the delivery of services associated with TPSP arrangements that pose higher levels of risks or critical TPSP arrangements. For critical TPSP arrangements, contractual obligations (eg service level agreement (SLA), risk management, compliance and operational resilience standards) equivalent to the TPSPs' obligations to the bank should be cascaded, as relevant, to the key nth parties. Further, such 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 or advanced technologies: Rapid adoption of new or 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 (refer to section on *Governance, risk management and strategy* below), it may be more challenging for banks to identify or evaluate risks associated with a new or advanced 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 International Organization for Standardization (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 regarding the effectiveness of risk management processes at the TPSP for 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

Principle 1: The board of directors has ultimate responsibility for the oversight of the bank's third-party risks and should approve a clear strategy and define the bank's risk appetite and associated tolerance for disruption.

Principle 2: The board of directors should ensure that senior management implements 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 to the board of directors.

15. Banks should implement a TPRMF,[21] supported by a strong governance structure led by the board of directors and effective risk management aligned with the banks' business strategy (eg business needs, and 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

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

PSMOR and POR, banks' TPRMF should align with their: (i) governance; (ii) risk management practices; and (iii) strategy.

Governance

16. The board of directors has ultimate responsibility for oversight of the bank's third-party risks. Banks should utilise their existing governance structure[22] for approval of the TPRM policies and critical TPSP arrangements, and hold senior management accountable for the TPRMF's implementation.

17. 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 arrangement life cycle.

18. The bank's third-party arrangement life cycle and services under TPSP arrangements should be integrated into the three lines of defence.[23] 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"[24] between the bank and the TPSP. The concept of shared responsibility does not abrogate the board of directors' ultimate responsibility for oversight of the banks' third-party risks.

Risk management

20. Banks should establish a comprehensive TPRMF, aligned with their broader operational risk management framework (ORMF),[25] and the TPRM strategy approved by the board, to manage the risks posed by TPSP arrangements.

21. A bank's TPRMF should consider the bank's size, complexity, business model, risk profile and cross-border presence as well as the risks and criticality of the TPSP arrangements. The TPRMF should clearly outline criteria, processes and frequency for: (i) risk identification and assessment; (ii) monitoring and reporting; and (iii) application of controls.

22. Banks should maintain complete and up-to-date registers of all TPSP arrangements and key nth parties. Banks should include key elements of each arrangement in the registers (eg criticality of the arrangement, substitutability of the TPSP's services, contingent providers, whether proprietary or confidential information is shared, location(s) of service and data, and legal entity identifier (LEI), where available). Registers should be updated periodically or when there are relevant changes (eg entering into another arrangement with the TPSP, changes in contractual terms, changes in criticality, changes to the service location, availability of a contingent provider, and mergers and acquisitions). Banks should use the information in the registers to map

[22] Consistent with PSMOR and POR, this document refers to a management structure composed of a board of directors and senior management. The BCBS is aware that there are significant differences in legislative and regulatory frameworks across countries regarding the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management and general management) so as to ensure that the latter fulfils its tasks. For this reason, in some cases, it is known as a supervisory board. This means that the board has no executive functions. In other countries, the board has a broader competence in that it lays down the general framework for the management of the bank. Owing to these differences, the terms "board of directors" and "senior management" are used in this paper not to identify legal constructs but rather to label two decision-making functions within a bank.

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

[24] See Basel Committee on Banking Supervision, *Digitalisation of finance*, May 2024, www.bis.org/bcbs/publ/d575.pdf.

[25] See PSMOR for a definition.

dependencies and interconnections related to arrangements, particularly those associated with higher levels of risks and those supporting critical services. Banks should be prepared to share the registers 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 bank-level concentration risk of TPSPs. Where exposed to bank-level concentration risk including concentrations in their supply chains, banks should enhance monitoring and other measures (eg testing at more frequent intervals) to mitigate the risk of critical TPSP arrangements. Banks should also explore multiple options (eg the provision of critical services from multiple 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, and retaining capability to bring the service back in-house) to manage bank-level concentration risk within their risk appetite and tolerance for disruption.[26]

Strategy

24. The board of directors should approve a TPRM strategy (which could also be part of the bank's overall risk management strategy). It should be consistent with other relevant strategies and the bank's risk appetite. It should cover the following:

- whether and the extent to which 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
- the conditions, if any, that should trigger an exit from TPSP arrangements.

25. Banks' risk appetite, risk tolerance[27] and tolerances for disruption should reflect the risks from TPSP arrangements, be forward-looking and, where applicable, subject to scenario and stress testing. This includes consideration of the risks and benefits posed by new or advanced technologies when developing their third-party strategy, and as part of the implementation of their TPRMF.

26. Banks should maintain an adequate level of staffing, in-house knowledge, experience, competency, and training and awareness programmes to identify, assess, manage and monitor the risks posed by TPSP arrangements. Banks may engage external support to supplement the qualifications and technical expertise of in-house staff.

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 the life cycle of a TPSP arrangement.

[26] See PSMOR for a definition of "risk appetite" and POR for a definition of "tolerance for disruption".

[27] See PSMOR for a definition of "risk tolerance".

27. The *risk assessment* stage of the life cycle is where banks identify and assess (i) the types and levels of risks; and (ii) the criticality of potential services associated with a proposed TPSP arrangement.

28. As part of assessing the types and levels of risks, banks should consider risks related to TPSP arrangements, including bank-level concentration risk, the risk stemming from a long or complex supply chain, as well as new or advanced technologies, and other financial and non-financial risk. Complimentary to this is the assessment of criticality. Banks should consider their tolerance for disruption of the service provided by the TPSP; the nature of any data or information shared with the TPSP; or the substitutability of the service. Banks should also assess the potential impacts of entering into any TPSP arrangement on their operations (eg activities, functions, systems and data). Further, banks should document the methodology and results of the analysis performed.

29. Based on the risk assessment results, banks should: (i) assess the adequacy of their current control environment to incorporate TPSP arrangements; (ii) plan appropriate risk monitoring, reporting and escalation; (iii) plan mitigation measures; (iv) communicate expectations of the proposed TPSP arrangement to stakeholders;[28] and (v) develop related proposed contractual terms and conditions.

30. In their risk assessments, banks should consider how an arrangement would align with their TPRMF and TPRM policies, and consider the expected benefits and costs of the proposed TPSP arrangement. The outcome of the 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 and complexity) (refer to section on *Due diligence*).

31. The risk assessment is an iterative process throughout the life cycle of a TPSP arrangement. Risks may change throughout the life cycle of the TPSP arrangement. Therefore, banks should perform risk assessments on a regular basis and whenever there are major changes impacting the arrangement (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.

32. 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.

33. 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 profile.

34. Banks' due diligence, including inputs from monitoring any relevant prior arrangements, should support the analysis of: (i) the TPSP's capacity and ability to deliver the services; (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.

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

Capacity and ability

35. 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;
- 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 a disruption;
- effectiveness of internal controls and risk management, including its ability to manage information and communication technology,[29] cyber[30] and other operational risks;
- ability to manage supply chain risks (eg identification of key nth parties, providing relevant information to the bank when requested); 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

36. As part of the assessment of known and potential risks associated with TPSPs, banks should consider:

- how responsibility for security, resilience and technical configurations (eg access management controls) will be shared between the bank and TPSP with respect to the delivery of services and the associated risks;
- the TPSP's financial soundness insofar as it can affect the delivery of the relevant services;
- geographic dependencies and management of related risks (eg probability of natural disasters, 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 between the bank and TPSP (including key nth parties);
- track record, recent or pending relevant complaints, investigations or litigation including (if relevant) against the TPSP or its key nth parties;
- the TPSP's approach to insurable risks;
- availability of potential alternative TPSPs and assessment of related risks; and
- whether the arrangement under consideration may result in unacceptable bank-level concentration risk (refer to *Definitions* and paragraph 14).

Relative benefits and costs

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

[29] See PSMOR for definition.

[30] See POR Principle 7.

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

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.

38. 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. Contractual provisions should facilitate effective risk management and oversight of the TPSPs and relevant services by the banks, and specify the expectations and obligations of both the banks and TPSPs. Banks should negotiate a contract that meets their own business goals and risk management needs.

39. TPSP arrangements should be governed by clearly written, legally binding contracts.[31] The nature and details of these contracts should be appropriate to the banks and to the risks and criticality of the services provided by the TPSPs and reflect legal and regulatory obligations in the jurisdictions where the banks and TPSPs operate.

40. Banks' contracts governing TPSP arrangements should consider:

- key performance benchmarks;
- rights for banks to receive accurate, comprehensive and timely information (including regarding TPSPs' TPRM practices and incidents impacting the services they are receiving);
- rights of the TPSPs related to provision of the services outlined in the SLAs (eg technical requirements and facility access);
- rights of banks to access (including premises), audit and obtain relevant information from the TPSPs (refer to "Audits and assurance" in paragraph 14);
- 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 payment arrangements;
- ownership, access to and use of logical assets (eg data, applications, application programming interfaces (APIs), models and intellectual property rights) and physical assets (eg hardware,

[31] 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 an 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.

records and 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;
- 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 due to regulatory or supervisory requirements; and
- provisions to support banks' exit strategies for eventual termination.

41. Banks' contracts governing critical TPSP arrangements should include the provisions covered in paragraph 40 and those listed below:

- conditions governing key nth parties (eg prior notification of use or change, and incident reporting);
- additional indicators and metrics for key performance benchmarks including the methodology for measurement (eg SLA and standards, BCP testing results, control effectiveness test results and 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 key nth party;
- rights of banks to access, audit and obtain relevant information from key nth parties (refer to "Audits and assurance" in paragraph 14);
- 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; and
- obligations and responsibilities for BCPs and DRPs (eg minimum service uptime and/or maximum service downtime commitments, recovery time objectives (RTOs) and recovery point objectives (RPOs)).

42. 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 onboarding of a new TPSP, including for the resolution of any issues identified during due diligence or interpretation of contractual provisions.

43. When a TPSP is onboarded, banks should ensure that the TPSP 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 registers and map interdependencies (refer to paragraph 22).

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.

44. 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.

45. 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 onboarding and contractual obligations of the TPSPs. It should include key nth parties.

46. 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 or conflicts of interest), the TPSP (eg organisation, location of services, and introduction of new or advanced technologies) or the external environment (eg political, economic, social, legal and financial landscape, and any potential impediments to the delivery of activities). TPSP arrangements that pose a higher level of risks and/or critical TPSP arrangements should be assessed more frequently.

47. 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 updated registers of all TPSP arrangements and key nth parties, reflecting any changes in risks and criticality (refer to paragraph 22). Banks should also maintain an up-to-date mapping of their interdependencies or interconnections for critical TPSP arrangements including for key nth parties.[32] Banks should leverage this information to identify and monitor bank-level concentration risk at a frequency commensurate with the changes to the operating environment.

48. 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.

[32] See POR Principle 4.

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

50. 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 with the banks' internal standards and requirements.

Reporting

51. The outcome of the risk assessments (eg portfolio level and 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 any resulting impact on the bank's risk profile; (iii) breach of established triggers and thresholds; and (iv) items in need of prompt attention (eg a major disruption resulting from an incident at a TPSP or bank-level concentration risk).

52. 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 banks with the ability to monitor incidents related to TPSPs (refer to section on *Contracting*). For critical services, banks should incorporate 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 threat and intelligence gathering and BCP). Banks should also analyse updates on the remediation of reported incidents and use this information to update their risk assessments of TPSPs.

Response

53. Ongoing monitoring could result in differing responses by banks, including processes for incident management, renewal of contract or termination of a contract.

54. If the outcome of ongoing monitoring is not satisfactory or in case of a disruption of services provided by TPSPs, banks' monitoring should provide timely: (i) oversight of remediation actions by TPSPs, including 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.

55. 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.

56. When monitoring determines that a given TPSP is no longer a viable option and banks decide not to 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.

57. Banks should manage their dependencies on TPSP arrangements within their BCM processes. Banks' BCM processes 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, or deployment across different geographic 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 contingent providers.

58. Banks' BCM processes governing critical TPSP arrangements should include the provisions covered in paragraph 57 and those listed below:

- assurance from TPSPs that they develop and periodically review and update BCPs that set out clear and measurable indicators (eg RTOs and RPOs) that support banks' tolerance for disruption (refer to paragraph 41); and
- assurance testing by the bank (eg walkthroughs, tabletops and simulations) that the TPSP's BCM processes are robust.

59. For critical TPSP arrangement, banks should also consider joint design and testing of BCPs, or utilise an independent party or parties to do the same (refer to "Audits and assurance" in paragraph 14).

60. In cases where alternative TPSPs do not exist for critical services, banks' BCPs should address actions to be taken to ensure the continuity of the service.[33]

Termination

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

61. The *termination* stage is where banks manage planned or unplanned (unexpected) 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.

62. Banks should maintain appropriate and proportionate exit plans for planned terminations. 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.

[33] See POR Principle 5.

63. 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, handling of sensitive data, archiving and destruction of data, and system access revocation);
- adequate budget allocation; and
- clear identification of responsibilities to coordinate and manage the exit.

64. Banks' exit plans for the termination of critical TPSP arrangements should include the provisions covered in paragraph 63 and those listed below:

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

65. Banks should maintain appropriate and proportionate exit strategies for unplanned terminations for all TPSP arrangements taking into consideration the criticality and substitutability of the services provided. Although unplanned terminations may occur less frequently than planned terminations, they potentially pose more risks and banks should prepare for such events. Such exit strategies for unplanned termination should be based on plausible scenarios and reasonable assumptions.

66. Banks' exit strategies for the unplanned termination of critical TPSP arrangements should 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 and temporary workers) to transition the services.

Role of supervisors

Principle 10: Supervisors should evaluate third-party risk management as an integral part of ongoing assessment of banks.

67. 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 and support their operational resilience. Supervisory evaluations should cover the entire third-party arrangement life cycle. Emphasis should be placed on how banks integrate TPSP arrangements within their overall risk management processes (eg incident management, cyber security processes and BCM).

68. As certain TPSP arrangements may require specialised skills, supervisors should periodically evaluate the knowledge and skills of supervisory staff.[34]

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

Principle 11: Supervisors should analyse the available information to identify potential systemic risks, including those posed by the concentration of one or multiple TPSPs providing services to the banking sector.

69. Concentration of services provided by TPSPs, combined with other factors (eg lack of substitutability of TPSPs or TPSPs' access to banks' sensitive data), are relevant to the identification of systemic risks. To assess and monitor such risks across the banking sector, supervisors should be able to obtain information from banks on their arrangements with TPSPs.[35] The types of information supervisors could leverage include registers of TPSP arrangements; maps of interconnections and interdependencies;[36] 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 and data analytics). Based on the assessment, supervisors could further evaluate the potential systemic risk mitigation measures within their powers.

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

70. Bank supervisors should promote coordination and dialogue among themselves, supervisors of other sectors (eg FMIs, telecommunications, energy and data protection authorities) and relevant stakeholders to monitor systemic risk. Such collaboration may include a variety of efforts to support the resilience of critical infrastructure (eg industry- and/or supervisory-led business continuity exercises).

71. Additionally, collaboration may comprise: (i) appropriate cross-border coordination and cooperation mechanisms (eg enhancement of bilateral and multilateral memoranda of understanding, leveraging supervisory forums[37] and coordination related to cross-border incident management) fostering direct collaboration with critical TPSPs of 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 the cross-border resilience of critical and internationally active service providers (eg information-sharing, tabletop exercises, coordinated responses and recovery exercises, and joint examinations).

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

[36] See POR Principle 4.

[37] See Basel Core Principle 3.