Just in Time

Digitalisation of Finance:

Regulation, Risks and Opportunities

Jul 2024

Executive Summary

Digitalisation is radically transforming the banking sector and has enabled **technological trends** to be used to take advantage of them, seeking to understand the **implications for banks and banking supervision** and to issue **standards** or **guidelines** to **mitigate emerging risks**.

The "Digitalisation of Finance" document published by the **Bank for International Settlements (BIS) partly builds on the paper from 2018, "Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors"**, published by the **Basel Committee on Banking Supervision (BCBS);** it was crucial in **outlining sound practices** and the **implications of fintech developments** for **banks** and **bank supervisors.**

In this context, the European Central Bank published the **Occasional Paper Series, "Digital innovation and banking regulation"** with the aim to **highlights** the **importance of balancing innovation with regulatory oversight to ensure stability and security in the financial sector.**

At a Glance

Keywords: Digital Innovation, Artificial Intelligence, Risk, Supervision

01

Introduction

Committee's 2018 Paper

Introduction

Committee's 2018 Paper

The document **"Digitalisation of Finance" published in May 2024** revisits several topics discussed in a previous paper from **2018**.

Advances in digitalisation and financial technology ("fintech") continue to **affect the landscape of the financial system**, including the provision of banking services. 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 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 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**. 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 are **more than twice** the amount invested before 2018

The technologically enabled **competitors** on banking playing growing roles in the provision of financial services, with **increasing chains of interconnections**

key technologies embedded in the banking value chain have all raised important questions about their **potential impact on banks, banking and supervision**

02

Key Areas

Innovative Technologies and their Applications

New Competitors and Business Models

Risk of Digitalisation

Banks' Risk Management

Regulatory and Supervisory Initiatives

Implications for Banks and Supervisors

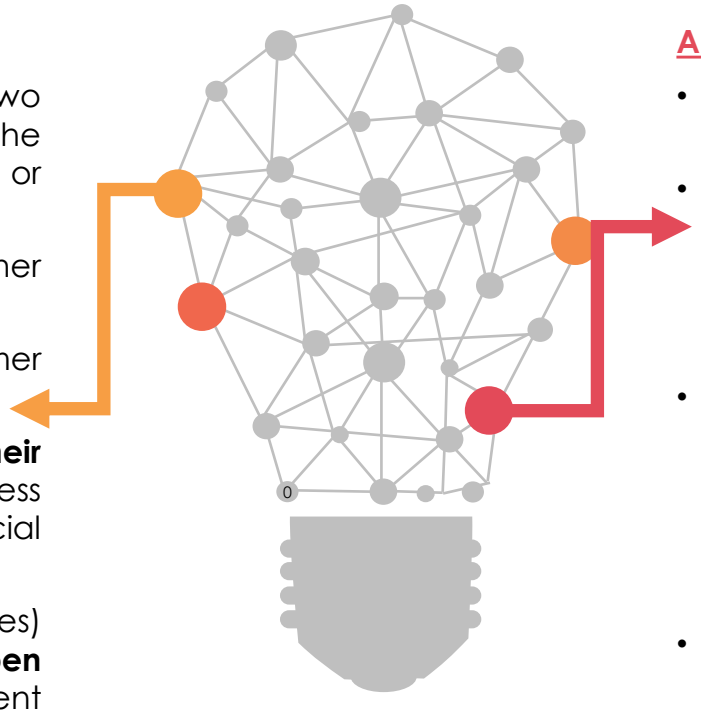
Key Areas 1/13

Innovative Technologies and their Applications 1/2

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.**

APPLICATION PROGRAMMING INTERFACES

- **Facilitate the sharing of data** between two distinct applications and allow for the execution of certain financial activities or services.
- It is considered **more secure** than other data-sharing techniques.
- Allow a **greater control** over how customer data can be accessed and by whom.
- Aim to the banks be able to **increase their knowledge of customers** by having access to a broader range of personal financial data.
- APIs (Application programming interfaces) are commonly used in **open banking/open finance frameworks** (eg investment decisions and/or bank loans using transaction-based underwriting).



ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

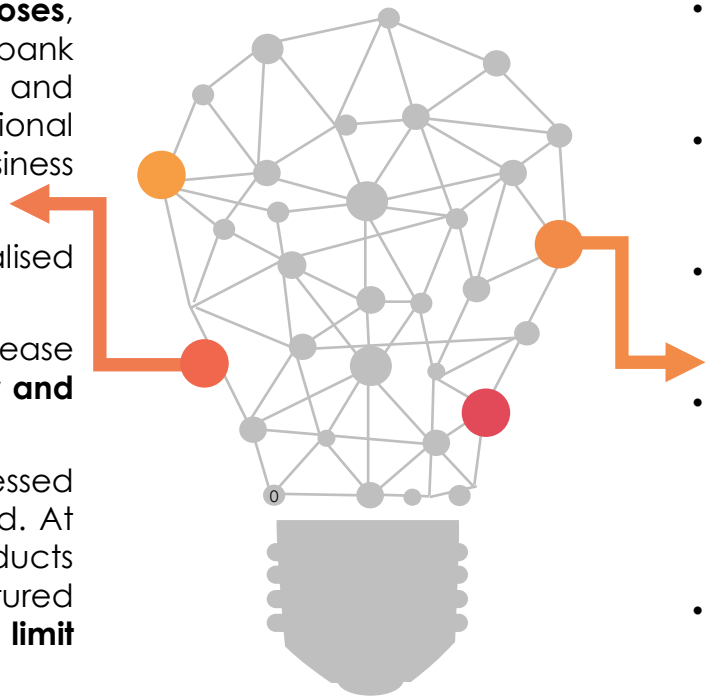
- Their **applications in a variety of settings**, for both back office and front office functions.
- They possess the ability to **predict a wide variety of complex phenomena** and have the potential to increase banks' operational efficiency, risk management capabilities and product offering (eg robo-advisory services).
- 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 has received **significant public attention,** and some banks are exploring or piloting generative AI applications internally to improve operational efficiency and staff productivity.

Key Areas 2/13

Innovative Technologies and their Applications 2/2

DISTRIBUTED LEDGER TECHNOLOGY

- 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)
- Its **use in the cryptoasset** and decentralised finance (**DeFi**) ecosystems
- Has the potential to lower costs and increase efficiencies by **allowing for cheaper, faster and more customised services**
- There are several **risks** 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**
- 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



CLOUD COMPUTING

- Allows the **sharing of on-demand computer processing** resources in a way that promotes efficiencies and economies of scale
- 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
- **Lower the barriers** to entry for firms expanding into new products and services, and over time reduce costs in financial services
- Cloud services allow banks to avoid building costly on-premise data centers that cover peak-level computing burdens and, instead, allow them the **flexibility to accommodate seasonal fluctuations in the need for computing**
- 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**

Key Areas 3/13

New Competitors and Business Models 1/2

Innovative technologies have facilitated the **entry of new digital-only participants, fintechs** and **larger technology companies** into the provision of banking and financial services. These firms often have an **advantage in data and technology** relative to traditional banks and **may not be subject to prudential regulation** or supervision. **For consumers**, new entrants may **expand access to financial services**, **reduce transaction costs**, provide **greater transparency** with simpler products, provide greater convenience and efficiency, and enable **tighter controls** over spending and budgeting.

Business model: Neobanks aspire to compete with traditional banks **by better customizing online products** and **delivering services faster**. They typically **target individuals**, entrepreneurs, and **small and medium-sized businesses**, offering services including **deposit** and **business accounts**, **credit cards**, **financial advice** and **loans**.
Features: While **unencumbered by legacy systems**, neobanks may face challenges such as **less stable deposit funding**. They can **leverage new technology at a lower cost**, more rapidly, and in more modern formats. Several incumbent banks have also launched neobanks as subsidiaries to offer digital-only services, but **to date neobanks' share of banking assets remains small** in most jurisdictions.

Business model: Fintechs often specialize in **offering** a particular **product or service that targets a specific segment of the banking value chain**. The greatest number of fintech companies offer **lending and payments services**, followed by enterprise tech provisioning, capital raising, and wealth tech.
Features: **They mostly rely on digital channels** such as social media and websites, **or partnerships** with local financial institutions, to acquire customers. While fintechs remain small relative to traditional financial institutions, **they are continuing to expand**, particularly in **higher risk segments** of the financial system.

Business model: 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. Examples include **e-commerce platforms**, **social networks** and **search engines**. They have expanded rapidly and **are significant providers of financial services in several countries**, particularly in the **provision of payments**.
Features: They have the **potential to become dominant competitors in financial services**, given the advantages conferred by their **collection of data** and **large established networks**.

Key Areas 4/13

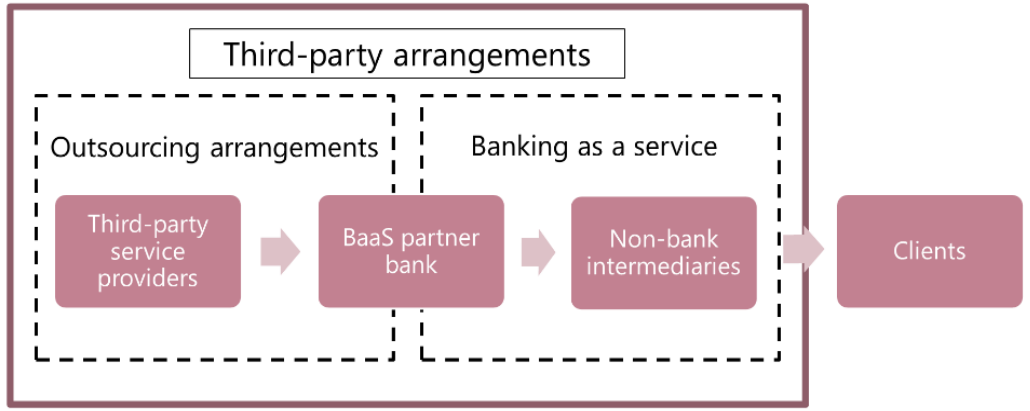
New Competitors and Business Models 2/2

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**. 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.

Banking as a Service (BaaS)

- ***Banks:*** **providing banking services to non-bank intermediaries** such as **holding deposits**, **processing payments** and **extending credit**.
- ***Platform providers:*** including **non-bank technology companies that provide the infrastructure** needed to connect banks with non-bank intermediaries.
- ***Non-bank intermediaries:*** may include **fintechs**, **big techs** or other **non-financial firms** (eg retailers or online marketplaces). **They bring advantages in product development, data analytics** and **user experience..**

Banking as a service (stylised example)



Source: Digitalisation of finance – Bank of International Settlements

While **BaaS does not currently represent a significant portion of banking services delivery, there is variation across jurisdictions.** Many banks that focus on BaaS are relatively small, though there are notable examples of larger banks involved. **Factors such as the inability to afford technology upgrades and competitive pressures lead smaller banks to adopt BaaS**. BaaS arrangements allow them to **expand** and **diversify their customer base** beyond specific regions or markets and **outsource functions** like customer onboarding, verification, and credit scoring to third parties more efficiently.

Key Areas 5/13

Risk of Digitalisation1/2

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.

Strategic risk drivers

- **Competition from non-bank competitors: In response to new digital entrants**, banks may seek to **develop internal technological capabilities, partner with new entrants or diversify revenues**. These strategies come with potential risks including **dependency on external entities** and **technological inadequacies**.
- **Large-scale digital transformation projects:** Large-scale digital transformation projects can be impeded by **legacy infrastructure** and **lack of expertise**, particularly in smaller banks, leading to **competitive disadvantages** and **financial vulnerabilities**.
- **Bank partnership with non-banks firms:** Banks partnerships expose banks to **loss of control over volumes**, **product design, origination process** and **customer base switching**.

Reputational risk drivers

- **Operational failures and non-compliance with relevant laws and regulations:** As result of **bank' use of technologies and partnerships with non-banks**. 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**.
- **BaaS arrangements:** Issues with non-bank partners could **affect the bank's reputation among consumers** and **investors**, potentially limiting the ability to **obtain liquidity or professional services** from external parties.
- **"Step-in" risks: Bank's may feel obliged to Intervene** to maintain continuity of service and/or to protect the values of end-users' assets **in cases of financial distress with non-bank partners**.

Data issues risk drivers

- **New data-intensive technology:** Poses significant **data governance challenges** for banks, particularly in managing the **increased volume**, **velocity, variety, quality,** and **integrity of data**.
- **Alternative data sources:** For example, payments information and social media, **introduce specific risks around privacy, consent, and potential biases**, especially when used in **AI/ML applications**.
- **Greater interconnectivity:** Increase the risk of **potential data breaches**.
- **Partnerships with non-banks:** It can **complicate data ownership** and access, **making regulatory compliance**, such as AML/CFT monitoring, **more complex.**

Key Areas 6/13

Risk of Digitalisation 2/2

Financial stability risk drivers

- **Increased interconnections:** **Innovative technologies in finance increase interconnectivity** among banks, fintechs, and tech firms, **complicating risk assessment** for supervisors and remaining **untested in economic downturns**.
- **Regulatory arbitrage:** Where non-banks are **not subject to equivalent regulatory expectations,** they could introduce additional vulnerabilities into the banking system.
- **Contagion:** Technological advances that **increase the speed of financial transactions** and real-time transmission of information through digital channels, could **increase the speed with which contagion may spread across institutions or markets.**
- **Amplification of financial risks:** Digitalization amplifies traditional financial risks, notably **liquidity risks** with **faster digital withdrawals** and **tokenized assets increasing liquidity demands**. Fintech dependencies can stress banks' financial stability while **AI-driven trading** and smart contracts can magnify **procyclical behaviors**.
- **Fragmentation risks:** The proliferation of **new infrastructure** (eg DLT) increases **risks of interoperability** and potentially **market and liquidity fragmentation**.
- **Concentration risks:** Concentration risks in market infrastructure, models or third parties can lead **to systemic impacts**, while **outages at a systemically important service provider** could result in significant **disruptions across the banking** and **financial systems**.

Operational risk drivers

- **Model risk:** The use of **AI/ML** gives rise to potential model risks such as **lack of explainability**, **overfitting** and **unethical outcomes**.
- **Technology risk:** banks' **legacy IT systems or implementation practices** may be **inadequate** to adapt to new technologies.
- **Cyber risk:** Increased use of APIs, cloud computing, and other **technologies that increase connectivity with less regulated entities** may **expose the banking system** to greater **cyber threats**.
- **Legal uncertainty:** **Emerging technologies challenge existing legal frameworks**, raising uncertainties around the **legality of products** like digital tokens and **the attribution of accountability and liability** for decisions made by AI or smart contracts.
- **Compliance risk:** Banks that **rely on non-bank partners** to undertake **KYC and AML checks** or engage with **cryptoassets** may be exposed to **heightened compliance and legal risks** if the processes of the non-bank partners are not appropriately vetted.
- **Fraud-related risk:** Digitalisation facilitates **new types of fraud** such as the use of **deepfakes** to commit account takeovers, loan fraud or wire fraud.
- **Third-party risk:** While **outsourcing** can reduce costs and improve operational flexibility, it can also **amplify issues relating to information and cyber security, privacy and operational resilience**. Banks may find it challenging to exercise effective oversight and monitoring over these third parties.

Key Areas 7/13

Banks' Risk Management 1/2

Banks have adopted various **strategies** and **practices to mitigate the risks arising from the digitalisation of finance**. However, their efficacy **has not yet been tested** through different phases of the business cycle or periods of stress.

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**. These structures and processes may include:

- **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 their **revenue**.
- **Staff development** to 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) and **Principles for operational resilience** (POR).
- Processes for **monitoring new business lines compliance** with **regulatory requirements**.
- **Robust strategic IT processes** to 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.

Model risk management

Banks are refining model risk management frameworks **to mitigate AI/ML risks**, considering **model impact**, **complexity** and **usage**. Greater **human oversight** is common **for material AI approaches**. Banks also emphasize the importance of **understanding model outputs**, including biases and robustness, to support effective decision-making and risk management. They **are developing tools to explain model functions** and account for their limitations. Moreover, some banks are **updating governance structures to oversee AI risks** and apply **extra measures for third-party AI models**, including **security scans** and **contractual restrictions** on data use. Additional **potential risk mitigants of generative** AI include **limitations on its usage**, **data sources tracing**, **model grounding** and **enhanced security of the technology used**.

Key Areas 8/13

Banks' Risk Management 2/2

Data governance

Banks are adopting various methods to **manage data-related risks** associated with **innovative technologies**. **Master service agreements** are used to set out **data maintenance**, **access**, **rights**, **ownership**, **intellectual property**, and **security protocols** when **sharing data with third parties**. Additionally, some banks conduct due **diligence on third-party data controls** and assign **risk ratings** to data based on the specific use case, influencing the decision on **whether to share** specific data with third parties. 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. For **managing challenges** associated with new data sources, **banks generally apply their** broader **data governance** and **risk management frameworks with additional controls for higher risk cases**. Some banks are also **increasingly considering ethics** in their data decision-making, ie not just "could" but "should" they use the data.

Third parties

Banks manage **third-party risks** through **due diligence**, **operational risk management**, **ongoing monitoring**, and **contracts that set out responsibilities**, service levels, and **audit rights**. **Outsourcing frameworks** should define the **governance** and **risk management** practices surrounding activities or functions that are outsourced. **Contractual frameworks** are expected to define the **rights, obligations, roles** and **responsibilities** of the bank and the third-party providing the outsourced service. To **mitigate the risks** posed by **cloud technology** banks typically **require cloud service providers (CSPs)** to establish stringent **security measures**, encompassing key security domains including **data encryption access controls** and log monitoring, through contractual means, and **assurance** via **third-party security assessments or certifications**. Concentration risks can be reduced by **developing multi-cloud strategy and exit strategies** to facilitate a smooth transition **in case of terminations**.

Key Areas 9/13

Regulatory and Supervisory Initiatives 1/2

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**.

Regulatory Frameworks

Standard-setting bodies and **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".**

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**, apply a proportionate and risk-based approach, request additional information related to unique issues associated with a digital-only business model, implemented distinct processes or criteria for licensing digital-only banks. These frameworks may permit licensees to **be exempt from certain prudential requirements and**, in some cases, **has been imposed 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.**

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.

Key Areas 10/13

Regulatory and Supervisory Initiatives 2/2

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 **(i) the technical complexity** of many new technologies and a lack of specialist knowledge by supervisors, which is compounded by the speed of innovation; **(ii) limited oversight** of certain activities and entities, and gaps in existing regulatory frameworks for addressing the full spectrum of risks, **(iii) uncertainty regarding the legal status** of certain products and **(iv) lack of standardisation and interoperability** of certain technologies and networks (eg APIs and DLT) which can lead to fragmentation.

Supervisory approaches and tools

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

- **Strategy and frameworks:** focused on **understanding** and **assessing** digitalisation-related risks.
- **Organisation:** changing in their internal organisation of supervision functions to include **specialist risk teams or specialist supervision teams** that focus on new/specialist banks or novel activities or arrangements **between banks and fintechs**.
- **Training and capacity building: implementing 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.
- **Prior notification or approval:** requiring notification by banks prior to their adoption of certain technologies, or entry into partnerships or other arrangements with third parties.
- **Prudential reviews:** conducting thematic reviews on digitalisation-related topics such as cyber security and IT risk.
- **Business model analysis:** increasing 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.

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 solutions to **improve communication** and **clarity** on regulatory requirements and expectations.

Supervisors are **increasingly engaging with other public and private sector participants on digitalisation-related topics and areas of interest; noting a blurring of the boundaries between prudential regulation.**

Many supervisors have also recognised the importance of close cooperation and collaboration with **(i) industry, technology experts and academic institutions on digitalisation and regularly engage in dialogue with (ii) non-bank firms and (iii) banking sector**, to discuss the latest risks, trends and developments and to promote encourage digital innovation, including showcase events, roundtables, seminars and practical training sessions.

Key Areas 11/13

Implications for Banks and Supervisors 1/3

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.

Macro-Structural considerations

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

- The digitalisation of finance presents **both opportunities** and **risks for banks and supervisors.** 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.
- Digitalisation may also potentially alter risks to banks, making it important to consider the **interactions of those risks in tandem with traditional financial risks**.

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.**
- 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.**

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.
- 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.

Key Areas 12/13

Implications for Banks and Supervisors 2/3

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.** 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 questi**ons 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.

The use of service providers

- Banks are **engaging** with service providers 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**. 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.**

The role of human judgment in bank risk management and supervision

- 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 management and board.
- 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.**

Key Areas 13/13

Implications for Banks and Supervisors 3/3

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.
- **Broader dialogue with technology experts, academia and other public sector authorities** may also be mutually beneficial.

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**.

03

EU Banking Regulation and Digital Trends

EU Banking Regulation and Digital Trends 1/2

The **European Central Bank (ECB)** is aiming to foster **digital transformation** in all sectors by **2030**. It has pioneered cross-sectoral legislation on artificial intelligence, cloud computing services and crypto-assets for this purpose. Yet compared with the work done on ESG, the prospective banking regulation regime has still to articulate more purposefully how the industry should manage the risks from digital trends and how supervisors should assess them.

Transparency of exposures within the perimeter of prudential consolidation

New impetus is provided by the updated Basel Core Principles for effective banking supervision (BCBS, 2024) which formulate the expectation that supervisors will monitor risks to banks from financial technology activities. Supervisory powers and reporting should cover NBFIs (Non-Bank Financial Institutions) within a banking group and any limitations will need to be remedied.

CRR III has new definitions of financial holding company and ancillary services undertaking useful to capture fintech, AI, cloud computing service providers and BigTech parent companies or affiliates is one way of ensuring supervision. It is not a panacea, though, because non-financial affiliates require technically savvy supervisory expertise.0

Linking the requirements laid down in the regulatory framework for digital trends with those provided in banking regulation

What is still missing is a detailed articulation of how **banks will abide by the requirements in the AI Act, MiCa (Markets in Crypto-Assets Regulation) and DORA (Digital Operational Resilience Act) that links the obligations flowing from these acts with the obligations under CRR III/CRD VI**. Ultimately, this involves providing guidance on how risks from digital trends should be captured and when quantitative or qualitative measures have to be applied.

Cooperation and information sharing between authorities to avoid duplication

The regulatory framework for digital trends attributes oversight and supervisory competences to national and EU supervisory authorities. **Close cooperation between prudential supervisory authorities and the competent authorities and lead overseers under MiCa, DORA and the AI Act will be essential to avoid regulatory arbitrage.** Timely information is crucial when responding to cyberattacks or licensing crypto-asset providers, because the technological challenges and opportunities are global.

To allow for such a flow of information and to **adapt to a fast-evolving world of supervisory architecture, the requisite framework for exchange of supervisory information may need to be adapted, in particular Articles 53-59 CRD**. Information Sharing and Analysis Centers (ISACs) are a practical example of informal international cooperation.

When the BCBS completes its work on Pillar 1 for crypto-assets, this will be implemented into EU law. The question that then arises is whether **further reflection is required for Pillar 2 prudential assessment and Pillar 3 disclosures.**

EU Banking Regulation and Digital Trends 2/2

On one hand, banks are required to **hold capital and liquidity for the risks** they face and demonstrate their capital or liquidity adequacy in ICAAP and ILAAP. **On the other hand**, they need to abide by the **specific obligations** in the newly enacted regulatory framework **for digital trends.**

Pillar II

Digitalisation plans are suggested as a means of providing a comprehensive overview of all the risks from digital trends used by a bank

The supervisors recommend that high-level strategies should be coupled **with mandatory digital innovation plans offering a comprehensive overview of all the risks from digital trends** to which a bank is exposed, and **detailing how** it **assesses**, **manages**, **monitors** and **mitigates** these.

To ensure the necessary degree of proportionality, this obligation could be stipulated for large, listed banks. New technologies implemented by banks and supervisors, such as DLT, **open new gateways for delivering data to supervisors**.

The bank does not need to collect data and transmit them to supervisors, and the cost of compliance is therefore reduced. Consequently, **digital innovation will likely change the way supervisors interact with the banks** they supervise, growing into a **new concept** for transcend digital operational resilience: **real-time supervision**.

Voluntary bank disclosures concerning use of digital trends and strategies are already promising in terms of breadth. Consistency of terms used and comparability across peers remain an issue, though, because some widely-used terms are not defined.

Pillar III

Pillar 3 disclosures regarding the use of digital trends may be considered

Pillar 3 disclosures **would help investors determine the level of digital innovation and literacy in a bank**, which can reveal a great deal about its **business model** and **future profitability**.

If the **European legislator** decided to go down this road, an **explicit legal basis would need to be incorporated in the CRR**, and the EBA would provide guidelines and templates for disclosure.

04

Final Remarks

Final Remarks

Just in Time

BIS

The Committee's 2018 paper describes the **«Sound Practices»** as concern:

1. **Technological Innovations and Applications:** it discusses the deployment of technologies like artificial intelligence (AI), machine learning (ML), cloud computing and distributed ledger technology (DLT) in banking**. Banks are integrating these technologies at various levels**, from back-office operations to customer-facing interactions, enhancing operational efficiencies and customer services.
2. **New Competitors and Business Models:** the entry of fintechs and big tech companies has introduced **new competitive dynamics in the banking sector.** These entities often operate under lighter regulatory frameworks, **leveraging their technological prowess to offer innovative financial products and services that challenge traditional banks.**
3. **Risks:** the BIS paper outlines **multiple risks associated with digitalisation**, including strategic risks from increased competition, reputational risks linked to technological failures or data breaches, and operational risks from reliance on complex systems and third-party providers.
4. **Regulatory and Supervisory Responses:** it details how regulatory bodies are adapting to the digital transformation. This includes **expanding** regulatory frameworks to incorporate **new digital banking models and establishing guidelines to manage risks associated with technology adoption in financial services.**

ECB

The ECB document describes the «**Digital Finance Strategy»** is fostering digital trends by means of an innovative comprehensive regulatory framework, including inter alia for AI systems, crypto-assets and cloud computing service providers.

- The interplay with the banking regulation regime **could be reflected more purposefully in the regulatory framework**.
- **Digital innovation plans** are suggested as a means of providing a **comprehensive overview of all the risks** to which a bank is exposed by **using various types of digital trends.**
- Consideration could also be given to **harmonising Pillar 3 disclosures concerning banks' use of digital trends**. Ultimately, digital trends have the potential to revolutionise the way prudential supervision is performed.

ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

iason is an international consulting firm that has been supporting both financial institutions and regulators in topics related to Risk Management, Finance and ICT since 2008

Strategy

Strategic advisory on the **design** of **advanced frameworks** and **solutions** to fulfil both **business** and **regulatory needs** in Risk Management and IT departments

Methodology & Governance

Implementation of the designed **solutions** in bank departments **Methodological support** to both **systemically important financial institutions** and **supervisory entities**

Solution

Advanced **software solutions** for **modelling, forecasting, calculating** metrics and **integrating** risks, all on cloud and distributed in Software-as-a-Service (**SaaS**)

KEEP IN TOUCH

iason

Company Profile

Iason is an international firm that consults Financial Institutions on Risk Management. Iason integrates deep industry knowledge with specialised expertise in Market, Liquidity, Funding, Credit and Counterparty Risk, in Organisational Set-Up and in Strategic Planning.

Dario Esposito

Bianca Ghilardi

This document was prepared in collaboration with Stefano Rossi, who at the time was working for Iason Consulting.

www.iasonltd.com