



TOPICS:

Operational Risk

SOURCE:

Bank for International Settlements

BIS: Principles for the Sound Management of Third-Party Risk

- The Basel Committee's December 2025 publication introduces a comprehensive **framework for managing third-party service provider (TPSP) risk** in the banking sector, replacing the 2005 Joint Forum outsourcing paper. Recognising the increased reliance on TPSPs due to digitalisation and operational complexity, the document sets out **12 principles** - nine directed at banks and three at supervisors - structured around the TPSP arrangement lifecycle.
- Key principles require **banks** to embed third-party risk management (TPRM) into their **governance and risk strategy**, with boards holding ultimate responsibility for oversight. Banks must implement **a risk-based**, proportionate TPRM framework that evaluates the criticality and risk profile of TPSP arrangements throughout their lifecycle - covering risk assessment, due diligence, contracting, onboarding, monitoring and termination.
- **Contracts** must be legally binding, address key risks (e.g. resilience, data security, incident reporting) and include specific provisions for critical arrangements, including supply chain (nth party) risks.

Continuous **monitoring and reporting** of TPSP performance is mandated, especially for high-risk or critical services. Banks must maintain updated third-party registers, map interdependencies and manage concentration risk both at bank-level and sector-wide.

- The framework emphasises the need for robust business continuity management (BCM), with contingency plans and exit strategies for both planned and unplanned terminations. BCM must be tailored to the criticality of services and include scenario testing and joint resilience planning with TPSPs.
- For **supervisors**, the principles stress incorporating TPRM into ongoing supervisory assessments, analysing systemic risks arising from sector-wide reliance on certain TPSPs, and fostering cross-border and cross-sector collaboration. Supervisors are encouraged to collect information such as TPSP registers and interdependency maps, and to coordinate incident management strategies for critical service providers.

