Financial Stability Institute

Sound management of third-party risk – Executive Summary

Background

A third-party service provider (TPSP) is an entity or individual that performs services, activities, functions, processes or tasks directly for a bank.

Banks enter into formal arrangements with TPSPs for various reasons, including enabling access to specialised expertise, reducing costs and improving scalability, efficiency and operational resilience.

While such arrangements allow banks to focus on their core activities, they can also reduce banks' direct control over their operations and assets (including data) and may introduce new or increase existing risks. These risks include:

- **risks to critical services** – risks arising from disruption to a TPSP service that is critical to a bank's viability, critical operations or ability to meet key legal and regulatory compliance obligations
- **supply chain risks** – risks arising from disruption to a service provider that is part of a TPSP's supply chain (nth party) and is essential to the ultimate delivery of a critical service to a bank
- **concentration risk** – risk arising from a dependency of a bank on one or more services provided by a single TPSP or a limited number of TPSPs; such dependency may also occur at the banking or financial sector level, leading to systemic risk

Banks therefore need to have appropriate risk management of their TPSP arrangements to enhance their ability to withstand, adapt to and recover from operational disruption, and be able to mitigate the impact of potentially severe disruptive events.

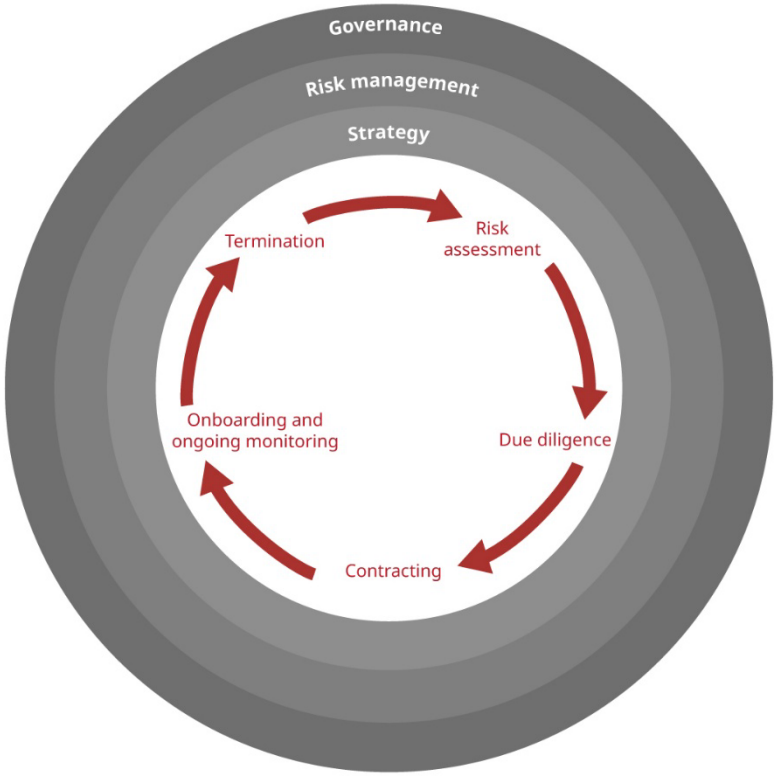
The Basel Committee on Banking Supervision (BCBS) Principles

In this context, the BCBS issued the *Principles for the sound management of third-party risk*.

The principles, which supersede the 2005 Joint Forum paper *Outsourcing in financial services* in respect of the banking sector, build on more recent BCBS publications, such as the *Principles for operational resilience* and the revised *Principles for the sound management of operational risk*.

The principles relating to the sound management of third-party risk follow the life cycle of a TPSP arrangement as illustrated in the following chart. 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.

Third-party arrangement life cycle



The principles seek to accommodate a diverse range of bank risk management practices and approaches and aim to promote international engagement, as well as greater collaboration and consistency, with a view to reducing regulatory fragmentation.

These principles are outlined in the following table. Principles 1 and 2 provide guidance on TPSP arrangements in relation to governance, risk management and strategy, which are integral to each stage of the TPSP life cycle. Principles 3–9 provide guidance on the effective management of TPSP risks at different stages of the life cycle: risk assessment, due diligence, contracting, onboarding, ongoing monitoring and termination. Principles 10–12 provide guidance for prudential supervisors.

Principle	Description
Governance, risk management and strategy	
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.
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.
Management of TPSP risks	
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.
4	Banks should conduct appropriate due diligence on a prospective TPSP prior to entering into an arrangement.
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.

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.
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.
8	Banks should maintain robust business continuity management to ensure their ability to operate in case of a TPSP service disruption.
9	Banks should maintain exit plans for planned termination and exit strategies for unplanned termination of TPSP arrangements.
Guidance for prudential supervisors	
10	Supervisors should evaluate third-party risk management as an integral part of ongoing assessment of banks.
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.
12	Supervisors should promote coordination and dialogue across sectors and borders to monitor systemic risks posed by critical TPSPs that provide services to banks.

Large internationally active banks and their prudential supervisors in BCBS member jurisdictions are the target of the principles. 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.

This Executive Summary and related tutorials are also available in FSI Connect, the online learning tool of the Bank for International Settlements.