April 2024

# Workshop 5
# Digitalisation of finance

Chair: Arthur Yuen, Deputy Chief Executive of the Hong Kong Monetary Authority

Advances in digitalisation and financial technology continue to affect the landscape of the financial system, including the provision of banking services. Technological developments are disrupting the financial system through three main channels: first, through an expansion in the set of financial services and products, and the distribution channels through which they are offered; second, through the emergence of new technological suppliers of these services, such as big techs, fintechs and other third-party providers; and third, through the increasing use of digital innovations for the management, mitigation and oversight of risks.

The *Core Principles for effective banking supervision* ("Core Principles") have been amended to reflect the impact of new risks, including risks relating to the ongoing digitalisation of finance. Technology-driven innovation and the digitalisation of finance are changing both customer behaviours and the way that banking services are provided. New products, new entrants and the use of new technologies present both opportunities and risks for supervisors, banks and the banking system. Digitalisation may amplify traditional risks (eg liquidity, operational and strategic risks), while digital communication channels can more rapidly propagate banking stress. For banks, risks associated with digitalisation emphasise the importance of effective risk management processes and operational resilience given an increased reliance on third parties. For supervision, it is important that supervisors can continue to review the overall activities of a banking group (including those undertaken by service providers) and understand the risks posed by technologically enabled non-bank financial institutions to banks and the banking system.

## Innovative technologies and their applications

A defining feature of the ongoing digitisation of finance is the emergence and growing use of a wide range of innovative technologies across various aspects of the banking value chain. Banks are actively using artificial intelligence (AI)[1] and machine learning (ML)[2] in a range of contexts, including both back-office and front-office functions. Current applications include credit underwriting, trading activities, pricing models, regulatory capital and planning, liquidity requirements and planning, fraud detection and prevention, anti-money laundering (AML) tools, as well as the implementation of chatbots and marketing strategies. AI/ML techniques possess the ability to predict complex phenomena, and have the potential to enhance banks' operational efficiency, bolster risk management capabilities and expand their product offerings.

At the same time, the responsible and ethical use of AI is an important factor. This involves creating AI systems that are transparent, fair, secure and accountable, while also incorporating ongoing

[1] Tasks conducted by computers that previously required human sophistication (FSB 2017).

[2] The use and development of computer systems that can learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data (Oxford languages).

human oversight and stakeholder engagement. It also includes creating AI applications that are explainable, allowing stakeholders to understand the decision-making process as well as implementing measures to detect and mitigate biases, especially those that could lead to unfair or discriminatory outcomes.[3] The use of AI/ML should align with existing regulatory frameworks and industry standards.

In addition to AI/ML, banks may also benefit from employing a range of other innovative technologies, including application programming interfaces (APIs)[4], distributed ledger technologies (DLTs)[5] and cloud computing[6]. However, this embrace of advanced technologies requires a strategic approach that considers the associated risks and applies commensurate risk mitigants.

Q1. What is your experience with the use of innovative technologies in banking in your jurisdiction? Have you observed any innovative use cases related to the use of AI, ML, APIs, DLTs or cloud computing?

## Operational risk and mitigants

While digitalisation can benefit both banks and their customers, it can also create new vulnerabilities and amplify existing risks to banks and financial stability. The revised CP25 Operational risk and operational resilience specifies in greater detail, the expectations on banks related to managing operational risk and resilience. This is particularly relevant as banks are increasingly depending on third-party service providers to support the operational aspects of technology-based financial services. The primary motivations for outsourcing include cost reduction, operational flexibility, heightened security and enhanced operational resilience. However, outsourcing or engaging with service providers can introduce challenges related to information security, cybersecurity and privacy.

In the context of cloud services, additional concerns may arise regarding the geographical location of data storage and legal implications, potentially limiting banks' adoption of such services. The utilisation of new technologies and a growing reliance on third parties heighten cyber risks, as these entities can serve as potential entry points to banking systems. For instance, operational and cybersecurity risks associated with the unsafe use of APIs may encompass data breaches, misuse and falsification of data. Such breaches, in turn, can escalate into significant reputational and legal risks for banks. The interconnectedness of banks via new technologies and service providers can also create concentration risks on a system-wide level.

It can be challenging for banks to ensure that governance and risk management processes and practices keep pace with the use of new technologies. Risks could be heightened when (i) banks' governance frameworks are not modified to adapt to new technologies (eg the use of AI/ML); (ii) there is inappropriate accountability and responsibility; (iii) there is a lack of technological literacy, including the

[3] UNESCO (2022).

[4] A set of rules and specifications for software programmes to communicate with each other, and an interface between different software programmes that facilitates their interactions (BCBS 2018).

[5] DLT refer to the protocols and supporting infrastructure (ie distributed ledgers, blockchains and the bundle of related technologies) that allow computers in different locations to propose and validate transactions and update records in a synchronised way across a network. DLT solutions have the potential to be applied for multiple purposes, including new forms of money (eg central bank digital currencies), tokenisation of assets and deposits, and improving the operational management of existing business activities (BCBS 2018).

[6] Refers to the use of an online network of hosting processors to increase the scale and flexibility of computing capacity. In this model, a bank accesses an on-demand network of a shared pool of configurable computing resources (eg networks, servers, storage facilities, applications and services) maintained by the cloud service provider. (NIST 2021; FSB 2019; FSI 2018).

inability to attract, build and retain talent; and (iv) there is poor oversight of data governance and inappropriate use of systems and applications developed by third parties.

The safety and soundness of banks can be enhanced by ensuring effective governance structures and risk management processes that appropriately identify, manage and monitor risks arising from the use of financial technologies as well as associated new business models, applications, processes or products. These include, for example, risk management processes in line with the Committee's *Principles for sound management of operational risk* (PSMOR) and *Principles for operational resilience* (POR)[7] that are relevant to financial technology developments. Banks that rely on innovative technologies must prioritise the establishment of effective IT and risk management processes, along with robust control environments capable of addressing emerging sources of risk. In parallel, bank supervisors play an important role in enhancing safety and soundness by ensuring that banks adopt risk management processes and control environments that are not only effective but also proportional to the risks associated with specific use cases.[8]

Q2. How do you ensure that banks properly mitigate operational risks stemming from the use of new technologies?

Q3. What enhancements to current risk management frameworks might be necessary to better ensure that banks appropriately manage the risks from innovative technologies?

## New competitors and business models

The rise of financial technology has coincided with the emergence of new players and business models. To date, these developments have affected the banking system primarily through: (i) competition from new entrants, particularly in payment services; and (ii) the formation of strategic partnerships between banks and other entities.

Fintech has paved the way for various non-bank firms, including startups and larger technology companies, to enter the realm of banking and financial services. These entities often possess a technological advantage over traditional banks and generally operate without the constraints of prudential regulation or supervision. Digitalisation has also increased the presence of neobanks, or digital-only banks, who provide retail banking services primarily through smartphone apps or internet-based platforms. Unburdened by legacy infrastructure, they can harness new technology at a lower cost and more rapidly, presenting a modern and competitive alternative for customers.

To respond to competition from new entrants, some incumbent banks are partnering with non-banks and technology firms to deliver products and services across different parts of the banking value chain through banking-as-a-service (BaaS) arrangements. The key characteristic of BaaS is that although banks ultimately facilitate the provision of the banking services, the non-bank intermediaries retain the direct customer relationships. While such new arrangements exploit the comparative advantages of the bank and non-bank partners, it may also amplify certain risks.

Q4. How has competition from technologically enabled entrants affected banking in your jurisdiction? Do you see banks adjusting their business models to stay competitive?

[7] BCBS (2021)

[8] BCBS (2018).

## Regulatory and supervisory implications

The digitalisation of finance raises several implications for banking supervisors in terms of defining the regulatory perimeter, assessing the adequacy of existing rules and regulations and adapting supervisory frameworks and approaches. It may also increase the interconnections across different sectors of the global financial system, increasing financial stability risks.[9] The challenge for regulatory authorities lies in striking a balance between ensuring the safety and soundness of the banking system while not unduly impeding the benefits of innovation.

Existing regulatory definitions of activities may not capture the full perimeter of emerging products and services, allowing non-banks to compete with banks outside of the scope of supervisors' authority. To ensure fair competition, it is crucial that non-banks offering products with superior returns or lower costs than banks achieve this through genuine technological advancements rather than exploiting regulatory arbitrage.

The digitalisation of finance also raises issues that go beyond the scope of prudential supervision to other public policy objectives, such as safeguarding data privacy, consumer protection, promoting financial inclusion and fostering competition. In light of these challenges, regulatory and legal frameworks must be crafted to enforce the principle of "same risk, same activity, same regulation." This principle ensures that regardless of the entity providing financial services, the regulatory requirements should be equivalent when the risks associated with the activity are the same.[10] This approach helps to maintain a level playing field, promote fair competition and preserve the integrity and stability of the broader financial system. Consequently, supervisory authorities should ensure that they communicate and coordinate with relevant regulators and public authorities. This could include, for example, those authorities charged with consumer protection, data and privacy protection, competition and national security. Given the growth in firms operating across borders, supervisory exchange and coordination at the global level is also important for cross-border supervision.[11]

Q5. Which aspects of supervisory standards or guidance could benefit from review in response to the digitalisation of finance?

Q6. Considering the potential benefits and challenges associated with the digitisation of finance, on which topics would increased international collaboration among supervisors be most useful?

9 Hernández de Cos, P (2024)

10 FSI (2022)

11 BCBS (2018).

## References


Basel Committee on Banking Supervision (2018): "Implications of fintech developments for banks and bank supervisors", Sound Practices, February.

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

Financial Stability Board (FSB) (2017): "Financial Stability Implications from Fintech", June.

——— (2019): *"Third-party dependencies in cloud services - Considerations on financial stability implications,"* December.

Financial Stability Institute (FSI), *Regulating and supervising the clouds: emerging prudential approaches for insurance companies* (5 December 2018)

——— (2022): "*Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs*", August 2022.

Hernández de Cos, P (2022): "*International cooperation in a world of digitalisation*", keynote speech at the 22nd International Conference of Banking Supervisors (virtual), 29 November.

——— (2024): "*Two truths and a myth in banking regulation*", speech at the Eurofi High Level Seminar, Ghent, 23 February.

National Institute of Standards and Technology (2011): "*The NIST Definition of Cloud Computing*".

Oxford languages: The language data is provided by Oxford Languages, part of Oxford University Press.

UNESCO (2022): *"Recommendation on the Ethics of Artificial Intelligence"*.