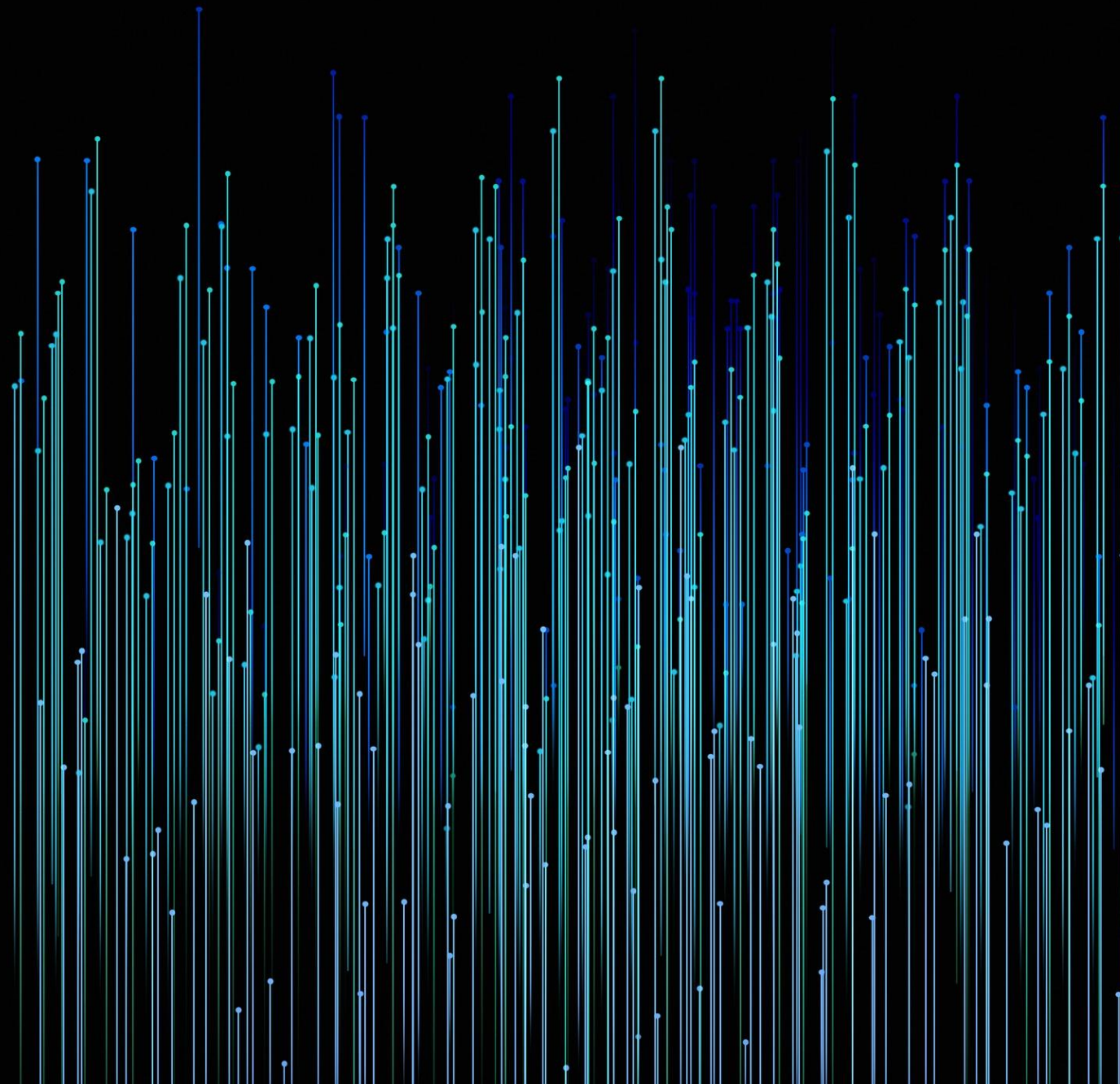
REPLY AVANTAGE

BCBS Principles for the Sound Management of Third-Party Risk



December 2025

FT FINANCIAL TIMES statista | UK'S LEADING MANAGEMENT CONSULTANTS 2025

REPLY AVANTAGE

Table of Contents

1. Overview and Background

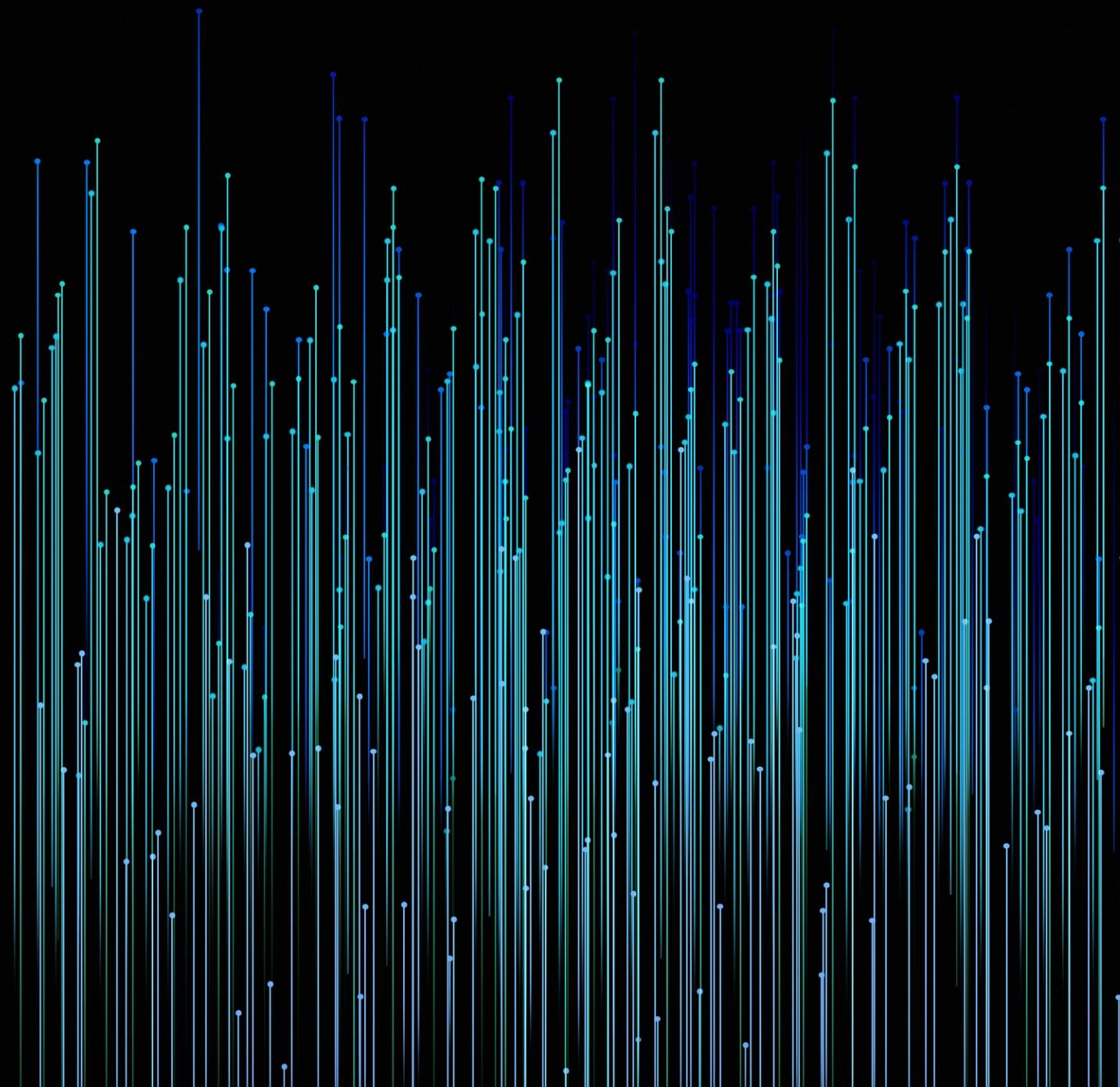
2. Why Do These Principles Matter?

3. How the Principles Are Structured

4. Concepts Across the Third-Party Arrangement Lifecycle

5. Potential Challenges and Industry Risks

6. Appendix: The Principles in Detail



An Overview and Background

The Basel Committee on Banking Supervision (BCBS) published Principles for the Sound Management of Third-Party Risk in the banking sector (the Principles) in December 2025. The Principles supersede the BCBS 2005 paper on outsourcing in the banking sector, expanding the scope from traditional outsourcing to broader third-party service provider (TPSP) arrangements driven by digitalisation, innovation, and increased dependencies.

Why Were These Principles Needed?

Expanded Reliance on Third Party

- The 2005 BCBC paper focused primarily on outsourcing as a subset of third-party arrangements.
- Banks increasingly depend on TPSP to access specialist expertise, improve efficiency and scalability, enhance resilience, and focus on core activities.
- Digitalisation and fintech growth have expanded third-party reliance, introducing amplified risks (e.g., concentration, supply chain, and technology threats), requiring supervisory attention on all third-party arrangements, not just outsourcing.

Overview

Scope and Applicability

- Applied to large, internationally active banks operating in BCBS member jurisdictions, though they may also be beneficial for others.
- Directed at both banks and prudential supervisors, establishing expectations for firms and oversight authorities.
- Covers all TPSP arrangements, extending beyond traditional outsourcing.
- Includes intragroup service providers where they function as third parties.

Regulatory Intent and Approach

- Promotes a principles-based third-party risk management (TPRM) framework.
- Designed to be applied on a proportionate, risk-based basis, reflecting each bank's size, complexity and risk profile.
- Technology-agnostic, ensuring relevance across cloud, digital, data and emerging technology services
- Complements operational risk management and builds on existing Basel standards to strengthen banks' ability to withstand, adapt to and recover from operational disruption, with significant overlap with the DORA framework.

Main Changes

- The 2025 Principles cover the wider universe of TPSP arrangements than the 2005 paper
- The new Principles adopt a full lifecycle approach (risk assessment to termination) to TPRM and introduce key concepts such as criticality, proportionality, supply chain (nth-party) risk and concentration risk.
- The updated Principles include specific guidance for prudential supervisors on systemic and cross-border risks
- Terms necessary and relevant from a banking perspective are specifically defined to ensure common understanding, clarity, and consistency.

Why Do These Principles Matter?

The Basel Committee has reframed TPRM, evolving from traditional outsourcing oversight to a comprehensive, system-wide approach focused on operational and financial sector resilience.

Third-party risk is now a primary determinant of operational resilience.

Banks' ability to deliver critical services increasingly depends on external providers, making third-party resilience inseparable from enterprise resilience.

The principles reflect a structural shift from outsourcing to ecosystem dependency.

Modern banking operates through interconnected third-party and supply-chain ecosystems, where concentration, substitutability and systemic exposure are central risk considerations.

Accountability is explicitly reaffirmed at board and senior management level.

The framework reinforces that risk ownership remains with the bank, irrespective of delivery model, contractual arrangements or shared-responsibility constructs.

Supervisory scrutiny is expanding from individual firms to shared infrastructure.

Heightened focus on concentration risk and critical TPSPs signals a move toward monitoring vulnerabilities that can propagate across institutions and markets.

Third-party risk management is positioned as a strategic enabler, not a compliance exercise.

Effective governance, resilience and exit readiness are framed as prerequisites for safe innovation, scalability and sustained use of advanced technologies.

How the Principles Are Structured

The Principles are organised into 12 principles that operate as a coherent framework rather than as standalone requirements. They are structured around the TPSP arrangement life cycle, divided into five key analytical groupings, with governance embedded throughout.

Governance, Risk Management and Strategy (Principles 1-2)

- Establishes clear accountability, with the **board retaining ultimate responsibility** for oversight, strategy, risk appetite and tolerance.
- Positions TPRM as a **strategic capability aligned to the bank's business model, operating strategy and resilience objectives**.
- Requires **senior management to translate strategy into effective policies, controls and reporting**, ensuring third-party risks are visible, managed and escalated appropriately.

Risk Assessment, Due Diligence and Contracting (Principles 3-5)

- Ensures third-party arrangements are **informed**, e.g. criticality, concentration risk and potential impact on operations are considered.
- Differentiates between assessing the risk of the service and the specific capabilities, resilience and financial soundness of the provider.
- Uses **contractual design as a primary risk-control mechanism**, embedding performance, resilience, access, audit and exit rights.
- Places **heightened expectations on critical third-party arrangements**, including supply-chain transparency.

Onboarding and Ongoing Monitoring (Principles 6-7)

- Focuses on operationalising TPRM, ensuring providers are fully integrated into the bank's control environment.
- Requires **continuous monitoring of performance, incidents, financial health and changes** in risk or criticality throughout.
- Emphasises **timely escalation, reporting and remediation where risks materialise or assumptions change.**
- Treats third-party risk as dynamic, requiring **regular reassessment** rather than static compliance.

Business Continuity and Termination (Principles 8-9)

- Recognises **disruption and provider failure as plausible scenarios that must be actively planned for**, not exceptional events.
- Requires banks to **embed third-party dependencies into business continuity and disaster recovery planning**, supported by regular testing and assurance.
- Mandates **credible, proportionate exit plans** for both planned and unplanned termination, particularly for critical services.

Role of Supervisors (Principles 10-12)

- Expands **supervisory focus from firm-level controls to system-wide dependencies** on critical TPSPs.
- Highlights **concentration risk as a potential source of systemic vulnerability**, requiring aggregation and analysis across institutions.
- **Promotes cross-border and cross-sector coordination** to address shared dependencies on common infrastructure and service providers.

Principles for banks Principles for prudential supervisors

Concepts Across the Third-Party Arrangement Lifecycle

Effective TPRM is a continuous, iterative cycle from assessment to termination. Controls must match each TPSP's risk. Insights from any stage should refine the entire process, underpinned by core principles across all stages.

Proportionality

- TPRM should reflect a bank's size, complexity, business model and the risk and criticality of the arrangement.
- While approaches in applying these Principles may differ between banks, proportionality does not justify exempting a TPSP arrangement from appropriate risk management.

Criticality

- Banks should apply comprehensive oversight and more rigorous risk management where TPS arrangements support critical services.
- Assess arrangements that contribute to concentration risk, where disruption across non-critical services could threaten viability, critical operations, or regulatory compliance.

Concentration

- Banks are responsible for identifying, monitoring and managing concentration risk within their own arrangements, while supervisors monitor systemic concentration risk.
- Banks should also assess the relative systemic importance of TPSPs, based on available reliable information

Intragroup TPSP Arrangements

- Banks should not assume intragroup third-party arrangements are inherently lower risk.
- Apply proportionate risk management reflecting the risks and criticality of the intragroup arrangement such as level of control and cross-border complexities.

Nth Parties and Supply Chains

- Banks should apply proportionate risk management to identify, monitor and manage risks from complex/lengthy supply chains.
- For higher-risk or critical arrangements, ensure their contracts and risk standards extend to key subcontractors.

New or Advanced Technologies

- The rapid adoption of new and advanced technologies has increased banks' reliance on TPSPs, potentially amplifying existing risks and introducing new ones.

Audits and Assurance

- Banks may rely on multiple audits and assurance sources when conducting due diligence and ongoing monitoring of TPSPs, including independent, pooled, or TPSP-commissioned audits, as well as industry certifications and standards.

Potential Challenges and Industry Risks

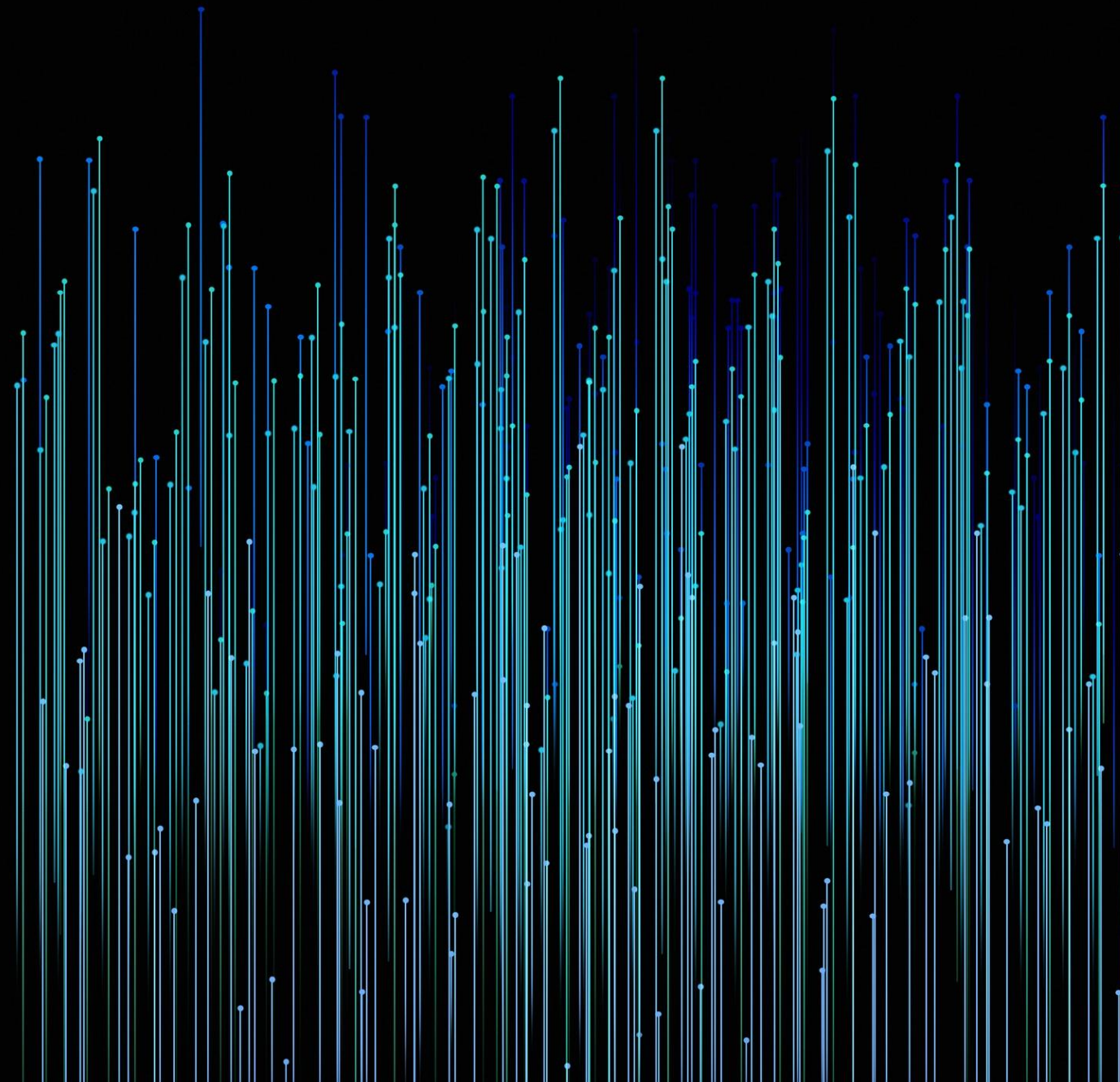
This overview outlines the potential implementation hurdles and systemic risks banks face under the proposed principles.

Operational Complexity	Implementing a proportional yet comprehensive lifecycle management framework across diverse TPSP arrangements will be a significant operational challenge.
Systemic Concentration Visibility	Banks can map their own dependencies but have limited insight into peer exposures and overall market substitutability, which limits their ability to assess sector-wide concentration risk.
Nth-Party Control Limitations	Expectations for material nth-party dependencies (cascading obligations, information rights for critical arrangements) remain challenging due to control degradation beyond Tier 1 vendors. Enforcement in complex chains is difficult, though EU banks have often already negotiated sub-outsourcing clauses under EBA rules.
Contractual Rigor	Securing cascading requirements, nth-party audit/access, incident reporting, and robust exits can still test leverage with dominant providers. However, for EU banks, much of this rigor was already required under the 2019 EBA Guidelines, reducing incremental burden compared to non-EU jurisdictions.
Regulatory Overlap and Fragmentation	These principles build on existing regimes (e.g., operational resilience, ICT risk). Without harmonization, banks face duplicate governance, inconsistent processes, and repeated assurance requests.
Trade-offs with Innovation	Stronger assurance, resilience testing, and exit planning requirements can slow the adoption of new technologies and may disadvantage smaller providers, potentially increasing market concentration.
Resource Intensity	Developing in-house expertise (particularly for emerging technologies), conducting thorough due diligence, and maintaining continuous monitoring demand significant budgets and skilled staff.

REPLY AVANTAGE

Appendix

The Principles in Detail



Governance and Strategy: Principles 1 - 2

Establishing clear accountability and strategic ownership of third-party risk at board and senior management level.

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.

In practice:

- Confirms that accountability for third-party risk sits unequivocally with the board, regardless of whether services are performed internally or by third parties.
- Requires board approval of a third-party risk management strategy, aligned with the bank's overall business and risk management strategies.
- Mandates explicit articulation of risk appetite and tolerance for disruption arising from TPSP arrangements, including those supporting critical services.
- Reinforces that use of TPSPs must not impair the bank's ability to operate in a safe and sound manner or meet legal and regulatory obligations.

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.

In practice:

- Requires senior management to operationalise the board-approved strategy through a comprehensive third-party risk management framework (TPRMF).
- Expects clearly defined policies, procedures, roles and responsibilities covering the full TPSP life cycle.
- Mandates regular, structured reporting to the board on TPSP performance, risk exposures, incidents and concentration risks.
- Requires timely escalation of issues and visibility of mitigating actions, ensuring the board can exercise effective oversight and challenge

Summary

- Third-party risk management is positioned as a **strategic governance issue**, not a purely operational or procurement concern.
- **Accountability** for risk outcomes **remains with the bank**, including in **shared-responsibility** and **intragroup arrangements.**
- **Effective governance** depends on strong information flows, escalation mechanisms and management accountability, **proportionate to risk and criticality**.

Risk Assessment, Due Diligence & Contracting: Principles 3 - 5

Embedding risk-based decision-making and enforceable controls before entering third-party arrangements.

Principle 3

Banks should perform a comprehensive risk assessment under the third-party risk management framework (TPRMF) to evaluate and manage identified and potential risks both before entering into and throughout the life cycle of a third-party service provider (TPSP) arrangement.

In practice:

- Requires banks to identify and assess the types and levels of risk associated with a TPSP arrangement, alongside the criticality of the services provided.
- Explicitly calls out risks arising from concentration, long or complex supply chains, new or advanced technologies, and other financial and non-financial risks.
- Requires assessment of the impact of disruption, including tolerance for service unavailability, sensitivity of data shared, and substitutability of services.
- Mandates that risk assessments are documented and iterative, informing decisions both at inception and throughout the life cycle.

Principle 4

Banks should conduct appropriate due diligence on a prospective TPSP prior to entering into an arrangement.

In practice:

- Requires banks to assess whether a specific TPSP has the capacity and capability to deliver the services in line with the bank's objectives and regulatory obligations.
- Mandates evaluation of the TPSP's operational resilience, internal controls, cyber and ICT risk management, and ability to manage supply-chain and nth-party risks.
- Requires consideration of financial soundness, geographic dependencies, conflicts of interest, litigation history and availability of alternative providers.
- Explicitly requires banks to weigh the relative benefits and costs, including the feasibility and risks of exit, transition or insourcing.

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.

In practice:

- Positions contracts as a core risk-control mechanism, translating risk assessments and due diligence outcomes into enforceable obligations.
- Requires contracts to address performance standards, access and audit rights, information and incident reporting, security and resilience, and data and asset ownership.
- Mandates clear provisions for business continuity, disaster recovery, termination and exit, aligned to the bank's risk appetite and tolerance for disruption.
- Imposes heightened contractual expectations for critical TPSP arrangements, including requirements relating to key nth parties and supervisory access.

Summary

- Establish a structured, evidence-based basis for deciding **whether and how** to enter TPSP arrangements.
- Clearly distinguish between **service-level risk** (what is being outsourced) and **provider-level risk** (who delivers it).
- Reinforce that effective third-party risk management begins **before contracts are signed**, not after services commence.
- Embed resilience, transparency and exit readiness into the design of TPSP arrangements from the outset.

Onboarding and Ongoing Monitoring: Principles 6 - 7

Operationalising third-party risk management through continuous oversight, escalation and reassessment.

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.

In practice:

- Requires banks to ensure that TPSPs have a clear understanding of the bank's policies, processes, technology, facilities and interdependencies necessary to deliver the contracted services.
- Emphasises resolution of residual risks or issues identified during due diligence or contract negotiation before services become fully operational.
- Mandates updating of TPSP registers and dependency mapping at onboarding, ensuring visibility of criticality, interconnections and supply-chain dependencies.
- Reinforces that onboarding is a risk-critical transition point, not a purely operational or administrative step.

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.

In practice:

- Requires continuous monitoring of TPSP performance, control effectiveness and ability to meet contractual obligations, including service levels and resilience standards.
- Mandates monitoring of material changes in risk, including incidents, financial deterioration, security breaches, data loss, service interruptions and compliance issues.
- Requires regular reassessment of risk and criticality, particularly where there are changes to the bank, the TPSP, key nth parties or the external operating environment.
- Expects timely escalation, reporting and remediation, with clear oversight by senior management and the board.

Summary

- Treat third-party risk as **dynamic**, **requiring continuous reassessment** rather than reliance on point-in-time controls.
- Reinforce the importance of **up-to-date registers**, **interdependency mapping** and **concentration risk monitoring** throughout the life of the arrangement.
- **Embed third-party monitoring** into the bank's broader governance, risk management and incident response **frameworks**.
- Ensure that third-party performance and risk remain **visible**, **actionable** and **challengeable** at senior management and board level.

Business Continuity Management and Termination Planning: Principles 8 - 9

Ensuring resilience through disruption preparedness, recovery capability and credible exit readiness.

Principle 8

Banks should maintain robust business continuity management to ensure their ability to operate in case of a TPSP service disruption.

In practice:

- Requires banks to embed TPSP dependencies within their business continuity management (BCM) framework, rather than treating third-party disruptions as external events.
- Mandates development, regular review and testing of business continuity plans (BCPs) and disaster recovery plans (DRPs) covering TPSP arrangements.
- Requires banks to consider a range of recovery strategies, including alternative providers, geographic diversification, insourcing and compensating controls.
- Expects banks to incorporate lessons learned from incidents and resilience testing into ongoing BCM enhancements.

Principle 9

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

In practice:

- Requires banks to maintain appropriate and proportionate exit plans, aligned to the criticality and substitutability of the services provided.
- Distinguishes clearly between planned termination (e.g. contract expiry or strategic change) and unplanned termination (e.g. provider failure, regulatory breach or severe disruption).
- Mandates that exit plans address operational, legal, financial and resource considerations, including budget, technical infrastructure, data access and knowledge transfer.
- Requires exit plans to be regularly updated and tested, ensuring they remain credible and executable.

Summary

- Treat service disruption and provider failure as **plausible scenarios** requiring proactive planning.
- Reinforce that reliance on TPSPs must not compromise the bank's **operational resilience or ability to meet regulatory obligations.**
- Position continuity and exit readiness as **core components of third-party risk management**, not last-resort controls.
- Retain full accountability for safe, orderly continuity and termination with the bank.

Role of Supervisors: Principles 10-12

Strengthening system-wide resilience through supervisory oversight, concentration risk analysis and cross-border coordination.

Principle 10

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

In practice:
- Positions third-party risk management as a core component of prudential supervision, rather than a standalone or specialist topic.
- Requires supervisors to assess banks' third-party risk management frameworks in the context of their overall governance, operational risk management and operational resilience.
- Expects supervisory reviews to cover the full TPSP life cycle, including risk assessment, monitoring, incident management and exit preparedness.
- Recognises the need for supervisors to maintain sufficient expertise and capability to assess increasingly complex third-party arrangements.

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.

In practice:
- Shifts supervisory focus beyond individual institutions to sector-wide dependencies on common third-party service providers.
- Requires supervisors to leverage information such as TPSP registers, interdependency maps, incident reports and recovery plans to assess systemic concentration risk.
- Recognises that lack of substitutability, access to sensitive data and reliance on common infrastructure can amplify systemic vulnerabilities.
- Encourages the use of supervisory analytics, scenario analysis and aggregation of firm-level data to identify emerging risks.

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.

In practice:
- Acknowledges that many critical TPSPs operate across jurisdictions and sectors, beyond the reach of any single supervisor.
- Promotes cross-border and cross-sector coordination, including with authorities overseeing financial market infrastructures, telecommunications, energy and data protection.
- Encourages information-sharing, joint exercises and coordinated responses to incidents involving critical TPSPs.
- Supports the development of collective supervisory capability to enhance the resilience of globally important service providers.

Summary

- Reflect a shift from firm-level outsourcing oversight to **system-wide resilience supervision**.
- Recognise **third-party concentration** as a potential source of **systemic risk**, not just an individual-bank issue.
- Reinforce the importance of **data**, **transparency** and **coordination** in managing shared dependencies.
- Position **supervisors** as **key actors** in **monitoring** and **mitigating risks** arising from critical third-party ecosystems.

FT FINANCIAL TIMES
statista
UK'S LEADING MANAGEMENT CONSULTANTS 2025