Deloitte.

BCBS issues principles for the sound management of third-party risk

Initial perspectives on the Basel Committee on Banking Supervision's (BCBS) principle-based approach to aligning third-party risk management (TPRM) with business objectives for operational resilience

Center *for* Regulatory Strategy US

As the banking sector undergoes rapid digitalization, BCBS issued "*Principles for the sound management of third-party risk*" on July 9, 2024, with a comment period through October 9, 2024.[1] These principles are designed to address growing complexity from increased reliance on third-party service providers (TPSPs) and to strengthen the ability of banks to withstand, adapt to, and recover from operational disruption.

5 insights you should know

Board-level governance: The board of directors is ultimately responsible for the effectiveness of the third-party risk management (TPRM) framework and should hold senior management accountable to implement and communicate the TPRM vision. Leading governance practices should align the TPRM strategy and the overall risk profile of the TPSP portfolio. Keeping the board informed through regular reporting on areas of TPSP performance, risks, and mitigation can better enable them to validate that TPRM strategies and frameworks are functioning as intended.

Risk assessments and due diligence: Risk assessments should be iterative throughout the lifecycle of a service provider relationship and be based on financial, operational, and strategic importance of services provided. A proportionate level of due diligence when evaluating a TPSP and its own risk management capabilities can help align risk appetite to make more informed decisions. Assessment methodologies should consider known and potential risks as part of TPSP selection, including information security, supply chain, and concentration risks.

Contracting: Contracts provide institutions with the ability to hold TPSPs legally accountable to certain controls, restrictions, and obligations, while also providing clear guidance on the expectations, rights, and responsibilities of all parties in the arrangement. With the industry's rapid digitization, contractual arrangements are increasingly including covenants for information security, digital and physical access to assets, data protection and data processing locations, and handling of sensitive information. It's also important for banks to set clear standards for business continuity, disaster recovery, and incident notification.

Ongoing monitoring: Ongoing monitoring provides the lens into whether TPSPs consistently meet contractual, regulatory, and control standards. This risk-based process should be in-depth and adaptive, particularly when significant changes occur within the bank, TPSP, or external environment. Performance metrics and incident response times for critical situations are two key areas that enable timely regulatory reporting and continuity of services. Monitoring can better position banks to adapt their risk management practices, maintain a mapping of interdependencies, and foster third-party relationships that are compliant with bank policy.

Termination and contingency planning: TPSP contingency plans enable seamless transitions, whether for planned contract expirations or unplanned terminations due to disruption or inability of the TPSP to meet contractual requirements. Effective exit strategies should include aspects of financial, technical, and human capital considerations related to business continuity and risk mitigation. Regular updates to these strategies, along with adequate allocation of skills and resources, are important to adapt to changing circumstances and maintain operational resilience.

5 considerations to evaluate

1. **Strengthen board-level involvement in TPRM:** Engaging the board on material program decisions, escalations, and periodic reporting of risks and program performance is critical to sound management of third-party risk. Banks should look for opportunities to develop or improve, as appropriate, clearly defined roles and responsibilities; targeted trainings, independent program assessments; and day-to-day integration with business objectives and overall risk management processes, such as security controls and incident management. These capabilities should be supported by periodic reporting using approved metrics and timely communication with the board from cross-functional leaders.

2. **Perform third-party assessments in proportion to criticality and risk exposure:** A risk-based approach guides resources to areas of greatest risk and evaluates TPSPs in the context of business strategy, third-party strategy, and risk tolerance. While technology and analytics can help drive efficiencies throughout the third-party lifecycle, rapid digitization may introduce new risks; it is important to continuously evaluate and refine assessment methodologies to address these evolving challenges. Banks may consider expanding their assessment scope to look deeper into systemic importance, how security and resilience responsibilities are to be allocated, and potential for concentration risk in terms of over-reliance on a single provider.

3. **Augment contract management with risk mitigation procedures:** Regular, ongoing monitoring to proactively identify and manage third-party risks is an important practice to help confirm that the TPSP is performing as expected. To better meet leading TPRM practices, risk appropriate periodic reviews can help validate continued relevance of legally documented requirements, address contractual gaps and limitations with assessment activity, and apply additional perspective to measurement of factors such as specifications for uptime and performance; obligations under certain certifications; recovery time and recovery point objectives; and level of capability to resolve, monitor, or otherwise mitigate risks.

4. **Build a strong monitoring framework for resilience:** A strong approach to TPSP monitoring should incorporate cross-functional process integration; linkages of assessment work across risk domains; and orchestration of tools, metrics, and dashboarding that correlate analytics, artifacts, and testing outcomes into centralized visibility, ongoing reporting, case management, and prioritized alerting. Frameworks should be dynamic enough to assess how material changes or events may impact TPSP services and be able to validate that TPSPs are consistent in exercising and updating their controls accordingly.

5. **Connect contingency planning with pre-positioned response and recovery capability:** Contingency plans should address mitigating traditional risks related to a disruption or abrupt exit from a third-party relationship and incorporate strategies for meeting challenging timelines for transitioning services in-house or to alternative TPSPs. Banks should be prepared to rapidly respond, make timely determination as an incident unfolds, and potentially face simultaneous demands for continuity and reporting. Exercises, trainings, and supply chain simulation—together with TPSPs—can help strengthen resilience and highlight lessons for continuous improvement in risk management.

Deloitte.

A comparison of BCBS principles to US Interagency Guidance on third party risk

The BCBS principles, when compared to US Interagency Guidance released in June 2023,[2] provide fundamentally similar elements for sound management of third-party risk. BCBS expands the discussion in a few areas that banks can consider when positioning third-party risk programs for operational resilience.

Center *for* Regulatory Strategy US

Integration of TPRM with the three lines model

BCBS principles discuss the need for banks to **integrate third-party life cycles into the three lines model.** With clearly defined roles and responsibilities for each, the first line (e.g., the business) presumably owns, manages, and monitors day-to-day TPSP risks; the second line (e.g., risk functions) provides guidance and oversight across TPSP risk management activities; and the third line (e.g., internal audit) provides independent assurance and review of the TPRM program. Further, banks are encouraged to be forward-looking and **supplement qualifications and technical expertise of in-house staff, as necessary, to achieve an effective integration**.

Shared responsibility designed with clear delineation of roles

The principles emphasize that a **shared responsibility model in certain arrangements with TPSPs (e.g., cloud services) "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." Banks are advised to understand the delineation of internal controls and risk management (e.g., cyber and information and communication technologies (ICT)), monitor that both parties are meeting their obligations and responsibilities, factor shared responsibility situations into concentration risk, and maintain personnel able to assess these risk-types prior to and throughout the TPSP relationship.

Registers of TPSP arrangements including interconnectedness

The principles discuss a "**complete and up-to-date register of all TPSP arrangements," comprised of key elements** on TPSP criticality, substitutability of the TPSP's services, contingent providers, nature of proprietary or confidential information shared, and location(s), among others. Registers should be **updated periodically or when relevant changes occur**, such as new and different contractual terms, merger and acquisition activities that alter corporate structures, adjustments to service locations, or revisions to criticality determinations. BCBS calls for registers to be used in assessment through monitoring phases and in **mapping of TPSP dependencies and interconnectedness for the identification of TPSP concentration risk**.

Unavoidable concentration risk management

The principles offer **several risk mitigation approaches in situations where banks determine concentration risk to be unavoidable**. Proposed operational and risk management actions include enhanced monitoring, more frequent validation of controls, geographic diversification in the provision of critical services, on-hand alternatives to existing TPSPs, and combined configurations of on-premise infrastructure with TPSP services. Discussion involves the use of **scenario and data-driven analytic models in assessment activity** and implies that banks should **be prepared to share supporting concentration risk analysis** with regulators, if requested.

Cross-sector/border collaboration

BCBS outlines ways to explore dialogue with a broader range of stakeholders across sectors and borders as part of resilience planning and efforts to evaluate for systemic risk. A range of collaboration approaches, from participation in **cross-border information-sharing forums and tabletop exercises** under bilateral and multilateral memoranda of understandings (MoUs) to the coordination of capabilities among relevant stakeholders to **support an ecosystem of business continuity,** focus on fostering direct **collaboration with critical TPSPs that provide services in multiple jurisdictions.**

Endnotes

[1] Bank for International Settlements (BIS), Basel Committee on Banking Supervision (BCBS), "Principles for the sound management of third-party risk," July 6, 2024.

[2] Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC),"Interagency Guidance on Third-Party Relationships: Risk Management," *Federal Register*, June 9, 2023.

Connect with us

Richard Rosenthal
Principal
Deloitte & Touche LLP
rirosenthal@deloitte.com

Suzanne Denton
Managing Director
Deloitte & Touche LLP
sudenton@deloitte.com

Laura Laybourn
Managing Director
Deloitte & Touche LLP
llaybourn@deloitte.com

Dave Beckman
Senior Manager
Deloitte & Touche LLP
dbeckman@deloitte.com

Tara Wensel
Senior Manager
Deloitte & Touche LLP
tawensel@deloitte.com

Will Beech
Manager
Deloitte & Touche LLP
wibeech@deloitte.com

Deloitte Center for Regulatory Strategy, US

Irena Gecas-McCarthy
FSI Director, Deloitte Center for Regulatory Strategy, US
Principal
Deloitte & Touche LLP
igecasmccarthy@deloitte.com

Aaron Salerno
Manager
Deloitte Services LP
asalerno@deloitte.com

Kyle Cooke
Manager
Deloitte Services LP
kycooke@deloitte.com