

Workshop 6

Building operational strength in an era of constant disruption

Chair: Fernando Restoy, Chair of the Financial Stability Institute (FSI)

The operational resilience of the banking sector remains a critical supervisory priority, particularly in today's rapidly evolving technological landscape, including quantum computing and frontier AI, which brings both opportunities and challenges. This topic has been a key focus for international standard-setting bodies for decades and holds particular importance for the Basel Committee on Banking Supervision. This workshop will focus on strategies to strengthen operational risk management and operational resilience within this dynamic context.

Disruption risks amid a rapidly evolving financial and technological environment

Key developments are being driven by the rapidly evolving technological landscape, including banks' (and the broader financial sectors') adoption of new technologies. This shift introduces important structural changes that necessitate a focused effort to identify and manage potential risks to critical activities of banks.

Third-Party Service Providers (TPSPs) related risks

Banks have long relied on arrangements with third-party service providers (TPSPs) including to access specialised expertise, reduce costs, improve scalability, efficiency and operational resilience. The ongoing digitalisation of finance has led to a rapid adoption of innovative approaches, increasing banks' dependency on TPSPs. The growing reliance on a small number of critical TPSPs, such as cloud service providers, has significantly increased concentration risks, where disruptions in these providers could have both bank-level and systemic implications. This risk is further exacerbated by complex and opaque supply chains, which amplify operational vulnerabilities, particularly when dependencies are not fully understood.

Non-Malicious Information and Communication Technology (ICT) risks

The dynamic interplay between legacy systems, adoption of new and emerging technologies, and the rapid digitalisation of banking operations and services, compound the complexity of ICT change management in banks as they strive to keep their infrastructure up-to-date and fit for purpose.

Non-malicious ICT incidents in banks have led to various impacts on their critical operations and customer services, with some cases proving to be particularly significant (BCBS 2026). For example, failure in system migration in one case caused a multi-channel service disruption affecting about 10% of the population in one jurisdiction. In another jurisdiction, a similar incident rendered critical banking operations unavailable for several days. The most frequently observed root causes of non-malicious ICT incidents in supervised banks are (BCBS 2026):

- (i) modifications to banks' ICT environment or its configurations without proper authorisation, review and rigor;

- (ii) gaps in system design, development and testing;
- (iii) system capacity and performance issues, such as challenges in managing peak loads or operational demands; and
- (iv) external dependency operational failure to meet expectations or contractual obligations for the provision of services or goods, due to ineffective or failed internal processes, people, controls or systems.

Malicious cyber risks

An important consequence of the growing reliance on new technologies and interconnectedness of the financial system is the heightened cyber risk faced by the banking sector. Banks are increasingly adopting technology-driven strategies that involve greater automation and deeper integration with external providers and customers. For instance, more data is being stored and processed outside the institutions' own perimeters, while service providers are granted access to internal environments to perform business and technology functions. This expansion of the attack surface creates greater opportunities for cyber adversaries, and has led to an increase in the frequency, severity and sophistication of cyber-incidents in recent years.

Basel Committee's approach to enhance operational resilience

The Committee has been at the forefront of international efforts to strengthen the operational resilience of the global banking sector.¹ Recognising the evolving risks posed by technological advancements, reliance on third-party providers, and the growing sophistication of cyber threats, the Committee has developed guidance and other tools to address these challenges.

For example, previous work by the Committee (BCBS, 2018) focused on reviewing different approaches to managing vulnerabilities and threats related to malicious cyber incidents. The findings highlighted that the international regulatory landscape for cyber-risk management and resilience exhibits both convergence and diversity. While high-level expectations are broadly aligned across jurisdictions, differences exist in technical specifications and supervisory practices, often shaped by variations in legal frameworks and levels of digitalisation. Key challenges identified include workforce skill shortages, limited adoption of response and recovery testing relative to protection and detection measures, and the lack of standardised metrics for assessing cyber-resilience.

A principles-based approach

The Committee has adopted a principles-based approach to promoting banks' operational resilience. This approach seeks to accommodate a diverse range of bank risk management practices and approaches. As such, 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 criticality of the different risks.

The Core Principles for effective banking supervision (BCP) introduced a new CP25 Operational risk and operational resilience in 2024. The new CP25 is closely aligned with the Committee's Principles for Operational Resilience (POR), which build upon the Committee's revised Principles for the Sound Management of Operational Risk (PSMOR). These standards and guidelines form the basis of the

¹ The Financial Stability Board (FSB) is also working extensively with a cross-sectoral global view in the area of financial innovation (including third-party risk management and oversight) and cyber resilience (building on the updated Cyber Lexicon, the FSB has explored ways to promote greater convergence in cyber incident reporting, and developing a toolkit to promote effective practices financial institutions response and recovery).

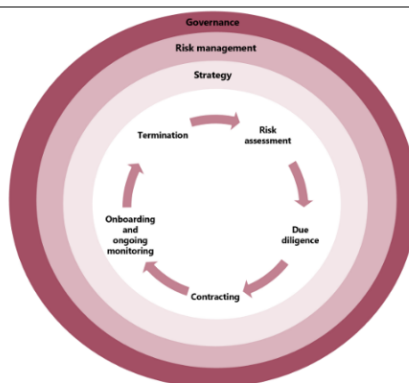
Committee's work on improving operational resilience. Additionally, the Committee has developed further detailed principles and range of practices more recently in specific areas, as described below.

Principles for the sound management of third-party risk (December 2025)

The Committee has developed a new set of principles, superseding the 2005 Joint Forum paper *Outsourcing in financial services* for the banking sector, to reflect the evolution of a larger and more diverse TPSP environment in the banking sector. The principles set a common baseline for banks and supervisors in managing risks associated with third-party providers, while allowing sufficient flexibility to adapt to evolving practices and regulatory frameworks across jurisdictions.

The effective management of third-party risk generally follows the stages of the life cycle for TPSP arrangements. Controls should be designed proportionally to the risks and criticality of each TPSP arrangement. As such, a risk management framework benefits from identifying the risks and criticality of bank operations supported by a TPSP arrangement at inception and periodically throughout its life cycle (Graph 1). The stages of the life cycle typically include risk assessment, due diligence, contracting, onboarding and ongoing monitoring, and termination. The bank's governance, risk management and strategy are integral to each stage of the life cycle.

Graph 1: Third-party arrangement life cycle



Source: BCBS, 2025.

Information and communication technology (ICT) risk management (June 2026)

To strengthen banks' operational resilience to ICT incidents in an increasingly digitalised world, the Committee analysed ICT risk management practices to address non-malicious ICT incidents across jurisdictions. The range of practices published in June 2026 seek to support banks in developing robust ICT risk management frameworks. Some of the key results can be summarised as follows:

- The five most frequently reported ICT risk management practices across surveyed jurisdictions include: management of changes to ICT systems and infrastructure; management of ICT risks arising from the reliance on third party services; testing the effectiveness and robustness of ICT business continuity and disaster recovery measures; ensuring effective incident response, containment, root cause identification and remediation; and implementing ICT systems to meet business requirements and to achieve the necessary quality, reliability and security assurance.
- Banking authorities of the surveyed jurisdictions indicated that they have ICT risk management regulations and/or guidance in place. In many surveyed jurisdictions, banks are subject to additional ICT risk management regulations and/or guidance at the national level from other

government agencies. However, banking authorities retain the primary authority to issue ICT risk management regulations and/or guidance, and exercise supervisory oversight on banks.

- Surveyed jurisdictions report several challenges faced by banks in their implementation of ICT risk management practices. For example, challenges were observed in maintaining traceability from business services to ICT assets and ensuring the completeness of system dependency mapping and ICT asset inventory. Talent shortages at banks, particularly in cyber security, cloud, artificial intelligence / machine learning (AI/ML), and legacy systems, are exacerbated by competition with the technology industry.

The forward-looking view – navigating emerging technologies

Emerging technologies are set to further redefine the financial and technological landscape, offering transformative opportunities but also introducing significant risks.

- **Quantum computing**, though still in its early stages, represents a critical long-term threat to the security of current cryptographic methods. By leveraging the principles of quantum mechanics, it has the potential to process information at unprecedented speeds and scales. A breakthrough in this field could render widely used encryption algorithms obsolete, exposing sensitive data to vulnerabilities and creating systemic risks across interconnected financial systems. This could erode trust in the global financial infrastructure by compromising the confidentiality and integrity of institutional data.
- **Frontier artificial intelligence (AI)** is emerging as both a powerful tool and a significant threat in the financial system. These advanced AI models can autonomously identify vulnerabilities, generate sophisticated cyber-attacks at unprecedented speed and scale, and simultaneously improve defensive capabilities such as vulnerability discovery, threat detection, cyber monitoring, and incident response. Supervisory authorities are responding by adapting expectations within existing cyber risk management and operational resilience frameworks, prioritising governance for faster decision-making, accelerated patching, and enhanced response and recovery capabilities (Table 1).

Potential risks stemming from emerging technologies transcend organisational and national boundaries, making stronger cross-border supervisory coordination and effective information sharing critical to maintaining operational resilience across the global financial system.

Examples of actions adopted by authorities

Table 1

	Key messages	Examples of recent responses by authorities
Proactive vulnerability identification	Call for proactive identification of vulnerabilities, updates to operational resilience plans, and addressing AI-exposed risks.	ECB, Bank of England, Bank of Spain, SARB, MAS
Governance and accountability	Emphasise governance frameworks, board-level accountability, and use of existing guidance for risk management.	ASIC, SARB, OSFI
Strengthening cyber resilience	Urge institutions to improve incident response, accelerate patch management, and manage third-party risks.	APRA, ASIC, Bafin, JFSA
Supervisory adaptation and innovation	Introduce new supervisory divisions, cyber resilience testing frameworks, and innovative inspection approaches.	Bafin, Monetary Authority, Federal Reserve Board

Source: Crisanto et al (2026).

Questions

Disruption risks amid a rapidly evolving financial and technological environment

Q1. What are the key priority areas on potential disruption risks in your jurisdiction? Have institutions demonstrated effective responses in identifying potential disruption risks and exploring opportunities to enhance operational resilience?

Aligning global efforts to enhance operational resilience

Q2. How do you address concentration risks from reliance on a small number of critical TPSPs with global reach, including through complex and opaque supply chains? What practices implemented by institutions have been most effective? Are there opportunities to enhance international cooperation to effectively tackle these challenges?

Q3. What supervisory strategies have been most effective in addressing incidents from legacy systems/gaps in change management? How do you encourage banks to strike a balance between upgrading legacy systems and managing the risks of rapid technological change?

Q4. What approaches are being used to address the skills shortage in cybersecurity and ICT risk management? How do you as a supervisor incentivise banks to invest in talent development and retention in these critical areas?

The forward-looking view – navigating quantum computing and frontier AI

Q5: What good practices have you identified for detecting and addressing vulnerabilities in the operational resilience of institutions in the face of emerging technologies? What measures are you considering/implementing to ensure that supervisory/regulatory frameworks for operational resilience remain agile and adaptable to the rapid pace of emerging technologies?

References

Basel Committee on Banking Supervision (2018): "Cyber-resilience: range of practices", December.

——— (2021a): "Principles for operational resilience", March.

——— (2021b): "Revisions to the principles for the sound management of operational risk", March.

——— (2024): "Core Principles for effective banking supervision", April.

——— (2025): "Principles for the sound management of third-party risk", December.

——— (2026): "Information and communication technology (ICT) risk management: range of practices", June.

Crisanto, JC, A Currat and J Yong (2026): "When machines attack: frontier AI cyber threats and policy responses in the financial sector", *FSI Occasional Paper*, no 28, September.