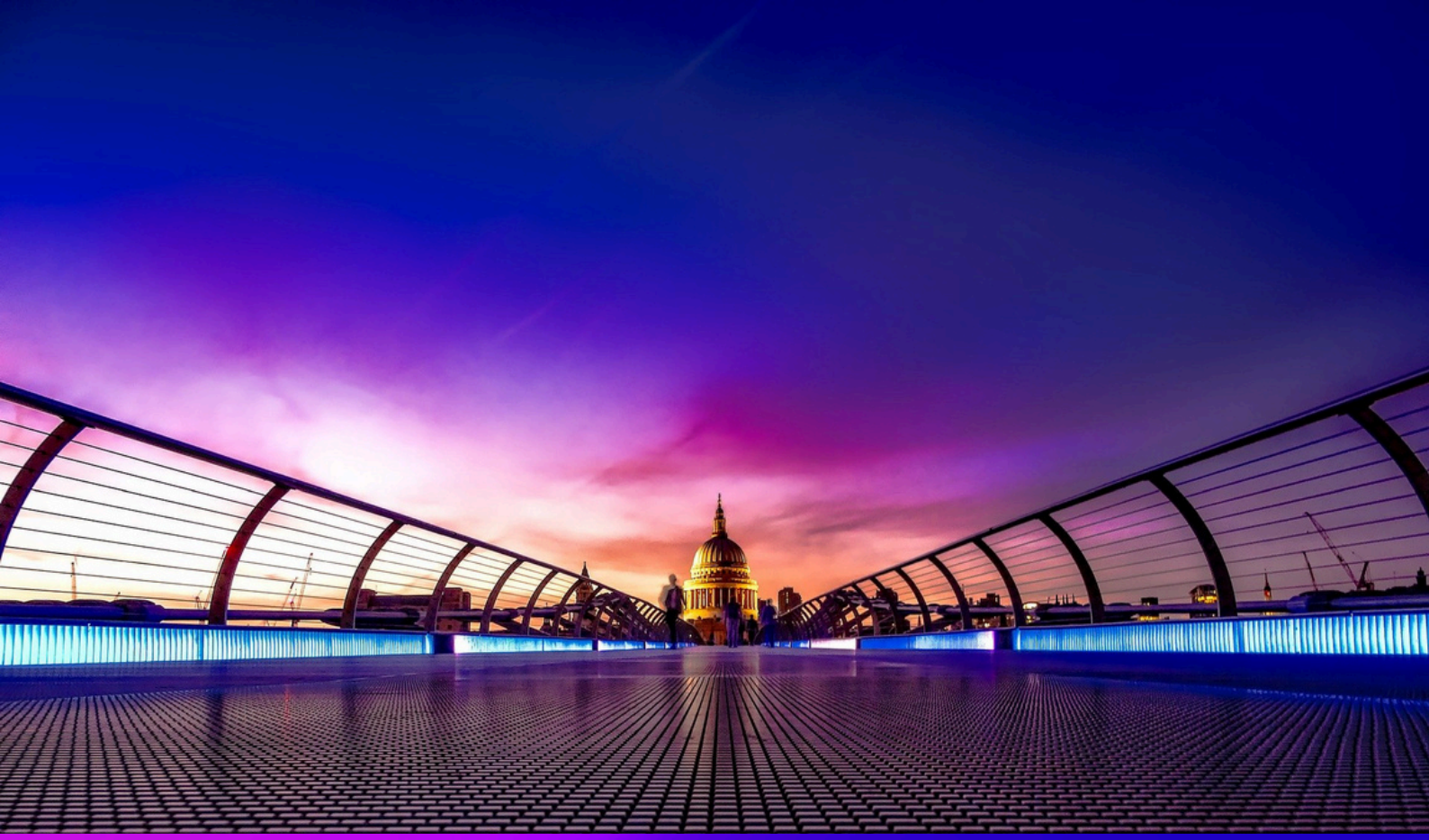

Third-Party Risk in a New Era: What the Basel Committee Principles Mean for UK Banks

Lawrence Hicks, Steph Stylianou and Marco Collina

Be SHAPING THE FUTURE

Introduction

Over the past decade, rapid **digitalisation, cloud adoption, fintech partnerships and specialised service providers** have made third-party service providers integral to banking operations. These relationships enable innovation but also introduce **operational, cyber, concentration and systemic risks** that go well beyond traditional outsourcing. Earlier guidance, such as the 2005 Joint Forum Outsourcing paper, was too narrow for today's interconnected supply chains. As **non-outsourcing third-party relationships** (e.g., data providers, software platforms, cloud services) have grown in importance, regulators have shifted toward broader, lifecycle-based supervisory models.

Supervisors have therefore shifted to broader, lifecycle-based expectations. In the UK, the PRA's SS2/21 Outsourcing and Third-Party Risk Management emphasises **governance, materiality, proportionality** and **end-to-end oversight**, recognising that third-party risk is a core element of operational resilience. Reflecting this increased scrutiny, the Basel Committee on Banking Supervision (BCBS) in July 2024 launched a consultation on the principles for the sound management of third-party risk in its role as an international standard setter for banking regulation and supervision.

This article will explore the finalised principles for the sound management of third-party risk published in December 2025 and explore how these could impact UK banks.

Consultation

To modernise global expectations, the Basel Committee on Banking Supervision (BCBS) issued a consultive paper on 9 July 2024: Principles for the Sound Management of Third-Party Risk.

The consultation aimed to:

- Establish a global, high-level framework covering all forms of third-party dependency, not just outsourcing.
- Provide a common baseline adaptable across jurisdictions.
- Ensure guidance is technology-agnostic, allowing flexibility as technologies evolve.
- Encourage supervisory alignment while enabling jurisdictional tailoring.

Industry participation

The consultation involved a wide range of market participants including Amazon Web Services, Google, Microsoft, BlackRock, Euroclear, Euronext etc. (Bank of International Settlements, 2024), reflecting strong industry recognition that modern third-party risk requires globally consistent oversight.

Proposed principles

The BCBS proposed 12 high-level principles structured in two groups (Lovegrove, 2024):

- **Principle 1-9: Guidance for banks** on governance, risk assessment, due diligence, contracting, onboarding, ongoing monitoring, business continuity, and exit strategy.
- **Principle 10-12: Guidance for supervisors** on evaluating banks' practices, identifying systemic concentration risks, and fostering cross-border cooperation.

Set out below is a summary of each of the 12 principles and their key requirements:

- **Principle 1 - Board Accountability:** The board is ultimately responsible for oversight of all third-party arrangements. It must approve a clear third-party strategy aligned to the bank's risk appetite and tolerance for disruption.
- **Principle 2 - Senior Management Execution:** Senior management is responsible for implementing the third-party risk management framework (TPRMF), ensuring policies, controls, reporting and escalation mechanisms operate effectively across the third-party lifecycle.
- **Principle 3 - Risk Assessment:** Banks must conduct comprehensive and ongoing risk assessments before entering into, and throughout, third-party arrangements. This includes assessing criticality, substitutability, data sensitivity, concentration risk and alignment with the bank's risk appetite.
- **Principle 4 - Due Diligence:** Banks should perform proportionate due diligence on prospective third parties to assess their operational capability, financial soundness, risk management, resilience, compliance posture and ability to manage their own supply chains (nth parties).
- **Principle 5 - Contracting:** All third-party arrangements should be governed by clear, legally binding contracts. Contracts must define roles, responsibilities, performance standards, audit and access rights, incident reporting, business continuity obligations, data ownership and exit provisions, especially for critical services.
- **Principle 6 - Onboarding:** Banks should allocate sufficient resources to ensure smooth onboarding, resolve due-diligence findings, update third-party registers and map dependencies.
- **Principle 7 - Ongoing Monitoring:** Banks must continuously monitor third-party performance, risk profile and criticality, including changes affecting the third party or its supply chain. Issues should be escalated, reported to senior management and addressed promptly.

- **Principle 8 - Business Continuity Management:** Banks must integrate third-party dependencies into their business continuity and disaster recovery planning. This includes testing scenarios involving third-party disruption, ensuring alignment with the bank's tolerance for disruption, and validating third-party service providers' (TPSPs) own continuity capabilities.
- **Principle 9 - Termination and Exit:** Banks should maintain documented and tested exit plans for both planned and unplanned termination of third-party arrangements. Exit strategies must ensure continuity of critical services, data portability, knowledge transfer and minimal disruption.
- **Principle 10 - Supervisory Assessment:** Supervisors should treat third-party risk management as a core part of their ongoing assessment of banks, evaluating governance, lifecycle controls and integration with operational resilience frameworks.
- **Principle 11 - Systemic Concentration Risk:** Supervisors should analyse information across banks to identify systemic risks arising from concentration in critical third-party providers, particularly where substitutability is limited.
- **Principle 12 - Cross-Border and Cross-Sector Coordination:** Supervisors should promote coordination and information-sharing across jurisdictions and sectors to monitor and manage systemic risks posed by critical third-party service providers operating globally.

Key themes

- Adoption of a full lifecycle approach to third-party risk management.
- Recognition of criticality, materiality and concentration risks, including risks arising from "nth-party" (a service provider that is part of a third-party service provider's supply chain) suppliers across the wider supply chain.
- Reinforcement of robust governance, clear board accountability, and proportionate risk-aligned controls.

Final principles

Published on 10 December 2025, the final BCBS Principles for the Sound Management of Third-Party Risk, replaced earlier outsourcing guidance (e.g. 2005 Joint Forum Framework) with a modern, comprehensive and technology-agnostic framework.

What the Final Twelve Principles Achieve

- Establishes a common global baseline covering all forms of third-party relationships beyond traditional outsourcing.
- Mandates a lifecycle approach in which banks manage risk across every stage of the relationship (selection, onboarding, contracting, monitoring, stress testing and exit).
- Highlights key operational vulnerabilities, such as concentration risk, deeper supply-chain (nth-party) dependencies, and potential systemic impacts.
- Reinforces board-level accountability for third-party/operational resilience outcomes.
- Equips supervisors with guidance for assessing banks' frameworks and enhancing cross-jurisdictionally coordination on common third-party exposures.

Key changes from the 2024 Consultation to the 2025 final principles

The final document largely retained the structure and intent of the 2024 consultation, but introduced important classifications, refinements and targeted enhancements reflecting both industry feedback and supervisory priorities.

- **Clearer focus on technology-agnostic and risk-based application:** While the consultation already signalled flexibility, the final principles more explicitly confirm that the framework is technology-agnostic and intended to remain relevant as technologies evolve. The final text reinforces that requirements should be applied based on risk and criticality, rather than the specific technology or delivery model (e.g. cloud, AI-enabled services), helping future-proof the framework.
- **Sharper articulation of proportionality and criticality:** The final principles sharpen how proportionality should operate in practice, distinguishing more explicitly between:
  - standard third-party service provider (TPSP) arrangements[CC1] [MC2] ,
  - higher-risk arrangements, and
  - **critical third-party service provider (TPSP) arrangements**, which attract enhanced expectations.

The consultation referenced proportionality throughout, but the final document provides more explicit guidance on applying heightened controls not only to critical services, but also to arrangements that materially increase bank-level concentration risk, even if individual services are not critical.

- **Strengthened expectations on concentration and systemic risk:** In response to consultation feedback, the final principles strengthen expectations around **bank-level concentration risk** and provide clearer guidance on how banks should assess dependencies across providers, regions and supply chains. The supervisory role in monitoring **systemic concentration risk** is also more clearly distinguished from banks' own responsibilities, reinforcing a coordinated, cross-jurisdictional approach.

- **More explicit requirements for registers and dependency mapping:** While third-party registers were already included in the consultation, the final principles provide more detail on:
  - the **minimum information** expected in third-party service provider (TPSP) and key nth-party registers (e.g. substituability, service, data locations, LEIs where available), and
  - the use of registers for **dependency mapping and concentration analysis.**

This reflects supervisory feedback that inventories should be decision-enabling, not merely compliance artefacts.

- **Refined approach to nth-party and supply-chain risk**: The consulation introduced the concept of nth-party, but the final principles go further by:
  - narrowing the definition of **key nth parties** to those essential to the delivery of critical services, and
  - clarifying when banks should require third-party service providers (TPSPs) to cascade contractual obligations and incident reporting to those parties.

This introduces greater practicality and avoids imposing blanket supply-chain obligations where risk does not justify them.

- **Clearer supervisory roles and greater international consistency**: The final principles strengthen the articulation of supervisors' responsibilities under principles 10–12, particularly around:
  - cross-border cooperation,
  - information sharing on common third-party service providers (TPSPs), and
  - monitoring systemic exposures.

This reinforces the Basel Committee's objective of **global regulatory consistency**, and signals reduced fragmentation across jurisdictions compared with the consultation draft.

The December 2025 principles do not represent a change in direction from the 2024 consultation. Instead, they **tighten, clarify and operationalise** the framework addressing concerns around proportionality, feasibility and futureproofing while strengthening global consistency and supervisory coordination.

What does this mean for the banking sector?

The Basel principles complement and, in some areas, extend the PRASS2/21 expectations.

Reinforced Expectations

- Stronger board accountability and governance of third-party risk.
- Demonstrable lifecycle management, including evidence of risk assessment, due diligence and ongoing monitoring.
- More robust contracts with access, audit and data provisions.
- Increased emphasis on the substitutability of critical services.

Expanded or Elevated Expectations

- Deeper concentration risk analysis at bank-level and sector-level.
- Heightened scrutiny into supply-chain (nth-party) dependencies.
- Thorough, tested exit strategies for both planned and unplanned scenarios.
- Enhanced resilience testing, particularly for major cloud and IT providers.

What UK Regulators Will Focus On

UK banks should anticipate increased supervisory scrutiny of:

- Accuracy and completeness of third-party inventories and registers.
- Maturity of supply-chain mapping for critical technology and cloud services.
- Contractual adequacy regarding supervisory access, audit and data portability.
- Depth and frequency of BCP and DR testing with major third-party service providers (TPSPs).
- Ability to operate through outages of key third-party service providers (TPSPs).

Global Regulatory Consistency

A core aim of the Basel Committee is core purposes is global regulatory convergence. Banks should therefore expect greater alignment across the PRA, EBA, FSB and other authorities, reducing the need for multiple, jurisdiction-specific frameworks.

Conclusion

The Basel principles modernise third-party risk standards, promoting consistent, tech-agnostic oversight to strengthen resilience and reduce regulatory fragmentation.

Banks should begin assessing readiness now. We stand ready to support firms across interpretation, design and implementation.

About us

Be | Shaping the Future is a leading pan-European financial services management consultancy, operating in 13 countries across Europe.

We are a disrupter to the top-tier consultancy brands, trusted by five out of ten of Europe's leading banks (alongside other leading financial institutions and FinTechs).

We are one of the fastest growing consultancies with dedicated specialist teams in:

- Retail and commercial banking
- Capital markets
- Cards and payments
- Risk, regulatory and compliance
- Finance & CFO advisory
- ESG

At Be UK, we've worked with a range of financial services firms to help design, implement, and enhance scenario testing frameworks.

Our team brings a wealth of experience in operational resilience, data strategy, and regulatory compliance equipping us to support firms wherever they are on their journey, whether it's improving cross-team collaboration, modernising testing methods or unlocking the value of data, we're here to help firms turn insight into action.

Utilising our broad experience from across the banking sector, we ensure our clients take advantage of market disruption to achieve lasting value.

Bringing deep industry expertise and expert consulting capabilities, we support our clients to tackle their biggest opportunities and challenges to deliver fundamental and enduring change to their businesses.

Contact

For more information on how we can help you on your risk journey, please get in touch.

Lawrence Hicks
Associate Partner - Non-Financial Risk
E: l.hicks@beshapingthefuture.co.uk
T: +44(0) 7891473391

Steph Stylianou
Manager - Non-Financial Risk
E: s.stylianou@beshapingthefuture.co.uk
T: +44(0) 7557678506

Marco Collina
Senior Consultant - Banking & capital markets
E: m.collina@beshapingthefuture.co.uk
T: +44(0) 7538032205