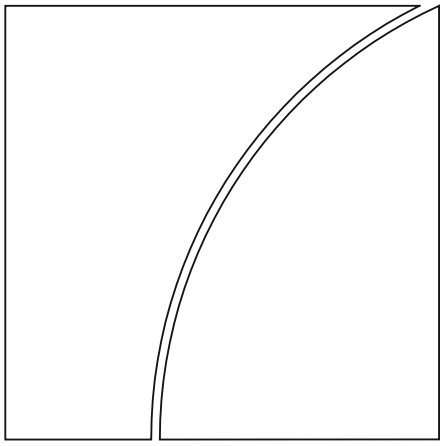
Basel Committee
on Banking Supervision



Digitalisation of finance

May 2024

BIS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-760-3 (online)

Contents

Executive summary

Technological innovation is transforming the provision of banking services through three broad channels: (i) an expansion in the set of financial services and products, as well as the distribution channels through which they are offered; (ii) the arrival of new technological suppliers of these services (eg big techs, fintechs and third-party service providers); and (iii) the increasing use of digital innovations for managing, mitigating and overseeing risks.

As the global standard setter for the prudential regulation of banks, the Basel Committee on Banking Supervision (BCBS) has a strong interest in monitoring digitalisation trends, understanding how these may impact banks and banking supervision, facilitating the exchange of information between supervisors to identify and address common challenges and, where appropriate, issuing standards or guidance to mitigate risks.

This report builds on the Committee's 2018 paper, *Sound practices: implications of fintech developments for banks and bank supervisors,* and takes stock of recent developments in the digitalisation of finance.

Section 2 reviews some of the key technologies across various aspects of the banking value chain. This includes the use by banks of application programming interfaces (API), artificial intelligence (AI) and machine learning (ML), distributed ledger technology (DLT) and cloud computing. Such technologies are being used by a wide range of banks, albeit with varying degrees of intensity and scope. For example, despite the growing interest around AI/ML, most banks appear to be using such technology cautiously at this stage, especially for customer-facing services and for revenue generation. In contrast, there has been a significant increase in the number of banks using cloud computing services in recent years, with this trend expected to continue.

Section 3 considers the role of new banking competitors and business models. To date, these developments have affected the banking system primarily through: (i) competition from new entrants (eg in payments services); and (ii) the formation of strategic partnerships between banks and other firms. As a result, the topology of the banking system is evolving, with new nodes and channels of interconnections.

Section 4 outlines the potential risks for banks and financial stability arising from the digitalisation of finance and the trends outlined in previous sections. While digitalisation can benefit both banks and their customers, it can also create new vulnerabilities and amplify existing risks to banks, their customers and financial stability. These include greater challenges by banks to adapt their business strategies ("strategic risk") to an increasingly digital environment, potentially heightened reputational risk to banks, a larger scope of factors that could test banks' operational resilience and operational risk, and challenges to banks' data governance. There are also system-wide risks that could result from the ongoing digitalisation of banking, including greater interconnection nodes across financial firms, a heightened degree of contagion in times of stress and the amplification of procyclical behaviour (eg fire sales).

Against that backdrop, Section 5 considers the various strategies and practices that are, in principle, available for banks to mitigate risks. Effective governance structures and risk management processes are fundamental to identifying, monitoring and mitigating risks associated with the digitalisation of finance. Banks may also mitigate specific digitalisation-related risks – such as those stemming from API or AI/ML models by enhancing controls and pursuing an "across the bank" human-centric approach to overseeing the use of such technologies. Similarly, banks manage data-related risks through robust governance arrangements and enhanced security protocols. Banks may also reinforce their due diligence and operational risk management to mitigate the risks stemming from their reliance on third-party service providers. In practice, many of these risk mitigants are still evolving and have not yet been tested through different phases of the business cycle or periods of stress.

Regulations and supervisory frameworks have also evolved in response to the digitalisation of finance. Section 6 reviews these developments. For example, some jurisdictions have expanded the scope

of the regulatory perimeter in their legislative frameworks. Most authorities also require new banking applications to follow the same framework applied to "traditional" bank entrants, with a few jurisdictions applying a distinct process for digital-only banks. Many jurisdictions have also issued specific supervisory guidance related to different aspects of the digitalisation of banking (eg on model risk management and cloud computing). Supervisors are also reviewing and adjusting their approaches and tools to mitigate the risks from digitalisation while also harnessing their benefits in a responsible manner.

Section 7 concludes by outlining the regulatory and supervisory implications for both banks and banking supervisors. At a macro-structural level, supervisors should continue to monitor – and it is important for banks to mitigate – the risks stemming from the evolving nature of banking as a result of technological innovations. The adoption of innovative technologies and business models should be guided by a principle of responsible innovation. It is important for supervisors to strike the right balance between enabling responsible innovation while also safeguarding the safety and soundness of the banking system and financial stability. As a result of the increasingly blurred lines between banks and the provision of banking services, integrating the principle of "same risk, same activity, same regulation" in regulatory and legal frameworks may help avoid regulatory arbitrage.

Section 7 also includes implications of specific digitalisation themes. It recognises data as a critical resource, which necessitates a commensurate level of safeguards. The use of service providers should be subject to robust risk management practices and processes in a risk-based and proportionate manner. More generally, advances in digitalisation should not diminish the role of human judgment in risk management and supervision.

This report also highlights the implications of digitalisation for capacity building and coordination. It is important for both banks and supervisors to have sufficient resources and staff with the necessary capabilities, knowledge and skills to assess and mitigate risks from new technologies and business models. Digitalisation raises issues that go beyond the scope of prudential supervision. Accordingly, communication and coordination among bank supervisors and other relevant authorities, within and across jurisdictions, is important to address these considerations.

The Committee will continue to monitor developments related to the digitalisation of finance. Where necessary, it will consider whether additional standards or guidance are needed to mitigate risks and vulnerabilities.

1. Introduction

Advances in digitalisation and financial technology ("fintech") continue to affect the landscape of the financial system, including the provision of banking services.[1] Technological developments are disrupting the financial system through three broad channels: (i) an expansion in the set of financial services and products, as well as the distribution channels through which they are offered; (ii) the arrival of new technological suppliers of these services (eg big techs, fintechs and third-party service providers); and (iii) the increasing use of digital innovations for managing, mitigating and overseeing risks.

As the global standard setter for the prudential regulation of banks, the Basel Committee on Banking Supervision (BCBS) has a strong interest in monitoring digitalisation trends, understanding how these may impact banks and banking supervision, facilitating the exchange of information between supervisors to identify and address common challenges and, where appropriate, issuing standards or guidance to mitigate risks.

In 2018, the Committee published a sound practices paper on the implications of fintech developments for banks and bank supervisors.[2] The paper sought to contribute to a common understanding of the opportunities and risks associated with fintech in the banking sector by describing observed practices. It outlined five, non-mutually exclusive, stylised forward-looking scenarios on the potential impact of fintech on the banking industry and bank supervision:

- *Better bank* – would see the modernisation and digitalisation of incumbent players.
- *New bank* – where incumbents would be replaced by challenger banks.
- *Distributed bank* – which would see the fragmentation of financial services among both incumbent banks and fintech firms.
- *Relegated bank* – where incumbent banks would become commoditised service providers and customer relationships are owned by new intermediaries.
- *Disintermediated bank* – where incumbent banks would become "irrelevant" as customers interact directly with individual financial service providers.

Since 2018, the digitalisation of finance has continued to accelerate across a number of fronts. Investments in fintech companies between 2019 and 2023 totalled $865 billion – more than twice the amount invested between 2013 and 2018.[3] Big techs, fintech firms, non-bank financial institutions and service providers are collectively playing growing roles in the provision of financial services, with increasing chains of interconnections. Developments in artificial intelligence and machine learning, cloud computing, distributed ledger technology, decentralised finance and various forms of cryptoassets have all raised important questions about their potential impact on banks, banking and supervision.

This report builds on the 2018 paper and takes stock of recent developments in the digitalisation of finance and is structured as follows. Section 2 provides a brief description of key technologies and relevant use cases within the banking industry. Section 3 considers the role of technologically enabled competitors on banking and banks' business models. Section 4 outlines the potential risks for banks and financial stability arising from the digitalisation of finance. Section 5 considers the various strategies and practices adopted by banks to mitigate risks. Section 6 describes different regulatory and supervisory initiatives in response to the digitalisation of finance. Section 7 concludes by outlining the potential

[1] Fintech refers to technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services (FSB 2017).

[2] BCBS (2018a).

[3] Statista data in 2023.

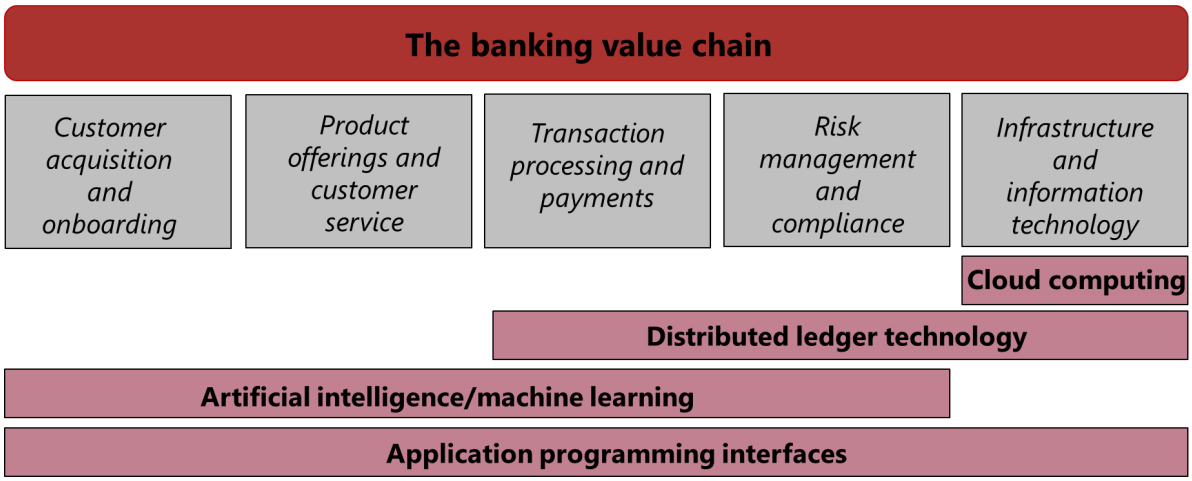
regulatory and supervisory implications for both banks and banking supervisors – these do not constitute formal standards or guidance. A glossary of terms used is provided at the end of this report.

The report has been developed based on research and analysis, supervisory exchanges, a survey of Basel Committee and Basel Consultative Group members,[4] and outreach with external stakeholders. The case studies referred to throughout the paper are intended to be informative only – they are not an endorsement by the Committee (or its members) of any particular practices, models or entities.

2. Innovative technologies and their applications

A defining feature of the ongoing digitalisation of finance is the emergence and growing use of a wide range of innovative technologies across various aspects of the banking value chain (Graph 1). Building on the 2018 paper, this section describes developments in innovative technologies and their use cases within banking and financial services.

Graph 1: Innovative technologies and the banking value chain



This report focuses on those technologies that are widely in use across banks – either in development or production – and it therefore does not consider those technologies (eg quantum computing) that may impact banks and banking over a longer time horizon. Nor does it consider the potential impact of central bank digital currencies on the banking system.

2.1 Application programming interfaces

In the context of financial services, application programming interfaces (APIs) can facilitate the sharing of data between two distinct applications and allow for the execution of certain financial activities or services. APIs allow for more efficient real-time processing between software programs and facilitate increased data connectivity. Banks are using APIs in various ways including to share or import data:

- between their internal systems, eg for mobile banking, which connects customer-facing applications with the bank's core systems;

[4] The Basel Consultative Group facilitates supervisory dialogue with non-member countries and provides a forum for deepening the Committee's engagement with supervisors around the world on banking supervisory issues.

- to or from external partners, eg under banking as a service arrangements (see Section 3.2) or when outsourcing certain functions; and
- to or from unrelated third parties, eg sharing a customer's account transaction data with an external accounting software provider or for reporting data to its supervisor.

APIs are generally considered more secure than other data-sharing techniques and may also afford banks greater control over how customer data can be accessed and by whom.[5] API usage allows banks to partner with specialist third-party firms to provide integrated modular services, develop new business models (and potentially new revenue streams) and more securely outsource processes to third parties instead of building internal systems.[6] Where there is reciprocity in terms of data-sharing, banks may also be able to increase their knowledge of customers by having access to a broader range of personal financial data.

APIs are commonly used in open banking/open finance frameworks. The aims of different open banking/finance regimes vary, but can include fostering innovation in financial services, improving competition and promoting financial inclusion. If the API is configured to allow it, consumers can also permit third parties to make account decisions for them (eg investment decisions). For businesses, open banking/finance can support faster verification of customer accounts, more efficient payment processing and access to better financial products (eg bank loans using transaction-based underwriting).

Many countries have already implemented, or are planning to introduce, open banking/finance initiatives (Graph 2). Globally, these regimes take different forms and vary in terms of:

- whether they are mandatory or voluntary, and regulatory led or market driven;
- the scope of frameworks, eg some jurisdictions have extended data-sharing to other sectors of the economy[7] or enable third parties to initiate actions on behalf of consumers in addition to being able to "read" their data;[8]
- the types of data that must be shared (eg payments data versus broader financial data);
- whether they mandate API usage and require the use of common protocols;
- the form and duration of customer consent;
- whether they require third parties seeking access to consumer data to be licensed or authorised; and
- arrangements regarding cost distribution.

Open banking/finance frameworks are expected to play a critical role in enabling customer-permissioned data-sharing at scale, which, in turn, is expected to encourage further innovations in business models and products.[9]

5 World Bank (2022).

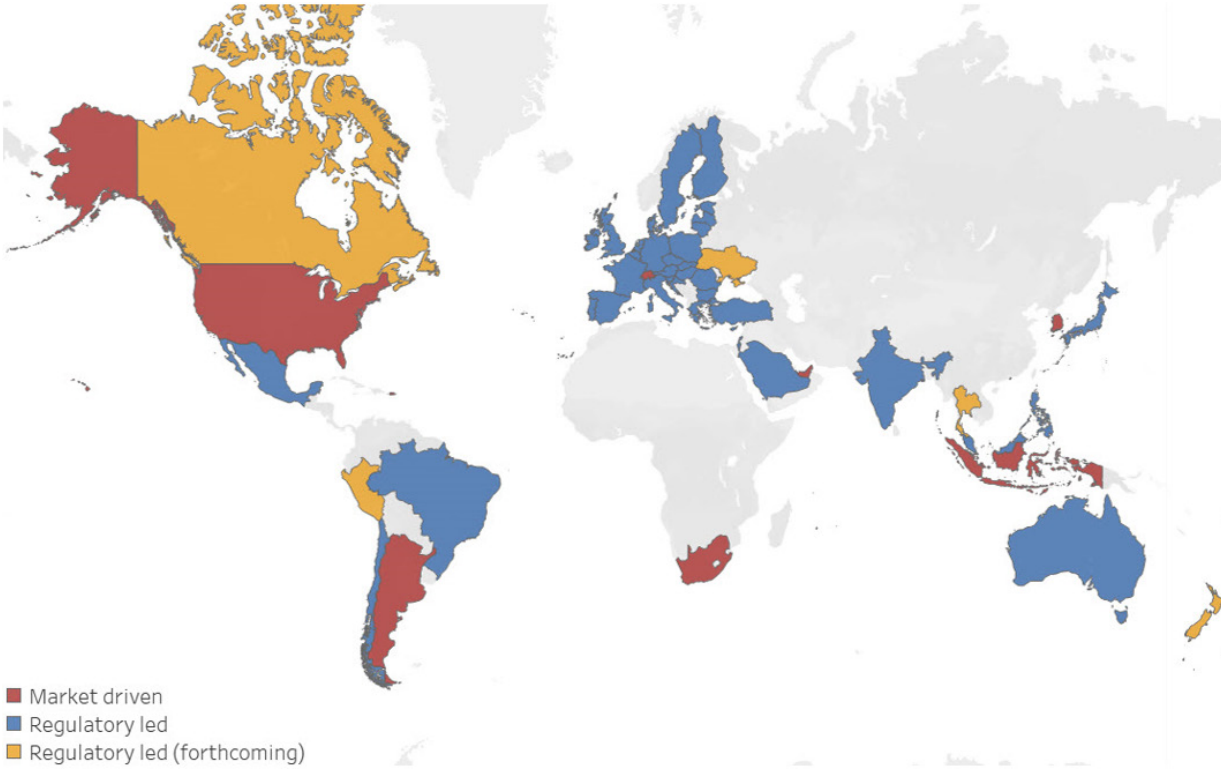
6 World Bank (2022).

7 For example, in Australia the Consumer Data Right enables individuals to share their data across the banking and energy sectors, with plans to extend the regime to non-bank lending.

8 For example, payments can be initiated under the EU Payment Services Directive 2015/2366 (PSD2).

9 World Economic Forum (2024).

Graph 2: Adoption of open banking/open finance



Source: BCBS member survey 2024.

Box 1

Open banking in South Korea

In 2019, the open banking system in Korea was implemented as a market-led financial infrastructure. In Korea, open banking is defined as an open payment platform that delivers core banking services to trusted participants through standardised open application programming interfaces (APIs). The Korea Financial Telecommunications and Clearings Institute (KFTC) acts as a central hub, facilitating the provision of payment services from financial institutions and fintechs to consumers.

Any licensed or authorised institution, including banks, financial companies and fintechs, have the option to voluntarily participate in the open banking system. Through agreements with the KFTC, participants can access functionalities and data from all providers. The open banking system in Korea leverages the benefits of network effects – as the number of participants grows, interlinkages among them increase, leading to a reduction in costs for each participant. Simultaneously, this growth significantly increases the overall benefits of the system.

The open banking system in Korea differs from other countries' open banking systems, which primarily offer inquiry APIs, by also providing transfer APIs. Specifically, it offers account transfer (eg withdrawal and deposit), account inquiry (eg balance, transaction history and account real name), card inquiry (eg card list and card information) and prepaid inquiry (eg prepaid list and prepaid balance). Participants can implement a variety of financial services (eg transfer, inquiry and payment) by combining open APIs provided via open banking. For example, simple funds transfer services can be delivered by combining withdrawal transfer APIs with deposit transfer APIs and balance inquiry APIs.

As of end-2023, 136 institutions (including all commercial banks (19), all credit card companies (8), securities companies (20) and fintechs (79)) were actively participating in the open banking system, with approximately 35 million subscribers (68% of the population).

2.2 Artificial intelligence and machine learning

Banks are using artificial intelligence and machine learning (AI/ML) applications in a variety of settings, for both back office and front office functions. To date, use cases include credit underwriting, trading activities, pricing models, regulatory capital and planning, liquidity requirements and planning, fraud detection and prevention, anti-money laundering and combating the financing of terrorism (AML/CFT), chatbots and marketing.

AI/ML techniques possess the ability to predict a wide variety of complex phenomena and have the potential to increase banks' operational efficiency, risk management capabilities and product offering (eg robo-advisory services). More specifically, the potential benefits of AI/ML applications include:

- improving the client experience, as the technology can help streamline customer interactions (such as applying for a loan) by removing manual steps;
- superior pattern recognition ability and predictive power compared with more traditional approaches (eg in improving investment performance, detecting fraud or expanding credit access);
- cost efficiencies (ie AI/ML approaches may be able to arrive at outcomes more cheaply, with no reduction in performance) such as enabling the development of multi-channel customer access and increasing self-service by customers;
- greater accuracy and consistency in processing compared with approaches that have more human input and higher "operator error" (such as detection of anomalies in AML monitoring); and
- better capability to accommodate very large and less-structured data sets, and to process those data more efficiently and effectively (eg ability to gain greater insight into customer needs and the provision of more tailored or customised services).

Box 2

Machine learning for credit scoring in Italy

Some banks are using machine learning (ML) for credit scoring to enhance the accuracy of risk scoring over conventional credit risk models. As they can use more data and more complex algorithms, ML models can provide greater accuracy in predicting defaults.[10] This, in turn, can allow banks to better assess the credit worthiness of potential borrowers and may also facilitate access to credit by underserved applicants.[11]

In Italy, some intermediaries (banking and non-banking institutions) are using ensemble ML models (ie decision trees, random forest and XGB boost) for credit approval and monitoring in their retail and small and medium-sized enterprise (SME)/corporate segments. These models exhibit a good balance between accuracy and explainability. In two cases, ML models have been used as modules for the calculation of risk-weighted assets. These models are usually developed in-house with the support of third parties, although there are a few examples of fully outsourced models.

The main purpose of these ML models is to support credit analysts in their activities, so the "human in the loop" makes the final decision (granting/rejecting loans or taking/not taking actions during the monitoring process). Some intermediaries are planning to use ML models for fast credit lending, thereby eliminating the human control after a test period to monitor performance. In addition, intermediaries are developing post hoc explainability tools (eg Shapley values and feature importance) to single out relevant variables for rejecting a credit application and/or

[10] Bazarbash (2019).

[11] Boukherouaa and Shabsigh (2021).

triggering specific monitoring actions. Such information is shared internally with senior management and business units, but is not disclosed to customers.

The analysis of discrimination biases is not widespread yet. Only half of the intermediaries have developed fairness standards to ensure there is no discrimination based on past biases via "fairness through unawareness". This technique entails removing all sensitive variables (ie gender and age) from the data set but does not consider the potential indirect effects these variables can have on others.

The main benefits that intermediaries expect from using ML models include better accuracy in the predictions, cost efficiency and the ability to embed different sources (ie text). Furthermore, these models may allow intermediaries to expand their customer base by covering new markets, due to enhanced predictive capability to model defaults, even without observations within the data set. The main risk of such models is operational, while reputational and legal risks are considered less material.

Box 3

Anti-money laundering initiatives in Asia

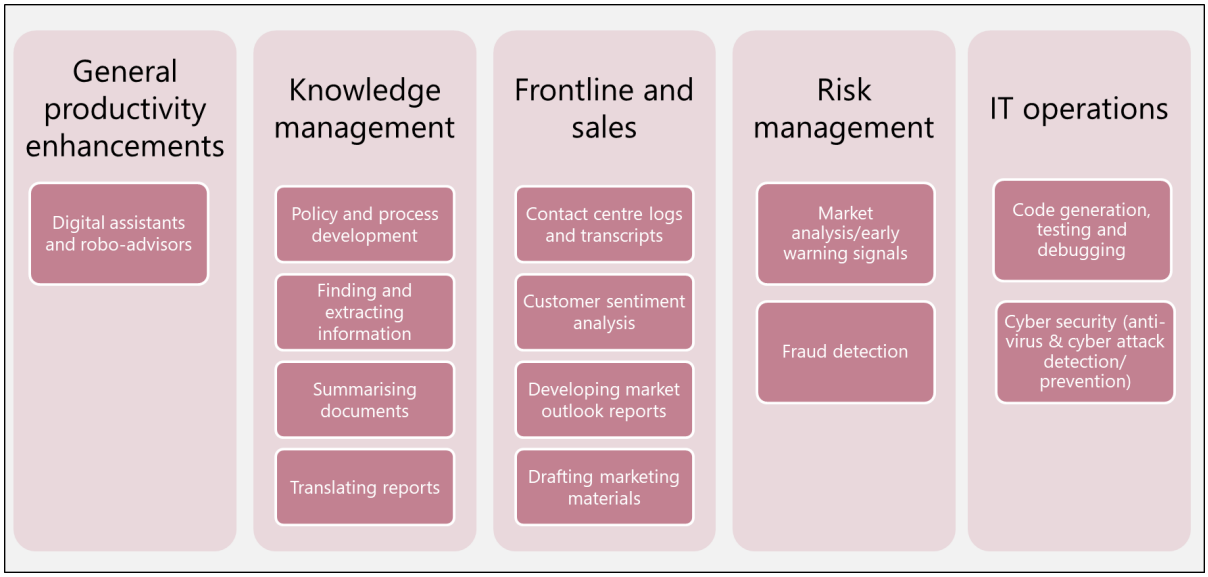
The Monetary Authority of Singapore (MAS) has actively encouraged banks to use artificial intelligence (AI) and data analytics to improve money laundering risk management. Early use cases included models to prioritise large numbers of transaction monitoring alerts for clearance. More advanced applications involve feature engineering to detect combinations of risk signals and anomalous patterns of behaviour that are suspicious. Banks are also using network analysis to find hidden relationships between potential bad actors. In supervising the use of AI models for anti-money laundering (AML), the MAS has emphasised the explainability of model outputs and effectiveness over conventional methods as key measures of success. It has required banks to put in place adequate model governance and oversight to achieve these outcomes. In addition, MAS has co-created a digital platform called COSMIC with six major banks to enable the banks to share analysis of high-risk persons and transactions at scale. COSMIC enables network analysis to be conducted across participant banks, which will increase over time, and flush out illicit activities to prevent them from spreading in the financial system.

Similarly, in Japan, a banking industry-wide initiative utilising AI has commenced to enhance AML/combating the financing of terrorism (CFT) measures. In January 2023, the Japanese Bankers Association established the Cooperation Agency for Anti-Money Laundering (CAML), which will provide AI scoring services for monitoring and filtering transactions. This service will not replace banks' transaction monitoring and filtering systems, but will provide a function using AI to score the riskiness of alerts. Transactions for which alerts are raised through a bank's monitoring system can be transmitted to a database of the new agency, where AI would be deployed to score the riskiness of each alert. Each bank would ultimately be responsible for reviewing the score and deciding on any necessary actions. Measures will be taken to ensure the quality of underlying data and to prevent issues of explainability. Handling large numbers of alerts or false positives could be optimised by utilising the AI scoring service.

Overall, banks appear to be using AI cautiously at this stage, although some are using AI more intensively. For higher risk uses cases, many processes have not been fully automated (eg AI/ML applications are used to benchmark primary models, or outputs are subject to, and/or used to support, human decision-making). Regulatory uncertainty with respect to expectations on accountability, ethics, data privacy, fairness, transparency and explainability has also been identified by some banks as a factor behind their more cautious approach, especially for uses with consumer implications.

More recently, generative AI (ie where an algorithm or model generates outputs such as texts, images and videos based on the patterns of data that it was "trained" on) has received significant public attention. Generative AI is not focused on a single application but can be adapted to a wide range of distinctive tasks. Banks' use of generative AI remains limited at present, especially for customer-facing services and higher-risk activities. Some banks are, however, exploring or piloting generative AI applications internally to improve operational efficiency and staff productivity. Specific use cases that have been observed are outlined in Graph 3.

Graph 3: Generative AI use cases in banking



Source: BCBS member survey and external outreach 2024.

2.3 Distributed ledger technology

Distributed ledger technology (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 banks' existing business activities (eg collateral management).[12] While the best known applications of DLT include its use in the cryptoasset and decentralised finance (DeFi) ecosystems, it has broader applications. In financial services, DLT has the potential to lower costs and increase efficiencies by allowing for cheaper, faster and more customised services. These benefits could come from immutable record keeping, digital identity, alignment of transaction legs through atomic settlement, and automation that allows for product customisation and a reduction in the number of intermediaries necessary to complete transactions. However, there are several hurdles (including legal issues) and risks (see Section 4) that must be addressed for these theoretical benefits to be realised. At present, no banks have DLT-based products that are at a systemic scale, as a fractured ecosystem and interoperability challenges limit potential network effects.

Banks across various jurisdictions are showing an increasing interest in tokenisation projects. Tokenisation is the process of representing claims digitally on a programmable platform, which has the potential to facilitate new ways of using financial assets to serve end users and unlock new arrangements that frictions in the monetary system have thus far made impractical.[13] While interest in tokenising real-world assets and liabilities is growing – with various proofs of concept, exploratory research projects and product launches occurring within the financial industry – only a few banks currently offer services or products using tokenisation.

Some of the most notable use cases by banks across jurisdictions include the issuance of security tokens backed by real estate; the tokenisation of banks' shareholders' equity; the tokenisation and custody of bank customers' shares; the tokenisation of financial instruments such as intraday repo options and

[12] BCBS (2018a).

[13] BIS (2023).

bonds; and even the tokenisation of the ownership rights in works of art, enabling investors to purchase and trade "shares" in a piece of art. On the other side of the balance sheet, banks are also experimenting with tokenised liabilities (including deposits) and stablecoins (see Box 4).

Beyond tokenisation, some banks are using or exploring DLT for other purposes, including identification verification, settlement of tokenised transactions, cross-border payments, digital asset custody and bookkeeping, among others. Specifically, some banks are exploring the utilisation of DLT for expedited payment platforms, digitalised bond holdings, cross-border payments between overseas branches or customers working abroad, customer onboarding processes, and real-time asset and collateral management. These initiatives demonstrate the diverse applications of DLT in the banking sector beyond just tokenisation. Nevertheless, at the current juncture, the size and volume of DLT activity remains small as a share of any single market.[14]

Most banks are planning to conduct activities on private permissioned, rather than public permissionless, distributed ledgers.[15] However, there are some projects that propose to use permissionless ledgers, allowing for closer integration with the broader crypto ecosystem and potentially saving significant development and maintenance costs, but requiring new forms of risk management. For example, some banks are exploring how to address AML risks and know-your-customer (KYC) requirements in permissionless blockchains by smart contracts or the use of verifiable credentials.

Box 4

EUR CoinVertible[16]

In December 2023, SG-FORGE (a fully regulated subsidiary of Société Générale) issued its own euro-backed stablecoin EUR CoinVertible (EURCV) on the Bitstamp exchange. It is marketed as a robust digital asset alternative for various on-chain transactions, including collateral, margining and wrapping to another blockchain.

EURCV is widely available for trading by any counterparty that is onboarded through Société Générale Group's compliance procedures (including know-your-customer, anti-money laundering and combating the financing of terrorism, and sanctions), subject to applicable selling restrictions. SG-FORGE has built permissioned access to EURCV on public distributed ledger technology (it will first be available on the Ethereum blockchain), although it can also be used on other platforms.

EURCV is considered a digital asset under French law. It has been designed to be compliant with the EU's Markets in Crypto-Assets (MiCA) Regulation, including the requirements relating to transparency, diversification risks and segregation of assets. EURCV's reserve assets can include only cash on deposit at a bank or certain securities meeting minimum rating and redemption requirements. The reserve assets are fully segregated from the issuer's assets and held in a trust managed by a third party. Holders of the stablecoin will have direct recourse to the collateral through the trust structure. To support transparency, SG-FORGE has committed to publishing compliance with the collateral eligibility criteria and confirmation that its value is at least equal to the amount of stablecoins on issue.

2.4 Cloud computing

Cloud computing allows the sharing of on-demand computer processing resources in a way that promotes efficiencies and economies of scale. Cloud solutions allow easier access to technology and computing infrastructure that would otherwise be expensive or take a long time to build and be costly to maintain.

[14] For example, a survey by the European Central Bank on digital transformation and the use of fintech highlighted that DLT was the technology with the lowest adoption rate among banks – fewer than 20% of respondents (ECB (2023)).

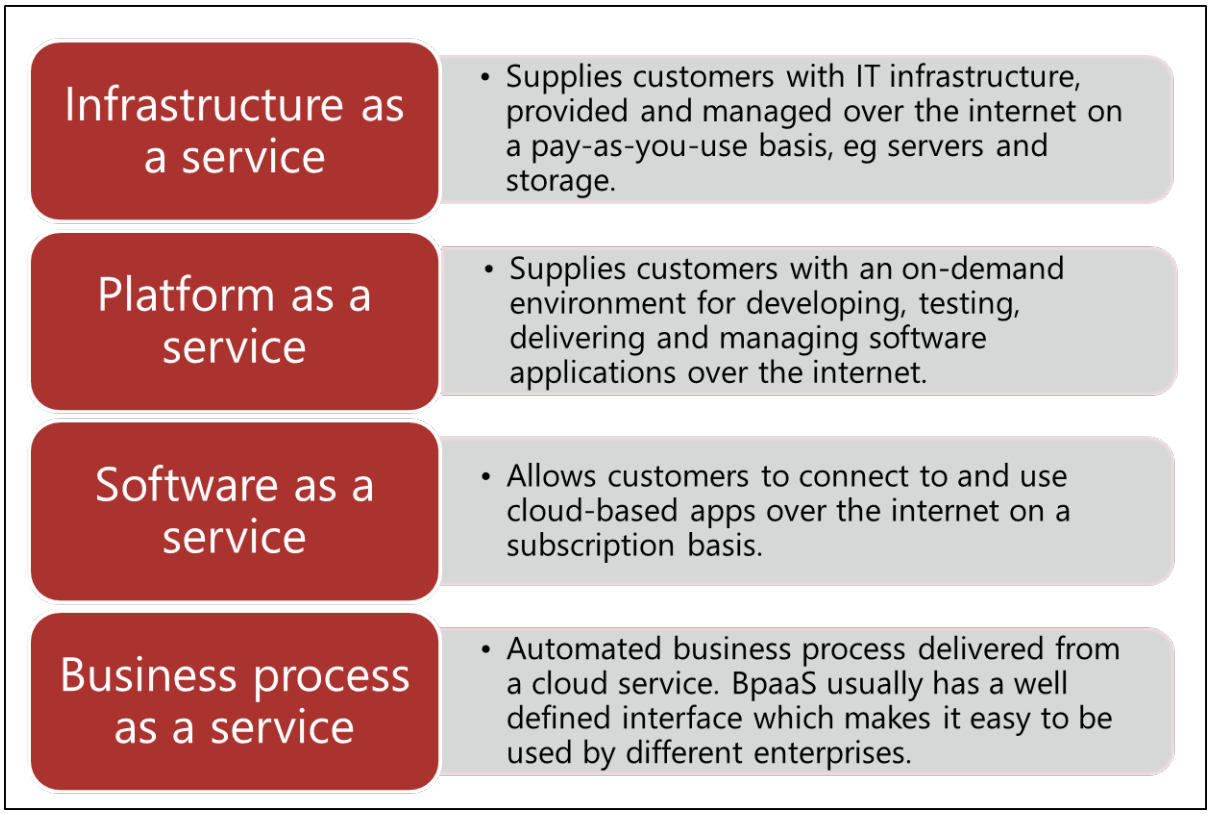
[15] Permissioned ledgers are closed networks in which a previously designated party or parties interact and participate in consensus and data validation. In contrast, permissionless networks do not limit who can participate in the consensus process used to validate transactions and data, and are decentralised across unknown parties.

[16] SG Forge (2023).

Cloud services may, therefore, lower the barriers to entry for firms expanding into new products and services, and over time reduce costs in financial services.

Participants in the financial services industry, including banks, service providers and fintech companies, use cloud services to support a range of different services and business lines. There are four main types of cloud computing service models (Graph 4), although others are also emerging.

Graph 4: Cloud computing service models



Sources: FSB (2019); NIST (2011).

There are three cloud services deployment models: public cloud, private cloud and hybrid cloud (Table 1).

Cloud services deployment models Table 1

Model	Definition
Public cloud	A third-party provider delivers computing resources and cloud services over the internet. While logical access control functions are provided to the company using publicly hosted cloud services (eg through authentication mechanisms), any other company can subscribe to the same services, available over the internet.
Private cloud	Computing resources are used solely by a single organisation, either physically in the company's on-site data centre(s) ("on-premises") or externally with the third-party provider ("hosted private cloud"). In the latter case, a virtual private network is typically set up between the company and the third-party cloud provider. In both scenarios, services are not accessible or even publicly visible over the internet.
Hybrid cloud	Combines public and private cloud with technology that allows data and applications to be shared between them. Technologies used therefore allow for portability of data and applications.

Sources: FSB (2019); NIST (2011).

Banks that can move their systems and data off legacy systems and into the cloud, are likely to benefit from greater efficiency and improved interoperability.[17] Cloud services allow banks to avoid building costly on-premise data centres that cover peak-level computing burdens and, instead, allow them the flexibility to accommodate seasonal fluctuations in the need for computing. Moreover, assuming a client bank selects appropriate security and resilience configurations, a cloud service provider can often offer an IT environment that is at least as robust from an operational resilience perspective as an individual bank's own on-premise data centre. In principle, economies of scale could help cloud service providers achieve a high degree of redundancy, geographic diversity, and advanced security and engineering at a much lower cost compared with most individual banks.

Recent surveys of banks and other financial firms suggest that a growing share of institutions use cloud computing for various purposes, including regulatory data, business operations and applications.[18] While there may be significant differences in the degree of cloud adoption across banks within a jurisdiction, supervisors have reported a significant increase in the number of banks using cloud computing services in recent years, and that this trend is expected to continue. This could, in part, be attributed to banks fast-tracking their digitalisation plans as a result of the Covid-19 pandemic.

Most banks using cloud computing services started out with Software as a service (SaaS), but many are now also using Infrastructure as a service (IaaS) and Platform as a service (PaaS), and have become comfortable with using the public cloud. The types of workloads that have moved to the cloud also vary from bank to bank. Some banks have moved only low-risk workloads to the cloud, while others are starting to move even their core banking systems. A few banks – particularly digital banks – have all their systems in the cloud, while other banks have now adopted a cloud-first strategy for new products and services.

Box 5

Cloud-only bank in Japan

Minna Bank, which was established in 2021, is a digital bank that runs entirely on the public cloud. Google Cloud is used for core banking systems, Amazon Web Services is used for the contact centre domain and Microsoft Azure is

[17] Petralia et al (2019).

[18] CSA (2023); ABA (2021); Accenture (2022).

used for virtual desktops used by employees. The bank chose the multi-cloud option to build a system that combines the best features of different cloud services. Digitally native customers, who are moving away from traditional face-to-face banking transactions, are expected to make up the majority of the working age population in Japan by 2030. Accordingly, Minna Bank was established as a part of the Fukuoka Financial Group, a large regional financial group encompassing three regional banks, to target digital natives nationwide. Minna Bank has a strategic focus on the provision of financial services (deposits, debit cards and small loans for individuals) through smartphones.

3. New competitors and business models

Advances in financial technology have coincided with the emergence of new entrants and new business models. To date, these developments have affected the banking system primarily through: (i) competition from new entrants (particularly in payments services); and (ii) the formation of strategic partnerships between banks and other firms. This section reviews the role of these entrants and the evolving business models of banks.

3.1 New entrants

Innovative technologies have facilitated the entry of new digital-only participants ("neobanks"),[19] fintechs and larger technology companies ("big techs") into the provision of banking and financial services. These firms often have an advantage in data and technology relative to traditional banks (eg digitally native platforms without legacy IT systems),[20] and may not be subject to prudential regulation or supervision.

Neobanks aspire to compete with traditional banks by better customising online products and delivering services faster. They typically target individuals, entrepreneurs and small and medium-sized businesses, and offer a range of services including deposit and business accounts, credit cards, financial advice and loans. As they are unencumbered by legacy infrastructure, they may be able to leverage new technology at a lower cost, more rapidly and in more modern formats. While unencumbered by legacy systems, neobanks may face other challenges including less stable deposit funding.[21] In some markets, neobanks are not licensed as banks and partner directly with incumbent banks (see Section 3.2). Several large incumbent banks have also launched neobanks as subsidiaries to offer digital-only services. To date, neobanks' share of banking assets remains small in most jurisdictions.

Fintechs often specialise in offering a particular product or service that targets a specific segment of the banking value chain. They mostly rely on digital channels such as social media and websites, or partnerships with local financial institutions, to acquire customers.[22] Reportedly, the greatest number of fintech companies offer lending and payments services, followed by enterprise tech provisioning, capital raising and wealthtech.[23] Payments are expected to remain the largest fintech segment by revenue in 2030, followed by lending, insurance, deposits, investments and financial infrastructure.[24] While fintechs remain

[19] In some jurisdictions, the term "neobank" is used to describe digital-only banks which are subject to the same rules as "traditional" banks, while in other jurisdictions it refers to digital-only participants which may not themselves be insured deposit-taking institutions.

[20] Petralia et al (2019).

[21] Online applications can enable customers to move funds more easily (Koont et al (2023)).

[22] World Economic Forum (2024).

[23] Cambridge Centre for Alternative Finance (2023).

[24] BCG and QED Investors (2023).

small relative to traditional financial institutions, they are continuing to expand, particularly in higher risk segments of the financial system.[25]

Big techs are large technology firms offering digital services that rely on data analytics, network externalities and interwoven activities, to bring in more users and provide more value to users. This, in turn, produces more data, which helps enhance services and user experience to attract even more users. Examples of big tech platforms include e-commerce platforms, social networks and search engines.[26] Big techs have expanded rapidly and are significant providers of financial services in several countries, particularly in the provision of payments.[27] They have the potential to become dominant competitors in financial services, given the advantages conferred by their collection of data and large established networks.[28]

Box 6

Big techs in Latin America: Mercado Libre

Mercado Libre is an online marketplace platform whose strategy revolves around leveraging technology to democratise commerce and financial services. It has over 100 million active users and operates in 18 countries across Latin America, applying a localisation strategy in which it tailors its platform to each country's preferences and needs.

Mercado Libre is the commerce business which connects buyers and sellers and generates revenue through transaction fees, sales commissions and advertising services. Mercado Pago is its digital financial services platform that offers payments, simple investment products, insurance and a crypto wallet. It also provides services to merchants including mobile point of sale and quick response (QR) code payments. Mercado Crédito provides credit products (including credit cards, consumer loans and merchant loans) to users within its ecosystem. To assess the creditworthiness of borrowers, it has developed credit scoring models using transaction data from its platforms. Mercado Pago holds different financial institution licences in the various jurisdictions in which it operates but is generally not regulated as a bank.

For consumers, new entrants may expand access to financial services (ie improve financial inclusion), reduce transaction costs, provide greater transparency with simpler products and clear cost disclosures, provide greater convenience and efficiency, and enable tighter controls over spending and budgeting.[29] These firms are generally considered to be more agile by being able to respond to market demand and providing a better user experience compared with incumbent banks. Nevertheless, some firms may seek to become regulated banks to access certain benefits that accrue to regulated entities, such as deposit insurance, access to central bank accounts and access to other key financial system infrastructure (eg certain payment systems).[30] For example, the Covid-19 pandemic exposed weaknesses in certain non-bank funding models, which may make the ability to access deposits by obtaining a banking licence more attractive.[31] Other non-banks may seek to access these benefits through partnerships with

25 Cevik (2023).

26 Doerr et al (2023).

27 For example, in China, Indonesia, Kenya and Korea (Doerr et al (2023)).

28 Petralia et al (2019).

29 Fintechs often target traditionally underserved customers, such as female, low-income and rural customers (World Economic Forum (2024)).

30 This could occur through either acquiring an incumbent bank (eg Lending Club's acquisition of Radius Bank) or by being licensed as a bank (eg Zopa) (Ben Naceur et al (2023)).

31 For example, fintechs that were more reliant on investor funding struggled to access this in the early stages of the pandemic (FSB (2022b)).

banks (see Section 3.2). Furthermore, as many of these firms are not licensed as deposit-takers, they cannot engage in maturity transformation and are more reliant on fee income for revenue.

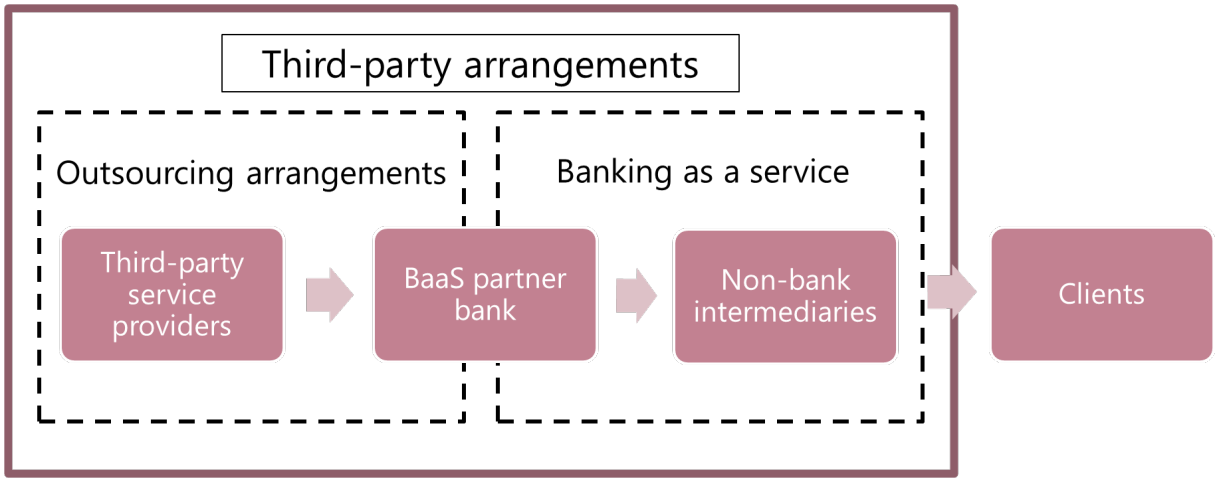
3.2 Banking partnerships

Banks are increasingly partnering with non-banks and technology firms to deliver products and services across different parts of the banking value chain. These partnerships can improve banks' operational efficiency, expand their product offerings and distribution channels, and strengthen customer relationships.[32] Many of these partnerships are facilitated by the use of APIs, which allow third parties access to banks' internal systems and infrastructure.

Banking as a service (BaaS) describes the provision of banking services by banks through non-bank intermediaries (eg fintechs, big techs and other firms) that serve as the interface to clients. While the network of entity relationships in these partnerships can be complex, generally they include:

- **Banks:** providing banking services to non-bank intermediaries. The most common functions performed by partner banks are holding deposits, processing payments and extending credit.
- **Platform providers:** such as non-bank technology companies that provide the infrastructure needed to connect banks with non-bank intermediaries. Some banks use their own proprietary infrastructure rather than a platform provider's software.
- **Non-bank intermediaries:** may include fintechs, big techs or other non-financial firms (eg retailers or online marketplaces). These non-banks act as the direct interface to customers.

Graph 5: Banking as a service (stylised example)



Banking partnerships aim to exploit the comparative advantages of the bank and non-bank partners. Banks have infrastructure, expertise and regulatory permissions which are usually expensive to replicate. Meanwhile non-bank intermediaries bring advantages in product development, data analytics and user experience. If successful, these arrangements may result in better, faster or more efficient services than those currently offered by banks on their own. In such cases, both the banks and non-bank intermediaries can profit from increased business, and consumers and businesses can benefit from increased competition resulting in greater efficiencies, lower prices and more innovation.

[32] Petralia et al (2019).

Box 7

Banking as a service platform providers in the United States

In the United States, platform providers such as Synapse, Synctera, Treasury Prime and Unit design and develop banking software solutions. While the business models are evolving rapidly, these providers generally offer an all-in-one solution that provides the technology, platform, coding and sponsorship arrangement that enable fintechs, embedded finance and banks to connect to each other via application programming interface (API) infrastructure, or other secure means, and offer payment, deposit, lending, identity verification, card issuance and investment services directly to end users. Platform providers may also facilitate other ancillary services, such as anti-money laundering and know your customer checks.

APIs allow fintechs to launch and scale financial products, and banks to automate and extend back-end operations. Non-financial companies can also embed these products with current services and products through API integration.

While BaaS does not currently represent a significant portion of the delivery of banking services, there is variation across jurisdictions. Many banks that currently focus on BaaS are relatively small, although there are notable examples of larger banks engaged in BaaS. Among other factors, smaller banks can face specific challenges that lead them to engage in BaaS arrangements, such as an inability to afford technology upgrades and competitive pressures. BaaS arrangements can allow smaller banks to expand and diversify their customer base, ie beyond a particular region or market, and outsource specific functions that may be undertaken more efficiently by a third party (eg customer onboarding, verification and credit scoring).[33]

4. Risks

Sections 2 and 3 of this report considered the different applications of innovative technologies and their potential benefits. For banks, many of the opportunities afforded by new technologies relate to innovation, efficiency gains and enhanced risk management capabilities. For consumers, digitalisation holds the promise of expanding access to financial services (ie improving financial inclusion), reducing transaction costs, improving customer experiences and increasing competition. While digitalisation can benefit both banks and their customers, it can also create new vulnerabilities and amplify existing risks to banks, their customers and financial stability. These potential risks and vulnerabilities are considered in greater detail below – note that the ordering is not intended to reflect relative materiality.

4.1 Strategic risks

Banks may face challenges in adopting strategies needed to remain competitive and profitable in an increasingly digital environment. Increased competition from non-bank competitors (eg fintechs and big techs) that offer financial services bundled with other services, together with open banking/finance regimes that facilitate portability and induce switching, may reduce banks' market share and revenues, and erode bank profitability. In response, banks may seek to either develop their own technological capabilities, partner with new entrants to increase their digital offerings or otherwise look to diversify their revenues (eg through strategic partnerships with non-financial services firms such as e-commerce platforms). These strategies may, in turn, exacerbate certain risks.

[33] Ben Naceur et al (2023).

Large-scale digital transformation projects carry both strategic and operational risks. While many banks have been increasing their technological capabilities, efforts have been impeded by problems with legacy infrastructure and a lack of staff expertise. In this regard, smaller banks may be particularly vulnerable as they generally lack both the financial and technical resources to improve their digital capabilities. An inability to improve digital capabilities could put banks at a competitive disadvantage relative to more nimble, digitally native entrants.

Bank partnerships with non-banks or other technology-focused firms may also give rise to strategic risks. Dependencies on non-bank entities for the origination of business could leave banks vulnerable to loss of control over volumes, product design and origination processes, while remaining accountable for risks. In certain arrangements, banks may lose ownership of the customer relationship and thereby risk the possibility of non-bank partners taking their customer base elsewhere, which would result in a sudden loss of business for the bank with potentially significant implications for the bank's liquidity and financial performance. Bank partnerships may also give rise to narrow banking models in which banks provide only a limited set of services (eg deposits or payments) to non-banks. This lack of diversification could create business model and balance sheet vulnerabilities, such as an over-reliance on fee income.

4.2 Reputational risks

Banks' use of certain technologies and partnerships with non-banks or other interactions with third parties may also lead to heightened reputational risk. Reputational risk may arise from operational failures, or failures to comply with relevant laws and regulations, and can be particularly damaging for banks as the nature of their business requires maintaining the confidence of depositors, creditors and other market participants.

Banks may face reputational risk where they rely on certain models or automated processes. For example, the use of complex AI/ML models and their lack of transparency, may increase the risk of unfair or discriminatory outputs which could lead to considerable adverse publicity as well as regulatory penalties.

In BaaS arrangements or other interactions with third parties, issues with non-bank partners or service providers could affect the bank's business or operations, and its reputation among consumers, investors and professional service providers. This could potentially limit a bank's ability to, for example, obtain liquidity or professional services from external parties. Even where liability is clearly assigned between a bank and third parties, banks may still face considerable reputational risk in the event of customer grievances, eg when customer data are compromised as banks are often viewed as the custodians of customers' data.

In response to reputational risks, banks may also face "step-in" type risks. For example, a bank may feel obliged to act to maintain continuity of service and/or to protect the values of end-users' assets in cases of financial distress with non-bank partners.

4.3 Operational risks

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events (including legal risk, but excluding strategic and reputational risk).[34] Operational risks can manifest in a variety of different ways. Digitalisation-related developments share certain common features that introduce additional complexity in the delivery of banking services, and that could exacerbate or amplify operational risks, including:

[34] BCBS (2021a).

- **Model risk:** the use of AI/ML gives rise to potential model risks.[35] While these may present similarly to other analytical methods, they may also amplify (or introduce novel) risks depending on the specific use case. Certain AI approaches may exhibit a lack of explainability, including the ability to attribute the model's decision in each case to the most important variables (or "features") influencing the outcomes,[36, 37] or, in jurisdictions which require it, the specific factor(s) driving an adverse action. AI/ML approaches also have the potential to be "overfit" – that is, they hew too closely to the data on which they were trained and may not generalise to other conditions or circumstances. The use of AI/ML can also reflect biases and inaccuracies in the data they are trained on, and potentially result in unethical outcomes.
- **Technology risk:** banks' legacy IT systems may not be sufficiently adaptable, or implementation practices, such as IT change management, may be inadequate to support the use of new technologies. The integration of new technology with legacy systems can also add additional layers of complexity. Banks may also face challenges related to vendor lock-in risk and a lack of transparency of proprietary technology or models.
- **Cyber risk:** new technologies and new business arrangements can increase cyber risks if controls do not keep pace with change. Bank systems have multiple points of contact with outside parties, which provide potential interfaces and entry points for cyber attacks.[38] A heavier reliance on APIs, cloud computing and other new technologies which facilitate increased interconnectivity with actors or sectors not subject to equivalent regulatory expectations, could make the banking system more vulnerable to cyber threats.
- **Legal uncertainty:** certain technologies and use cases are testing the application of existing legal frameworks. For banks, this can introduce risks relating to: (i) legal certainty and the status of certain products (eg digital asset tokens), as well as the corresponding regulatory requirements; and (ii) accountability and liability, eg decisions made by AI or executed under a "smart contract" using DLT may challenge the conventional attributions of accountability and liability to "legal persons" (ie an individual or corporate entity).
- **Compliance risk:** banks that rely on non-bank partners to undertake KYC and AML checks may be exposed to heightened compliance and legal risks if the processes of the non-bank partners are not appropriately vetted. Similarly, banks may face increased compliance risks where they engage with cryptoassets or DeFi as the trustless nature of public DLTs introduces several risks related to money laundering, terrorism financing and other illicit uses.[39] Consumer compliance risks may also be exacerbated by certain characteristics of AI applications, such as difficulty in explaining the outcomes of a model.[40] BaaS arrangements may also elevate risks associated with

35 See BCBS (2022a).

36 A key concern with lack of explainability is the difficulty in assessing the conceptual soundness of an AI/ML approach, ie to assess the theory, design, methodology, data and development testing.

37 Issues relating to explainability may be exacerbated in the case of dynamically updating models (ie an AI approach that updates on its own with little or no human intervention), in which it may be harder to see exactly where and how the approach has modified itself.

38 BCBS (2018b).

39 While transactions can be traced and verified on the blockchain, this process occurs in an anonymous or pseudonymous way, without recourse to the real identity of the participant (OECD (2022)). Additionally, illicit actors are using anonymity-enhancing technologies (eg mixers and tumblers) to obfuscate the details of financial transactions. There are significant risks for those transacting in DeFi that they might engage with a sanctioned counterparty or with cryptoassets sourced through illicit activity (IOSCO (2022)).

40 FSOC (2023).

timely error resolution, inaccurate representations of deposit insurance or other unfair or deceptive practices.

- **Fraud-related risks:**[41] digitalisation can also facilitate new types of fraud, with fraudsters deploying more sophisticated techniques to target bank customers. This can include, for example, the use of deepfakes (a type of synthetic media technology that uses AI to manipulate or generate visual and audio content that appears real) to commit account takeovers, loan fraud or wire fraud.
- **Third-party risk:** banks are increasingly engaging with, and often rely on third-party service providers for operational support of technology-based financial services.[42] While outsourcing can reduce costs and improve operational flexibility, it can also amplify issues relating to information and cyber security, privacy and operational resilience.[43] Bank oversight of third parties can be limited in cases where banks have no contractual relationship with the third party (eg in the case of transactions on public blockchains, participants are operationally dependent on parties that cannot be identified or controlled), or where the third party has no regulatory authorisation (eg under certain open banking frameworks). Banks may find it challenging to exercise effective oversight and monitoring over these third parties.

More generally, operational risks may be exacerbated by poor governance and risk management practices. Risks could be heightened where banks' governance frameworks are not modified to adapt to new technologies; there is inappropriate accountability and responsibility; a lack of technological literacy, including the inability to attract, build and retain talent; poor oversight of data governance; and use of systems and applications developed by third parties. Effective management of operational risks is important to minimise potential operational disruptions and their impact on banks' operational resilience.

4.4 Data issues and related risks

Many new technologies and applications are data intensive and leverage new data sources – or existing data in new ways[44] – which may exacerbate banks' data governance challenges. In particular, the volume, velocity, variety, quality and integrity of data may heighten data governance risks.

Alternative data generally means non-traditional data or data not typically used to date by banks. For example, it can include utilities billing and payment information, as well as images, audio, video and social media information. Alternative data raise specific risks and challenges for banks' data governance, including use of data without a long history (and whether they will continue to be predictive and explainable though the lifecycle of the data or with changing conditions); issues with privacy and consent (especially obtaining customer consent upfront); and potential bias within the data. The use of alternative data in combination with AI/ML applications may also exacerbate bias and explainability concerns.

In addition, the use of new data sources or techniques may also present challenges in integrating these processes with legacy risk management processes. For example, the use of new data to underwrite credit products may be challenging to integrate with existing credit loss modelling when assessing the adequacy of allowances for credit losses.

Increased interconnectivity and the sharing of data between banks and third parties creates potential challenges for data security and protection, and may introduce additional vulnerabilities as different parties access a bank's data. This may increase the possibility of data breaches and result in a

41 For a more detailed discussion of digital fraud, see BCBS (2023).

42 See BCBS (2022b).

43 In the case of cloud services, additional concerns regarding the geographical location of data storage may inhibit banks' use of the cloud, particularly when it comes to migrating their core or critical workloads.

44 For example, the use of deposit account transaction data to construct cash flows for loan underwriting.

larger surface area for cyber attacks. New partnerships with non-banks may also present unique and potentially complex risks surrounding data ownership and accessibility. For example, in some jurisdictions the end user in a bank-fintech arrangement may also be a customer of the bank, necessitating the bank's collection of certain information on the arrangement's end users to understand its own compliance obligations and risks even in instances where the bank does not have a direct relationship with the fintech's end users. Some fintechs may differentiate between types of data, such as data about a customer and data about the customer's account, viewing some of it as proprietary and unnecessary to share with a bank that it views as a service provider. This may, in turn, inhibit the bank's ability to fulfil its regulatory requirements (eg account and transaction monitoring for AML/CFT).

4.5 Financial stability risks

New technologies, applications and the entry of new suppliers into financial services may also give rise to broader banking system and financial stability risks, particularly where activities may scale rapidly. These could include:

- **Increased interconnections:** the use of innovative technologies typically leads to greater interconnectivity and more interdependencies between market players (ie banks, fintechs and technology firms) and market infrastructures. This adds complexity and opacity, which can make it more difficult for supervisors to identify, assess and respond to risks. Moreover, the complexity of these networks and chains of interconnection are yet to be tested in an economic downturn.[45]
- **Regulatory arbitrage:** material growth in the provision of banking-like services by non-banks that are not subject to prudential rules or oversight could undermine authorities' ability to identify risks and the efficacy of supervisory tools to address financial stability risks. Where non-banks are not subject to equivalent regulatory expectations (eg technology and cyber risk management standards), they could introduce additional vulnerabilities into the banking system. Further, as different regulatory regimes evolve at different speeds, the risk of regulatory arbitrage may also increase.
- **Contagion:** technological advances increasing the speed with which financial transactions can occur, coupled with the real-time transmission of information through digital channels, may increase the speed with which contagion may spread across institutions or markets. The emergence of multiple forms of digital money (including tokenised money), may also increase the risk of contagion to bank deposits.[46] Increased interlinkages between the crypto/DeFi ecosystems and the traditional financial system – for example, due to banks issuing stablecoins, holding deposits for stablecoin issuers or tokenising assets – could increase the potential for spillovers and contagion between the two systems. While bank exposures to crypto and DeFi are currently small, banks could be exposed to stress in these markets through their lending activities, liquidity and funding, or where they offer other crypto-related services.[47] Contagion could also emerge through the novel use of tokenised traditional assets, eg through the use of tokenised money market funds as collateral or payment mechanisms.
- **Amplification of financial risks:** digitalisation-related developments may also amplify more "traditional" financial risks. Liquidity risks could be affected in various ways. For example, liquidity

[45] Cevik (2023).

[46] For example, retail customers could be easily confused if banks were to offer non-deposit forms of money (eg stablecoins) alongside deposits, and mistakenly assume that they have the same protections. Any event that prompts retail customers to lose confidence in a non-deposit form of digital money may spillover to a broader loss of confidence in bank deposits (Bank of England (2023)).

[47] FSB (2022a, 2023a).

stress may become more acute due to the speed at which deposits can be withdrawn; the use of tokenised assets could increase intraday liquidity needs; and fintechs' reliance on banks to hold reserves or maintain operating accounts could precipitate liquidity and/or other stress on the bank's financial condition if the fintech were to fail or to leave suddenly. The use of automated models may also encourage and amplify procyclical behaviours. For example, the use of smart contracts which automatically liquidate collateral could amplify declines in asset values, while the use of AI for trading activities could amplify swings in market prices and more rapidly propagate shocks.

- **Fragmentation risks:** the proliferation of new infrastructure (eg DLT) increases risks of interoperability and potentially market and liquidity fragmentation. Private alternatives to sovereign fiat currency may become dominant, issued by actors who are not accountable to the public and may not support the stability of the financial system.
- **Concentration risks:** concentration risks may arise in the form of market infrastructure (eg the Ethereum blockchain), models (eg foundation AI models) or third parties (eg cloud service providers and AI model developers). Flaws in infrastructure or model errors could have system-wide impacts, while outages at (or in extreme cases, failure of) a systemically important service provider could result in significant disruptions across the banking and financial systems.[48]

[48] For example, there have been past instances of outages at large CSPs that affected multiple customers and locations (Reuters, 2023 and RSM Stone Forest, 2023).

Box 8

Generative AI risks

Generative AI (GenAI) exhibits many of the same risks as other AI but these may present differently or more significantly with GenAI depending on the specific approach used. Specific risks may include:

- Model risks: GenAI may be susceptible to reasoning errors and cognitive limits,[49] as well as "hallucinations", ie the generation of responses that are factually inaccurate. Further, it may not produce consistent responses over time, even when given similar questions or prompts.
- Explainability: these models are complex and opaque, relying on hundreds of billions of parameters which can make it more difficult to explain the model's outcomes. Explainability techniques that have been used for "traditional" AI models may not be appropriate for GenAI.
- Data governance: the use of GenAI can increase the challenge of sound data governance given the very large data sets, which in some cases the banks do not control or cannot fully evaluate. GenAI may also rely on data that have shortcomings in terms of quality, suitability or reliability, and may also reflect – and even augment – human biases. Moreover, given the larger volume and variety of training data, issues around privacy and copyright are more pronounced.
- Governance and accountability: banks' governance frameworks and processes may not be adequate for GenAI usage. Banks may lack the appropriate skills and knowledge to build, scale and integrate foundation models, or to provide effective oversight.
- Third-party risks: banks may increasingly rely on third-party model providers because they lack the skills and resources to develop these models in-house. When banks use vendor or open source models, this can raise issues related to transparency, privacy and security and may also heighten cyber security risks. The allocation of responsibility and liability between the bank and vendor may also be unclear.

From a financial stability perspective, the broad adoption of generative AI may also lead to increased interconnectivity and interdependencies across the financial system, the amplification of traditional financial risks, including procyclical behaviours, and greater third-party concentration risks, particularly where the model vendors are also providing cloud services to banks.

5 Banks' risk management

Banks have adopted various strategies and practices to mitigate the risks arising from the digitalisation of finance, which are explored in further detail in the following sections. These practices are not universal and many are still evolving. Moreover, for many of these potential risk mitigants, their efficacy has not yet been tested through different phases of the business cycle or periods of stress.

5.1 Governance and risk management

Effective governance structures and risk management processes are fundamental to identifying, monitoring and mitigating risks associated with the digitalisation of finance.[50] These structures and processes may include:[51]

- Robust strategic and business planning processes that allow banks to adapt their business strategies to consider the potential impact new technologies and market entrants may have on

[49] See Perez-Cruz and Shin (2024).

[50] BCBS (2024).

[51] BCBS (2018a).

their revenue. Many banks are investing heavily to improve their own digital capabilities and improve their overall cost efficiency.[52]

- Staff development processes that ensure that bank personnel have the appropriate awareness and capability to manage financial technology risks.
- Sound new product approval and change management processes to appropriately address changes not only in technology, but also in business activities.
- Risk management processes in line with the Committee's *Revisions to the principles for the sound management of operational risk* (PSMOR)[53] and *Principles for operational resilience* (POR)[54] that are relevant to financial technology developments.
- Processes for monitoring and reviewing new products, services or delivery channels for compliance with applicable regulatory requirements, including, as appropriate, those related to consumer protection, data protection and AML/CFT. Outcomes under a range of contingencies are considered and are legally enforceable.
- Robust strategic IT processes that define how the bank's IT landscape should adapt to support the business transformation.
- Effective risk management and control environments that address new sources of risk stemming from all risk areas.

Box 9

API usage

Some banks are mitigating risks associated with their application programming interface (API) usage by adapting existing controls to assure robust and risk-based information technology risk management and the overall safety and soundness of outsourcing/third-party relationships. This may include initial and ongoing due diligence, secure coding practices, end-to-end encryption of data in transit and at rest, strong and layered authentication and access management protocols, logging of API activity, security audits and penetration testing.

Prior to granting access to their systems, banks may implement API practices, or other mechanisms specific to APIs, for controlling access to, and data flow between, the bank and third parties. More specific practices include:

- granting access to APIs according to the principle of least privilege (that is, strictly limiting access to services to what is needed only);
- use of API gateways and certificate pinning to manage connections to, and exchange of, data between banks' and other parties' systems;
- refraining from directly embedding API keys into code to prevent accidental exposure and storing API keys in a location outside the application's source tree;
- restricting use of API keys (eg to internet protocol (IP) addresses, verified uniform resource locators (URLs) and mobile applications) to reduce the impact of a compromised API key; and
- periodically regenerating API keys and updating applications to use the new keys only and deleting unnecessary API keys.

[52] There is some evidence that such investments in digital innovation can help mitigate the impact of competition from fintechs (Chen et al (2019)).

[53] BCBS (2021a).

[54] BCBS (2021b).

Box 10

Distributed ledger technology

Since distributed ledger technology (DLT) use cases are still mainly in exploratory stages, full risk management frameworks for specific DLT-related activities are not generally available at the current juncture. However, some banks are mitigating DLT-related risks through the application of risk and control frameworks to suitable governance subjects, reporting and monitoring frameworks, escalation frameworks and business continuity arrangements.

At present, DLT is generally being used to expand existing business cases rather than for completely new business (eg trading of cryptoassets instead of trading of traditional financial instruments and custody of cryptoassets instead of custody of traditional financial instruments). As such, existing risk management frameworks are being used and adjusted to reflect the risks associated with these expanded applications.

Additionally, some banks have innovation and fintech accelerator programmes in place aimed at supporting and promoting fintech startups by providing resources, mentoring and collaboration opportunities. In these programmes, both risks and opportunities are analysed. In other cases, banks are collaborating with third parties to explore DLT for different use cases. This collaboration may assist banks in gaining a better understanding of the technology and its potential applications.

Those banks that are more advanced in the adoption of DLT tend to use a phased and risk-based approach to determining the risk mitigating measures required. In these cases, banks usually first conduct pilots and proof of concept (PoC) exercises before moving to full-scale production, so that they can more concretely identify cyber security requirements, or any legal/data privacy issues, and ensure that they remain compliant with supervisory expectations. Some banks have also operated these pilots under different supervisory sandboxes, which enables them to obtain supervisory guidance earlier in the exploration process.

In some jurisdictions, banks are required to comply with minimum cyber security requirements and to establish sound and robust technology risk governance frameworks to maintain cyber resilience. This includes the implementation of secure coding, robust cryptographic key management, and controls to ensure the availability and security of information technology systems.

5.2 Model risk management

Model risk management frameworks play an important role in banks' efforts to mitigate risks from AI/ML, and may consider, among other things, model impact (ie materiality), model complexity and model usage. For more material AI approaches, there is generally also greater human oversight ("human in the loop").

Given the complexity of AI models and other applications that use advanced algorithms, ensuring that banks understand the outputs of their models – including potential biases, limitations and robustness – supports effective decision-making, risk management and oversight. The appropriate level and type of explainability may vary depending on the specific use and user. Some banks are developing or using additional tools to help explain how the model functions and arrives at outputs (ie post hoc explainers), and in these cases, the limitations of these tools also need to be understood and taken into account.

Some banks are also updating their existing governance structures and risk management frameworks to manage the risks introduced by AI applications. For example, some banks have established executive committees that are responsible for the oversight of AI-specific issues, including ethics, fairness, performance and explainability.

For generative AI, some banks are adopting a risk-based and graduated approach and are focused on building out controls. To mitigate risks, banks are implementing various measures that generally build on their existing model risk management frameworks. These are summarised in Table 2.

Potential risk mitigants: generative AI

Table 2

	Approach	Specific practices
Internal processes and frameworks	Internal rules and policies	Banks establish firm-wide artificial intelligence (AI) policies.
		Banks act according to internal rules or manuals that set out the responsible use of generative AI (GenAI).
	Human oversight	Human review of the model's outputs, including training humans to know what they are looking for.
	Employee education	Promotion of employee training to ensure the risks and limitations of the models are known and to enable users to identify potential errors in the output.
	Enhanced validation	Requirement for more validation even for lower risk use cases.
	Enhancing governance structures	Formal approval processes in place for use of GenAI (eg use of such models is subject to approval by the information technology department and model risk management function).
		Risk management processes (ie data, model and operational risk) that ensure management's ability to identify, measure, monitor and control risks.
		Clear allocation of roles and responsibilities between model owner/developer/user and model validators.
		Establishment of dedicated committees to assess use cases, complementing existing governance structures.
Technology usage	Limitations on the use of GenAI	Restricting use to non-strategic, non-decision-making activities (ie permissible for low-risk activities only).
		Limiting use to applications which are installed locally to avoid sharing data with external parties.
		Blocking access to public online models (eg ChatGPT).
		Use of separate networks.
		Limit access to relevant data and/or limit the data that can be used for creating prompts to non-sensitive data.
		Bounding the model by imposing constraints on the output, eg anchored in ethical/responsible AI guidelines.
	Grounding the model	Implementing retrieval augmented generation (RAG) to limit the potential model outputs to a vetted library of documents.
		Testing outputs to check whether the source document (or contents within it) exists.
	Enhancing security of the technology used	Use of open source or third-party models is subject to adaptation and security checks (eg access through gateways that apply data and cyber controls).
		Training data for fine-tuning models is subject to quality control procedures.
		Models subject to ex ante tests and security reviews, and ongoing performance monitoring once deployed (eg use of sensitivity analysis to support explainability).
		Conduct detailed prompting studies and extensive user tests.
	Trace data sources	Only adopt models which can trace the original data sources of generated texts.
		Implement mechanisms to ensure original data sources are investigated.

Sources: BCBS survey 2024.

In addition, when third-party AI models are used, some banks may also apply additional risk mitigation measures. These could include security scans of models/algorithms, use of contracts to restrict

the use of personal data and ensuring that internal controls can appropriately address risks. Some banks have also developed evaluation frameworks for vendor models, that allow them to question the model, test its strengths and weaknesses, and identify potential biases. More generally, many banks subject the use of third-party applications to their broader outsourcing frameworks (see Section 5.6 for details on third-party risk management practices).

5.3 Data governance

Banks are adopting various methods to manage data-related risks, such as data breaches and privacy protections, associated with the use of innovative technologies. Some banks manage the risks of sharing data with third parties through master service agreements which set out requirements relating to data maintenance, access, rights, ownership and intellectual property, and security requirements. Banks also conduct due diligence on third parties to assess their data controls and may also engage in an ethical review process to understand how the third party will use the data. Some banks assign risk ratings to data based on the specific use case and may not share certain data with third parties based on its risk classification and tiering. In some jurisdictions, banks are required to use more secure methods for sharing data for certain types of accounts, such as tokenised authentication through APIs, rather than screen scraping or reverse engineering. These secure methods enable banks to exercise greater control over the type and extent of data shared, and enable more secure access management and monitoring.

In terms of their use of new data sources, while banks are generally adopting a cautious approach in their use of alternative data, some banks are also exploring how to address some of the associated challenges. Banks are generally applying their broader data governance and risk management frameworks to alternative data. These minimum standards may be augmented by additional considerations and controls for higher risk cases, such as where an outcome needs to be explainable to a customer. Some banks are also increasingly considering ethics in their data decision-making, ie not just "could" but "should" they use the data. Regarding its use in AI/ML applications, some banks are managing alternative data as part of their broader AI/ML governance processes.

5.4 Third parties

Banks are seeking to manage and mitigate the risks heightened by third parties through due diligence, operational risk management, ongoing monitoring and appropriate execution of contracts with service providers that set out the responsibilities of each party, agreed service levels and audit rights. Where banks engage in outsourcing, they should have appropriate outsourcing and contractual frameworks in place. Outsourcing frameworks should define the governance and risk management practices surrounding activities or functions that are outsourced.[55] Contractual frameworks are expected to define the rights, obligations, roles and responsibilities of the bank and the third-party providing the outsourced service.[56] Many regulations, for example, require contracts to guarantee banks' rights to inspect and audit their third-party providers. Some jurisdictions also grant these rights directly to supervisory authorities.

As the banking sector increasingly adopts cloud technology, banks recognise the importance of implementing robust measures to mitigate potential risks and ensure the security and resilience of their cloud usage. To address cyber security concerns, banks conduct thorough risk assessments to evaluate potential risks, such as those associated with multi-tenancy, data protection and supply chain vulnerabilities prior to onboarding to the cloud. Banks typically require cloud service providers (CSPs) to establish stringent security measures, encompassing key security domains including data encryption,

[55] BCBS (2005).

[56] BCBS (2024).

access controls and log monitoring, through contractual means, and assurance via third-party security assessments or certifications. However, under the shared responsibilities model of the cloud, banks also bear specific responsibilities in upholding cloud security. For instance, while CSPs may support encryption using banks' managed encryption keys (known as bring your own key (BYOK)), banks retain responsibility for generating, transporting and protecting their keys.

Banks have adopted different approaches to managing potential concentration risks. Some banks accept this risk, citing streamlined internal processes and reduced operational costs of running on a single platform. Other banks have adopted a multi-cloud strategy, which involves distributing their workload across multiple CSPs or employing a hybrid model that combines on-premise systems with cloud services. To address the risk of lock-in with a sole CSP, banks have developed comprehensive exit strategies (including preparing for a stressed exit) to facilitate a smooth transition in case of terminations.

Box 11

Cloud service providers

Banks' use of cloud computing requires enhanced technological expertise to understand and supervise these systems effectively, and an appreciation of the shared responsibility model when it comes to cloud security. For example, while one industry view is that a cloud service provider (CSP) is responsible for security *of* the cloud infrastructure itself, and banks are responsible for security *in* the cloud, a bank may need to understand the level of security and resilience that the CSP provides for its infrastructure. A bank may also need to address risk and business needs by selecting certain security and resilience options from the CSP. Cloud adoption could also result in limitations on access rights of banks and supervisors, thus hampering oversight activities.

One notable challenge in cloud computing is the dominance of a small number of cloud service providers in the market. This can limit banks' ability to switch service providers due to contract terms, lack of alternatives or technical interoperability issues. Moreover, the complexity of cloud deployment models can lead to limited visibility regarding a bank's operational and concentration risk exposure when a fourth-party CSP is involved (eg when the CSP is used by a third party as its underlying infrastructure service provider). Although audit requirements are often stipulated in framework agreements, their enforcement may raise practical challenges.

To address these challenges, some banks are collaborating through industry initiatives like the European Cloud User Coalition to collectively represent their interests in dealings with cloud service providers. Joint audits at cloud service providers are conducted through initiatives such as the Collaborative Cloud Audit Group. Various forums, such as Fachgremium Informationstechnologie in Germany and the Financial Sector Cloud Resilience Forum in Singapore, facilitate discussions between banks and supervisors on common problems and challenges, and foster a collaborative relationship with cloud service providers to ensure the industry's resilience in utilising cloud services.

6 Regulatory and supervisory initiatives

Regulations and supervisory frameworks and approaches have also evolved in response to the digitalisation of finance.

6.1 Regulatory frameworks

As the scope and nature of risks to banks and the banking system are rapidly changing, rules and regulations may also need to evolve. While many of the risks raised by the digitalisation of finance may be addressed by existing regulatory frameworks, others may require amendments to existing frameworks or the introduction of new standards and guidance.

Internationally, standard-setting bodies have issued new standards and guidance, and clarified the application of existing principles to ensure that risks are appropriately captured. To date, these have tended to focus on specific activities or sectors. For example, the Committee issued a standard on the

prudential treatment of banks' exposures to cryptoassets,[57] and new and revised principles on operational resilience and operational risk.[58]

National authorities have also issued new standards and guidance and/or clarified the application of existing requirements to bank activities impacted by innovative technologies and digitalisation. Many authorities have adopted a technology neutral approach, and apply general standards and guidelines on risk management, consistent with the principle of "same activity, same risk, same regulation".

The effects of digitalisation are cross-sectoral and cross-cutting. As a result, both supervisory authorities and banks operate within broader legislative frameworks that cover, for example, issues relating to data protection and privacy, cyber security and the combating of financial crime.

Scope of the regulatory perimeter

In some jurisdictions, legislative frameworks have expanded the scope of the regulatory perimeter. For example, some authorities have been granted the ability to regulate certain cryptoasset activities, including establishing cyber security standards and information exchange protocols, or setting and enforcing minimum standards for issuers of cryptoassets, including a minimum level of own funds for stablecoin issuers. A few supervisors have also been given direct oversight of critical information and communication technology (ICT) third-party service providers, including the ability to request relevant information and documentation, conduct general investigations and inspections, and issue recommendations relating to ICT risk.

Box 12

European Union legislative initiatives

The European Union has finalised, or is in the process of finalising, several legislative initiatives targeting digitalisation and innovative technologies. These regulations aim to provide consistent rules and reduce regulatory fragmentation by mitigating risks while at the same time fostering innovation by ensuring legal certainty for new technical solutions and related business models. Several of these legislative initiatives grant the supervisory authorities additional oversight powers.

The Digital Operational Resilience Act (DORA) aims to strengthen the information technology security of financial institutions and make sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption. The lead supervisory authorities will be granted oversight powers for critical information and communication technology (ICT) third-party service provides, which is likely to include the major cloud services providers. This will include powers to request relevant information and documentation; conduct general investigations and inspections; issue recommendations relating to ICT risk; and request reports specifying the actions that have been taken or the remedies that have been implemented by the critical third parties in response to the recommendations.

The Markets in Crypto-Assets Regulation (MiCA) aims to create a harmonised European regulatory framework for cryptoassets that promotes innovation by enabling cryptoasset activities while ensuring financial stability, market integrity and consumer protection. MiCA establishes requirements for issuers of cryptoassets and providers of cryptoasset-related services. Issuers of asset-referenced tokens and e-money tokens will also be subject to certain prudential requirements and supervision.

In March 2024, the European Parliament adopted the Artificial Intelligence Act (AI Act), which aims to foster trustworthy AI in Europe by ensuring that AI systems respect fundamental rights, safety and ethical principles. While the act is cross-sectoral in nature, banking supervisors will have a role in overseeing banks' compliance with the AI Act, particularly for high-risk use cases.

[57] BCBS (2022c). Other standard-setting bodies have also issued principles related to cryptoassets, including the FSB (2023b, c) and CPMI-IOSCO (2022).

[58] BCBS (2021a,b).

Licensing frameworks and conditions

Most authorities do not have separate or distinct requirements for licensing digital-only banks, but require all applicants to follow the same framework to obtain a bank licence. Many, however, apply a proportionate and risk-based approach which could allow for some adaptations for digital entrants. Many supervisors will also request additional information related to unique issues associated with a digital-only business model as a part of that standard licensing process. Some have also published guidance outlining principles that will be considered when the authority assesses applications to authorise digital entrants.[59]

A few jurisdictions have also implemented (or are consulting on) distinct processes or criteria for licensing digital-only banks.[60] These frameworks may permit licensees to be exempt from certain prudential requirements, particularly where they have commenced operations on a "restricted" basis before transitioning to a full banking licence. Some jurisdictions have also removed legislative impediments to digital-only banks, such as the requirement to have a (physical) main office with customer service, to support innovation in the sector.

In addition, authorities also have the ability to impose conditions on licensees on a case-by-case basis. For example, some authorities may require additional reporting relating to risks from new products (including technology-enabled products). Some jurisdictions also allow new entrants to operate on a limited basis as part of regulatory sandboxes, prior to obtaining a full banking licence.

Use of innovative technologies

Across jurisdictions, many supervisors rely on guidance covering technology risk management, operational risk management and operational resilience, model risk management, cyber and IT risk management, outsourcing/third-party risk management and corporate governance requirements, to guide banks' use of new technologies. Some jurisdictions have also introduced domain-specific guidance for the use of certain technologies, which is considered in Table 3.

Technology-specific supervisory guidance — Table 3

Technology	Guidance
Application programming interfaces (APIs)	In several jurisdictions, open banking/finance frameworks have been established under specific legislation that covers, for example, data-sharing, customer privacy and consent. In some cases, supervisory authorities have provided additional guidance on better practices, or have worked with industry to develop a playbook that covers common and useful APIs for the industry and cross-sectoral stakeholders.[61] In some jurisdictions, the supervisor has introduced a specific API framework[62] or issued API specifications.[63] In other countries, industry has led the development of standards that address issues such as interoperability, customer authentication, data standards and operational standards.[64]

59 See eg HKMA (2018).

60 For example, a new fintech licence has been introduced in Switzerland with less strict requirements compared with a traditional banking licence (FINMA (2023a)).

61 See ABS and MAS (2016).

62 For example, Bangko Sentral ng Pilipinas's *Open finance framework* includes standards on API architecture, data (including format, structure, and protection and privacy rules), security and outsourcing (BSP (2021)).

63 For example, the Reserve Bank of India has issued technical specifications on APIs through its wholly owned subsidiary Reserve Bank Information Technology Private Ltd.

64 For example, in the United States, industry consortia such as the Financial Data Exchange (FDX) have led the development of technical standards for APIs.

Artificial intelligence (AI) and machine learning (ML)	A few jurisdictions have issued specific principles or guidance on AI/ML, which establish frameworks for the responsible use of AI by banks.[65] Some supervisors have also clarified that existing requirements and guidance apply to AI, including requirements to manage operational risk, technology risk, model risk, IT/cyber risk and outsourcing/third-party risks, as well as more domain-specific guidance (eg relating to fair lending or the use of ML for internal ratings-based models). These principles and guidance generally promote a risk-based approach to AI; that is, requirements should be commensurate with the risk of the specific use case and the model's complexity. Most supervisors consider that these approaches are also appropriate to manage risks associated with generative AI. Some supervisors have also established public/private forums to explore the safe adoption of AI/ML and to develop principles which cover issues such as explainability, data governance and ethics.[66] One authority is also partnering with the industry to develop a risk framework for the use of generative AI in the financial sector.[67]
Distributed ledger technology (DLT)	Many supervisors have adopted conservative rules for banks' exposures to cryptoassets, including total prohibitions in some jurisdictions. Several supervisors have also issued supervisory statements highlighting risks associated with the cryptoasset sector. One supervisor has published guidelines that cover DLT-related activities, including the issuance of stablecoins, use of blockchain and staking activities.[68] Another has published specific guidelines on blockchain technology that cover risks relating to the consensus mechanism, smart contracts and security vulnerabilities.[69] Some countries have introduced regulatory sandboxes that allow banks to use DLT subject to limits on their activity and close supervision. Some authorities require prior notification to the supervisor of DLT activities, and require banks to demonstrate that the DLT activity will be conducted safely and soundly, and that adequate risk management systems and controls are in place prior to implementation. Regarding tokenisation initiatives, jurisdictions have adopted various approaches, including: prohibitions on the issuance of tokenised coins; strict separation between crypto and traditional financial markets (eg prohibitions on cross-collateralisation across the two systems); requirements to transact only on a common permissioned platform; and setting supervisory expectations for how banks should mitigate the risk of contagion to deposits, in the event that retail customers lose confidence in tokenised forms of money (eg stablecoins).[70] In some countries, legislation has been introduced that recognises the issuance of electronic securities (including those using central registers and those that are decentralised crypto securities registers). Other jurisdictions are working to understand how different tokenisation use cases fit within their current legal frameworks.

[65] For example, the HKMA and MAS have both published AI principles (HKMA (2019b); MAS (2018)).

[66] See eg OSFI (2023); Bank of England and Financial Conduct Authority (2022).

[67] See MAS (2023b), Project MindForge which focuses on the areas of: (i) accountability and governance; (ii) monitoring and stability; (iii) transparency and explainability; (iv) fairness and bias; (v) legal and regulatory; (vi) ethics and impact; and (vii) cyber and data security.

[68] FINMA (2019a,b, 2023b).

[69] Bank of Thailand (2021).

[70] Bank of England (2023).

Cloud computing	Several jurisdictions are evaluating cloud-related risks for financial institutions and service providers.[71] In addition to more general technology, cyber, outsourcing and operational resilience guidelines, a growing number of jurisdictions have issued cloud-specific requirements. These range from requirements that information transferred to the cloud be subject to a contractual clause and that different cloud-specific issues be considered to ensure data security, to more specific requirements around what can be stored in the cloud and on data location, data segregation, data use limitations, security and exit. More recently, some authorities are actively considering implementing direct oversight mechanisms for critical third parties, including cloud service providers. Most supervisors do not yet have such oversight powers, and so supervision is generally limited to how banks manage their services providers. However, a few supervisors have the ability to require reports from, and conduct on-site inspections of, outsourcing contractors of banks including CSPs, while others have been given powers to directly oversee the services provided by critical third parties to the financial sector.[72]
Bank partnerships and use of third parties	Many authorities rely on existing regulations and guidance related to governance and control of outsourcing/third-party relationships, IT security, operational risk and operational resilience to supervise banking partnerships and other arrangements with third parties. A few authorities have also developed more specific guidelines, for example, covering banking as a service models or the provision of banking services through social media platforms.[73] In some jurisdictions, banks may be required to obtain prior approval or a "no objection" from their supervisor before entering into certain partnerships or material arrangements with third parties.

Sources: BCBS survey 2024.

6.2 Supervisory approaches and tools

Banking supervisors are also reviewing and adjusting supervisory approaches and tools considering both the benefits and risks of digitalisation. Some of the common challenges identified by supervisors include:

- The technical complexity of many new technologies and a lack of specialist knowledge by supervisors, which is compounded by the speed of innovation.
- Limited oversight of certain activities and entities, and gaps in existing regulatory frameworks for addressing the full spectrum of risks. The cross-border nature of many activities and entities can further complicate effective oversight.
- Uncertainty regarding the legal status of certain products (eg tokenised assets and liabilities) and lack of comprehensive legal frameworks to govern the use of specific technologies (eg AI).
- Lack of standardisation and interoperability of certain technologies and networks (eg APIs and DLT) which can lead to fragmentation.

More generally, authorities are considering how to strike the right balance between enabling responsible innovation and mitigating potential risks or harms. Supervisors continue to be guided by a risk-based approach to supervision.

[71] For example, the United States Treasury has noted some challenges associated with greater cloud adoption, such as insufficient transparency regarding CSPs' security and operational environment (US Department of the Treasury (2023)). The Bank of England and Financial Conduct Authority have proposed requirements and expectations for critical third parties in the United Kingdom financial sector (Bank of England and Financial Conduct Authority (2023)).

[72] For example, in the United Kingdom, entities that are designated as critical third parties under the Financial Services and Markets Act 2023 may be subject to additional requirements and enhanced oversight (Bank of England and Financial Conduct Authority (2023)). In the European Union, the Digital Operational Resilience Act 2023 will establish an oversight framework for monitoring critical IT third parties.

[73] See eg BRSA (2021); HKMA (2019a).

Supervisory approaches

Supervisory approaches are evolving to respond to many of the challenges associated with the digitalisation of finance.

- **Strategy and frameworks**: some authorities have adopted digital supervision strategies that focus first on understanding and assessing digitalisation-related risks, before looking to strengthen the supervisory framework. Some supervisors are reviewing their frameworks to ensure that they continue to support their ability to take early corrective action in all risk areas, including digital innovation.
- **Organisation:** some authorities have initiated changes in their internal organisation of supervision functions to include specialist risk teams (eg cyber risk and operational risk) or specialist supervision teams that focus on new/specialist banks or novel activities or arrangements between banks and fintechs. Many authorities have also established fintech or innovation hubs as centres to focus on digital innovations and conduct workshops with stakeholders, develop research papers, conduct experiments (eg techsprints) and engage with industry. The introduction of new legislation governing digital activities (eg on crypto or AI) has also required supervisory authorities to allocate more resources to implementation and monitoring efforts.
- **Training and capacity building:** many authorities have implemented internal training programmes to educate and upskill supervisors on specific technologies and broader topics beyond traditional financial risks, such as those relating to data protection, privacy, discrimination and bias. Staff have also been supported to attend external conferences and specialised training courses. Some recruitment efforts have focused on hiring staff with expertise in IT and innovative technologies. To disseminate knowledge throughout the organisation, some authorities prepare and distribute internal awareness papers on topical technologies. One institution has introduced a supervisory digital finance academy and some rely on internal networks of experts.
- **Prior notification or approval:** many supervisors require notification by banks prior to their adoption of certain technologies, or entry into partnerships or other arrangements with third parties. Some supervisors require banks to seek prior approval for certain digital activities or arrangements.
- **Prudential reviews:** many supervisors are giving greater emphasis and focus to the discussion of technology and cyber risks and operational resilience in prudential reviews, and have conducted thematic reviews on digitalisation-related topics such as cyber security and IT risk.
- **Business model analysis:** several supervisors have cited an increased focus on understanding new and emerging business models, and assessing and understanding how non-traditional business models can pose risks to banking safety and soundness.

Supervisory tools

Many supervisors are also making greater use of technology, including suptech tools, to enhance their oversight capabilities and improve the efficiency of supervisory decision-making. Suptech tools take many different forms, but some common use cases include text analysis and summarisation, entity sentiment analysis, market surveillance and risk identification, credit risk challenger tools, outlier detection in AML inspections and the automation of certain supervisory processes. Some supervisors are also using suptech to monitor trends and risks across the fintech sector, including monitoring crypto and DeFi projects.

Some authorities are using suptech solutions to improve communication and clarity on regulatory requirements and expectations. Relevant examples include interactive chat-style "regulation as a service" interactions using AI to respond to queries from regulated entities.

Supervisory cooperation

Supervisors are increasingly engaging with other public and private sector participants on digitalisation-related topics and areas of interest. Given the cross-sectoral and global nature of digitalisation, cooperation with other domestic agencies and international standard-setting bodies is increasingly important.

As many elements of digitalisation raise broader public policy issues, supervisors have noted a blurring of the boundaries between prudential regulation and, for example, consumer protection, competition/anti-trust, financial crime and the need for close cooperation with responsible authorities. Banking supervisors are also collaborating actively with peer supervisors, both bilaterally and through regional and global forums, on topics of common interest.

Many supervisors have also recognised the importance of close cooperation and collaboration with industry, technology experts and academic institutions on digitalisation. This can take various forms, and includes bilateral or industry-wide engagements on thematic topics (eg cyber risk and operational resilience), and open door initiatives that aim to facilitate open discussions on innovation between the supervisor and industry. Some authorities have established public/private forums or industry partnerships to explore specific technologies, with a view to developing principles or guidance to address risks.[74] Others have partnered with industry on specific pilot projects. Many authorities have also established regulatory sandboxes, which allow banks to test new technologies in a controlled environment, while also allowing supervisors to benefit from a better understanding of the associated risks and benefits, and build internal expertise and skills. Some supervisors also regularly engage in dialogue with non-bank firms, such as critical service providers, to discuss the latest risks, trends and developments.

Some authorities have engaged in various efforts to promote and encourage digital innovation across the banking sector, including showcase events, roundtables, seminars and practical training sessions to encourage fintech adoption across financial services. One supervisor has established a fintech support desk that acts as a one-stop contact centre for consultations on legal interpretations, while another has conducted roadshows that aim to help strengthen the digital capacity of smaller and rural banks.

Box 13

Cross-border cooperation: Project Guardian

Project Guardian aims to develop and harness the benefits of the digital asset ecosystem in a sustainable and responsible manner. It is an international collaborative initiative between policymakers and the financial industry to test the feasibility of applications in asset tokenisation while managing risks to financial stability and integrity.[75] The areas of collaboration include:

[74] For example, the United Kingdom's AI public-private forum to explore safe adoption of AI/ML and whether principles, guidance, regulation or industry good practice would support this adoption (Bank of England and Financial Conduct Authority (2022)). Canada established a Financial Industry Forum on AI to advance the conversation around appropriate safeguards and risk management (OSFI (2023)). Singapore's Project MindForge aims to develop a framework that addresses risks of generative AI which could feed into supervisory principles (MAS (2023b)). Saudi Arabia has established a cyber anti-fraud programme to develop best practices and industry-wide standards for cyber security, data protection and technology risk management (Saudi Central Bank (2023).

[75] The financial institutions participating in Project Guardian are listed at: https://www.mas.gov.sg/schemes-and-initiatives/project-guardian

- Industry pilots with traditional financial institutions and fintechs in Singapore and other jurisdictions to understand opportunities and risk areas.[76] These include tokenised funds, asset-backed securities, bonds and tokenised bank liabilities as well as a cross-border foreign exchange payment solution using smart contracts with blockchain interoperability. The pilots will pave the way for integration across the capital markets value chain including listing, distribution, trading, settlement and asset servicing.
- Policy development: developing a rulebook and governance model, as well as reviewing legal and regulatory frameworks for tokenised assets.
- Technology standards: developing technical standards, ie trust anchors, open networks and institutional grade DeFi.

In 2023, Monetary Authority of Singapore (MAS) published two reports: *Project Guardian: enabling open and interoperable networks*[77] and *Interlinking networks technical whitepaper*.[78] The former was a joint report with the Bank for International Settlements to propose a framework for designing open, interoperable networks for digital assets (ie tokenised real-economy and financial assets). The latter was jointly developed with the industry to present a technical framework for exchanging digital assets across networks to address liquidity needs.

MAS established the Project Guardian Policymaker Group to partner with peer regulators in France, Japan, Switzerland and the United Kingdom as well as the International Monetary Fund, to explore the development of international standards and frameworks to underpin asset tokenisation.

7. Implications for banks and supervisors

The previous sections discussed the wide-ranging channels in which advances in digitalisation are impacting the banking system and their risks and possible mitigants. These developments have implications for banks, banking supervision and prudential regulation across a number of themes described below. These implications do not constitute formal standards or guidance.

Macro-structural considerations

1. **The evolving nature and scope of banking risks resulting from the digitalisation of finance and their implications for traditional financial risks.**

Advances in digitalisation and financial technology continue to transform the financial system landscape, including the provision of banking services. The digitalisation of finance presents both opportunities and risks for banks and supervisors. Risks and vulnerabilities may include both immediate risks and the likely medium- to long-term implications of activities and practices.

Digitalisation can amplify risks to banks, particularly strategic and operational risks, which increases the importance of having effective governance, risk management processes and control environments in place when adopting (or adapting to) new technologies. Digitalisation may also potentially alter risks to banks, making it important to consider the interactions of those risks in tandem with traditional financial risks.

[76] For example, UBS, SBI Digital Asset Holdings and DBS executed a pilot repo agreement with natively issued digital bonds, working across Switzerland, Japan and Singapore. Bank of New York Mellon and OCBC are trialling a cross-border foreign exchange solution to enable secure, interoperable payment solutions across heterogeneous networks.

[77] MAS and BIS (2023).

[78] MAS (2023a).

It is important that banks mitigate, and supervisors monitor, the evolving nature and scope of risks from the digitalisation of finance, and their implications for traditional financial risks.[79] A focus on risks associated with the digitalisation of finance does not reduce the need to monitor traditional financial risks and interactions between the two.

The Committee will continue to monitor developments in digitalisation and take action in accordance with its mandate. This may include enhanced monitoring, ongoing supervisory exchanges or developing new standards or guidance, where appropriate.

2. **Safety and soundness principles and the adoption of innovative technologies and business models.**

Digitalisation can benefit both banks and consumers. For banks, many of the opportunities relate to innovation, efficiency gains and enhanced risk management capabilities. For consumers, digitalisation can expand access to financial services, reduce transaction costs, improve customer experiences and increase competition.

As previously noted by the Group of Central Bank Governors and Heads of Supervision, the adoption of innovative technologies and business models should be guided by a principle of responsible innovation.[80] It is important for supervisors to strike the right balance between enabling responsible innovation, while also safeguarding the safety and soundness of the banking system and financial stability.

The Committee has adopted a precautionary approach that includes actively monitoring developments, considering risks and the adequacy of existing frameworks, and developing new standards and guidance when existing policy is considered inadequate. Some supervisory authorities have similarly engaged in various initiatives to promote responsible innovation, including risk-based monitoring of novel activities and arrangements, as well as issuing new, or clarifying the application of existing, rules and guidance.

3. **The digitalisation of finance is blurring the lines between banks and banking.**

Products and services that were previously offered exclusively by banks are now being provided by entities or applications that may not be subject to prudential regulation and supervision. This is challenging the traditional entity-based supervision paradigm.

If non-banks can offer products with better returns or lower costs than banks, it should be the result of real technology improvements and not the result of regulatory arbitrage. Integrating the principle of "same risk, same activity, same regulation" in regulatory and legal frameworks may help avoid regulatory arbitrage.

Some banking supervisors have been given expanded oversight of certain products and entities. However, even where supervisors do not have direct oversight of non-banks, they may still have a role to play, in line with their mandates, to the extent these entities and applications interact with regulated banks and present risks to banking and financial system stability.[81]A review by bank supervisors of their current supervisory frameworks in light of digitalisation-related risks, may uncover ways in which elements of these frameworks could evolve in a manner that ensures appropriate oversight of banking activities.[82]

79 BCBS (2024).

80 BCBS (2022d).

81 BCBS (2024).

82 BCBS (2018a).

Specific digitalisation themes

4. **Data as a critical resource.**

Many innovative technologies and applications are data intensive and leverage a wide variety of data sources. This makes data a critical resource within digital ecosystems, including for banks and supervisors.

The importance of data necessitates a commensurate level of safeguards by banks and supervisors. For banks, this includes implementing robust data governance frameworks and adopting secure methods for sharing data.[83] Supervisors can support effective data governance by assessing the range of practices across banks, and communicating on the implementation of better practices.

An increased reliance on data also raises broader public policy questions related to data collection and consent, privacy, bias, and security and storage. Many of these challenges cannot be solved by banks or supervisors alone, and may require cooperation and coordination with a range of public sector authorities.[84]

5. **The use of service providers.**

Banks' use of service providers has increased, and this trend appears likely to continue. Banks are engaging with service providers (which can include third parties, intragroup entities and other parties further along the supply chain) to deliver products and services across different parts of the banking value chain, and to enhance their technological capabilities. Greater reliance on service providers can increase operational risks for banks. It may also increase banking and financial system stability risks due to increased interconnections and potential concentration risks.

It is important for banks to implement robust risk management practices and processes over any operations performed by service providers in a risk-based and proportionate manner.[85] The specific controls will depend on the risks introduced by the activity as well as considerations such as the importance of the service to the bank's critical operations.[86] Controls over these services should be reviewed in light of the standard applied to operations that the bank itself conducts and in a manner that is commensurate with the risk introduced by the activity.[87]

Supervisors may also have a role to play in identifying common points of exposure across banks to operational risks or vulnerabilities, including reliance on common service providers. Supervisors should assess potential systemic risks arising from the concentration of services provided by specific service providers to banks.[88]

6. **The role of human judgment in bank risk management and supervision.**

One of the benefits of digitalisation is increased efficiency arising from the automation of processes. While increasingly sophisticated models and applications may be able to perform a wider range of tasks, human judgment remains important in bank governance and risk management, and in supervision.

Automation cannot remove responsibility or accountability for decision-making. Ultimate responsibility for appropriate risk management resides with the individuals that comprise a bank's senior

83 BCBS (2013, 2024).

84 BCBS (2018a).

85 BCBS (2024); FSB (2023d).

86 BCBS (2021a,b).

87 BCBS (2018a).

88 BCBS (2024).

management and board.[89] Human judgment can also be an important means of mitigating risks from the use of models (ie keeping a "human in the loop").

Supervisors may also use innovative technologies or "suptech" as a tool to improve their efficiency and to support their processes, but this should augment rather than replace the role of supervisory judgment. The use of innovative technologies should not diminish supervisors' ability and willingness to take actions to address unsafe and unsound practices, including those related to digitalisation.

Capacity building and coordination

7. **Resources, staff and capabilities.**

It is important for banks and supervisors to have the requisite skills and expertise to understand digital innovations, implement new technologies and manage or supervise the associated risks. This may include assessments of current staffing and training programmes to ensure that the knowledge, skills and tools of staff remain relevant and effective. It may also include the addition of new staff with specialist skills to complement existing expertise.

Banks and supervisors may benefit from public/private forums or other initiatives to explore innovative technologies and use cases, and build their understanding of the associated risks and benefits. Broader dialogue with technology experts, academia and other public sector authorities may also be mutually beneficial.

8. **Communication and cooperation with relevant authorities.**

Digitalisation raises issues that go beyond the scope of prudential supervision, including public policy objectives such as safeguarding data privacy, cyber security, consumer protection, fostering competition and compliance with AML/CFT. Communication and coordination among bank supervisors and other relevant regulators and public authorities, both within and across jurisdictions, is important to address these considerations.

As new technologies and technologically enabled suppliers increasingly operate across borders, international cooperation is also helpful to promote effective policy responses and to limit risks that could arise from regulatory fragmentation. Financial stability could be enhanced by furthering existing supervisory coordination and information-sharing, where appropriate. The Committee provides a global forum for such supervisory exchange and cooperation.

[89] BCBS (2024).

Glossary of terms

Alternative data: non-traditional data or data not typically used, to date, by banking organisations.

Application programming interface (API): a set of rules and specifications for software programs to communicate with each other, and an interface between different software programs that facilitates their interactions.[90] APIs can either be public (a standard that is known to the public) or private (a standard that is known only to a permissioned group), and are generally considered more secure than other data-sharing techniques.[91]

Artificial intelligence (AI): while there is no single definition of AI, it has been defined as tasks conducted by computers that previously required human sophistication.[92]

Banking as a service (BaaS): the provision of banking services by banks though non-bank intermediaries that serve as the interface with clients.

Big tech: large globally active technology firms with a relative advantage in digital technology. Big tech firms have typically established global operations and a large customer base, and can use a vast amount of information about their customers to provide them with tailored financial services.

Cloud computing: the use of an online network of hosting processors to increase the scale and flexibility of computing capacity. The characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity (scalability) and measured service.[93]

Cryptoassets: private digital assets that depend on cryptography and DLT or similar technologies.[94] As a digital representation of value, cryptoassets may be used as a means of exchange and store of value, or for payment, remittance and investment purposes.[95]

Data governance: the practices, policies and control structures a firm has in place to ensure that the data it uses are properly safeguarded, reliable and sound, of sufficient quality, used appropriately, accessible, and consistent with applicable laws and regulations – including consumer privacy and protection.

Decentralised finance (DeFi): solutions that utilise DLT to provide various services such as lending, investing, settling payments, insurance, asset management, and trading or exchanging cryptoassets, without the need for a traditional centralised intermediary.[96] Instead of relying on a central authority, DeFi relies on protocols that utilise smart contracts or decentralised applications running on a public network of computers to automate transactions. DeFi protocols are generally governed by a community of participants who claim to be organised through decentralised arrangements.

Distributed ledger technology (DLT): 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.

Large language model (LLM): a type of machine learning model that can perform a variety of natural language processing (NLP) tasks, including generating and classifying text, answering questions in a conversational manner, translating text from one language to another, summarising text, coding and

90 BCBS (2018a, 2019).

91 World Bank (2022).

92 FSB (2017).

93 NIST (2011); FSB (2019); FSI (2018).

94 BCBS (2022c).

95 FSI (2023).

96 Auer et al (2023).

solving mathematical problems. LLMs use deep neural networks to generate outputs based on patterns learned from training data. They identify relationships between words in a sentence (regardless of their position in the text sequence) by using self-attention mechanisms.

Machine learning (ML): a subset of AI in which algorithms optimise automatically through experience and with limited or no human intervention.

Neobanks: digital-only banks, which make extensive use of technology, big data and advanced analytics to offer banking services predominantly through smartphone applications or internet-based platforms.

Open banking/finance: the customer-permissioned sharing of banking data between the primary holder of those data (eg a bank) with third parties (eg payment initiators or account aggregators) to deliver value added service to customers. Open finance refers to the customer-permissioned sharing of a broader suite of financial data (eg mortgages, insurance products and investments).

Service providers: includes third parties, intragroup entities (ie entities within a group such as parent, subsidiary or affiliate companies) and (if applicable) other parties further along the supply chain.[97]

[97] FSB (2023b).

References

Accenture (2022): *Banking cloud altimeter*.

American Bankers Association (ABA) (2021): *Cloud computing in the US banking industry*, June.

Association of Banks in Singapore (ABS) and Monetary Authority of Singapore (MAS) (2016): *Finance-as-a-service: API playbook*, November.

Auer, R, B Haslhofer, S Kitzler, P Saggese and V Friedhelm (2023): "The technology of decentralized finance (DeFi)", *BIS Working Papers*, no 1066, January.

Bangko Sentral ng Pilipinas (BSP) (2021): "Open finance framework", *Circular*, no 1122.

Bank of England (2023): *Innovations in the use by deposit-takers of deposits, e-money and regulated stablecoins*, November.

Bank of England and Financial Conduct Authority (2022): *Artificial intelligence public-private forum: final report*, February.

——— (2023): "Operational resilience: critical third parties to the UK financial sector", Consultation paper, no 26, December.

Bank of Thailand (2021): *Blockchain technology adoption in financial services*.

Banking Regulation and Supervision Agency (BRSA) (2021): *Regulation on the operating principles of digital banks and banking as a service model*, December.

Bazarbash, M (2019): "Fintech in financial inclusion: machine learning applications in assessing credit risk", *IMF Working Papers*, no 109, May.

Basel Committee on Banking Supervision (BCBS) (2005): *Outsourcing in financial services*, February.

——— (2013): *Principles for effective risk data aggregation and risk reporting*, January.

——— (2018a): *Sound practices: implications of fintech developments for banks and bank supervisors*, February.

——— (2018b): *Cyber-resilience: range of practices*, December.

——— (2019): *Report on open banking and application programming interfaces*, November.

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

——— (2021b): *Principles for operational resilience*, March.

——— (2022a): *Newsletter on artificial intelligence and machine learning*, March.

——— (2022b): *Newsletter on third- and fourth-party risk management and concentration risk*, March.

——— (2022c): *Prudential treatment of cryptoassets*, December.

——— (2022d): "Governors and Heads of Supervision reaffirm expectation to implement Basel III in full and as fast as possible; provide direction on future work on climate-related financial risks and cryptoassets", press release, September.

——— (2023): "Digital fraud and banking: supervisory and financial stability implications", *Discussion Paper*, November.

——— (2024): *Core principles for effective banking supervision*, April.

Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO) (2022): *Guidance on the Applications of the Principles for Financial Market Infrastructures to stablecoin arrangements*, July.

——— (2023): "Blueprint for the future monetary system: improving the old, enabling the new", *Annual Economic Report 2023*, June, Chapter III.

Ben Naceur, S, B Candelon, S Elekdag and D Emrullahu (2023): "Is fintech eating the bank's lunch?", *IMF Working Papers*, no 239, November.

Boston Consulting Group (BCG) and QED Investors (2023): *Global fintech 2023: reimagining the future of finance*, May.

Boukherouaa, E and G Shabsigh (2021): "Powering the digital economy: opportunities and risks of artificial intelligence in finance", *IMF Departmental Papers*, no 24, October.

Cambridge Centre for Alternative Finance (2023): *Fintech Ecosystem Atlas*.

Cevik, S (2023): "The dark side of the moon? Fintech and financial stability", *IMF Working Papers*, no 253, December.

Chen, M, Q Wu and B Yang (2019): "How valuable is fintech innovation?", *The Review of Financial Studies*, vol 32, no 5, May.

Cloud Security Alliance (CSA) (2023): *State of financial services in cloud*, June.

Doerr, S, J Frost, L Gambacorta and V Shreeti (2023): "Big techs in finance", *BIS Working Papers*, no 1129, October.

European Central Bank (ECB) (2023): *Take-aways from the horizontal assessment of the survey on digital transformation and the use of fintech*, February.

Financial Stability Board (FSB) (2017): *Financial stability implications from fintech*, June.

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

——— (2022a): *Assessment of risks to financial stability from cryptoassets*, February.

——— (2022b): *Fintech and market structure in the Covid-19 pandemic: implications for financial stability*, March.

——— (2023a): *The financial stability risks of decentralised finance*, February.

——— (2023b): *High-level recommendations for the regulation, supervision and oversight of crypto-asset activities and markets*, July.

——— (2023c): *High-level recommendations for the regulation, supervision and oversight of global stablecoin arrangements*, July.

——— (2023d): *Enhancing third-party risk management and oversight: a toolkit for financial institutions and financial authorities*, December.

Financial Stability Institute (FSI) (2018): "Regulating and supervising the clouds: emerging prudential approaches for insurance companies", *FSI Insights on policy implementation*, no 13, December.

——— (2023): "Crypto, tokens and DeFi: navigating the regulatory landscape", *FSI Insights on policy implementation*, no 49, May.

Financial Stability Oversight Council (FSOC) (2023): *Annual Report 2023*, December.

Hong Kong Monetary Authority (HKMA) (2018): *Guideline on authorisation of virtual banks*, May.

——— (2019a): *Supervisory policy manual: risk management of e-banking*, October.

——— (2019b): *High-level principles on artificial intelligence*, November.

International Organization of Securities Commissions (IOSCO) (2022): "IOSCO decentralized finance report", March.

Koont, N, T Santos and L Zingales (2023): "Destabilizing digital 'bank walks'", *George J Stigler Center for the Study of the Economy & the State Working Papers*, no 328, October.

Monetary Authority of Singapore (MAS) (2018): *Principles to promote fairness, ethics, accountability and transparency (FEAT) in the use of artificial intelligence and data analytics in Singapore's financial sector*, November.

——— (2023a): *Interlinking networks technical whitepaper*, November.

——— (2023b): *Emerging risks and opportunities of generative AI for banks: a Singapore perspective*, November.

MAS and BIS (2023): *Project Guardian: enabling open and interoperable networks*, June.

National Institute of Standards and Technology (NIST) (2011): *The NIST definition of cloud computing*, September.

Organisation for Economic Co-operation and Development (OECD) (2022): *Why decentralised finance (DeFi) matters and the policy implications*, January.

Office of the Superintendent of Financial Institutions (OSFI) (2023): *Financial industry forum on artificial intelligence: a Canadian perspective on responsible AI*, April.

Perez-Cruz, F and H S Shin (2024): "Testing the cognitive limits of large language models", *BIS Bulletin*, no 83, January.

Petralia, K, T Philippon, T Rice and N Veron (2019): "Banking disrupted? Financial intermediation in an era of transformational technology", *Geneva Reports on the World Economy*, no 22.

Reuters (2023): *Microsoft cloud outage hits users around the world*, January.

RSM Stone Forest (2023): *Lessons learnt from Microsoft's Azure outage*, March.

Saudi Central Bank (2023): "SAMA launches first edition of cyber anti-fraud program", media release, September.

SG Forge (2023): *EUR CoinVertible Stablecoin White Paper*, April.

Swiss Financial Market Supervisory Authority (FINMA) (2019a): *Payments on the blockchain*, August.

——— (2019b): *Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin offerings*, September.

——— (2023a): *Guidelines for fintech licence applications*, May.

——— (2023b): "Staking", *FINMA Guidance*, no 8, December.

US Department of the Treasury (2023): *The financial services sector's adoption of cloud services*, February.

World Bank (2022): *Technical note on open banking: comparative study on regulatory approaches*.

World Economic Forum (2024): *The future of global fintech: towards resilient and inclusive growth*, January.