WP/21/105

IMF Working Paper

Central Bank Risk Management, Fintech, and Cybersecurity

by Ashraf Khan and Majid Malaika

INTERNATIONAL MONETARY FUND

 WP/21/105

IMF Working Paper

Monetary and Capital Markets Department and Information Technology Department

Central Bank Risk Management, Fintech, and Cybersecurity

Prepared by Ashraf Khan and Majid Malaika

Authorized for distribution by Jihad Alwazir and Herve Tourpe

April 2021

Abstract

Based on technical assistance to central banks by the IMF's Monetary and Capital Markets Department and Information Technology Department, this paper examines fintech and the related area of cybersecurity from the perspective of central bank risk management. The paper draws on findings from the IMF Article IV Database, selected FSAP and country cases, and gives examples of central bank risks related to fintech and cybersecurity. The paper highlights that fintech- and cybersecurity-related risks for central banks should be addressed by operationalizing sound internal risk management by establishing and strengthening an integrated risk management approach throughout the organization, including a dedicated risk management unit, ongoing sensitizing and training of Board members and staff, clear reporting lines, assessing cyber resilience and security posture, and tying risk management into strategic planning.. Given the fast-evolving nature of such risks, central banks could make use of timely and regular inputs from external experts.

JEL Classification Numbers: G32, G34, G38, E50, E58, K23, O30.

Keywords: fintech, cybersecurity, central banking, financial supervision, law, technical assistance

Authors' Email Addresses: AKhan4@imf.org, MMalaika@imf.org

The authors are grateful for input from Ricky Satria, Yosamartha, Ronggo Gundala, Irman Pardede (Bank Indonesia), Ralph Ansumana (Bank of Sierra Leone), Jean Goetzinger (Central Bank of Luzembourg), Roman Hartinger (National Bank of Ukraine), review comments from Ben Norman (Bank of England), Gabriel Andrade (Bank of Portugal), Paul Woods (Central Bank of Ireland), Jihad Alwazir, Herve Tourpe, Bachir Boukherouaa, Gani Gerguri, Sanjeev Matai, Elie Chamoun, Lott Chidawaya, Stephen Swaray, Rudy Wytenburg, Parma Bains, Rangachary Ravikumar, Inutu Lukonga, Tanai Khiaonarong, Ryan Rizaldy, Gabriel Soderberg, Marianne Bechara, Juan Sebastian Viancha, Kathleen Kao, Nadine Schwartz, Victoria Bakhtina (IMF), and data assistance from Marc Engher. Danica Owczar provided invaluable administrative assistance. All remaining errors are our own.

READING GUIDE for IMF Working Paper on Central Bank Risk Management, Fintech, and Cybersecurity			
If you are interested in:		**(Sub)section(s)**	**Pages**
1	**General discussion** of fintech and (central bank) risk management	I, II	6–9
2	Specific **recommendations for central banks**	V	51–55
3	Operational findings from **technical assistance** on central bank risk management, fintech, and cybersecurity	III.A	9–19
4	Findings from IMF **surveillance** (FSAP/AIV) on (central bank) risk management, fintech, and cybersecurity	III.B, III.C	19–25
5	Concrete **fintech/cybersecurity risk examples** for central bank policies, functions, and organization	IV	25–51
6	Selected **central bank case examples** of fintech developments and risk management	Appendix II	60–71

CONTENTS **PAGE**

GLOSSARY

AI	Artificial Intelligence
AIV	IMF Article IV surveillance
AML/CFT	Anti-Money Laundering/Combatting the Financing of Terrorism
API	Application Programming Interface
BCBS	Basel Committee on Banking Supervision
BCL	Banque Centrale du Luxembourg
BCM	Business Continuity Management
BFA	Bali Fintech Agenda
BI	Bank Indonesia
BIS	Bank for International Settlements
BSL	Bank of Sierra Leone
CBDC	Central Bank Digital Currencies
CBLD	Central Bank Legislation Database
CER	Committee on Emerging Risks (of IOSCO)
DeFi	Decentralized Finance
DLT	Distributed Ledger Technology
ECB	European Central Bank
ELA	Emergency Liquidity Assistance
ERM	Enterprise-wide Risk Management
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FMI	Financial Market Infrastructure
FSAP	Financial Sector Assessment Program
FSB	Financial Stability Board
FSI	Financial Stability Institute
GFC	Global Financial Crisis
GRC	Governance, Risk, and Compliance
GSC	Global Stablecoin
HR	Human Resources
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IT	Information Technology
ITD	Information Technology Department
LIC	Low-Income Countries
LOLR	Lender of Last Resort
MCM	Monetary and Capital Markets Department, IMF
ML	Machine-Learning
NBG	National Bank of Georgia
NBU	National Bank of Ukraine
OECD	Organisation for Economic Co-operation and Development
ORM	Operational Risk Management
PF	Proliferation Financing
PFMI	Principles for Financial Markets Infrastructures
RBI	Reserve Bank of India
RCSA	Risk Control Self-Assessment
RMD	Risk Management Department
RTGS	Real-Time Gross Settlement
SME	Small and Medium Enterprises
SOC	Security Operation Center
SRA	Strategic Risk Assessment
TA	Technical Assistance
UMP	Unconventional Monetary Policies

I. INTRODUCTION

Effective risk management of central banks is imperative for managing a wide variety of increasing financial and nonfinancial risks. Central banks[1] across the globe have undergone an expansion of the risks that they run. This includes financial risks resulting from policy decisions, especially those in unconventional times, including during the COVID-19 pandemic—varying from asset purchase operations that have significantly expanded the balance sheets of central banks in, for instance, the United States, the United Kingdom, the European Union, and Japan, to central banks actively pursuing more aggressive, yield-increasing asset management strategies due to the low interest environment.

However, in addition to financial risks, central banks also run *nonfinancial* risks. These include strategy and policy risks, operational risks, and reputational risk in general. These risks can hold significant financial consequences for central banks. This has spurred an increasing number of central banks to try and quantify operational risks in particular.

However, nonfinancial risk management of central banks has traditionally not received as much attention as financial risks and their management. In an earlier IMF Working Paper,[2] we ascribed this to the fact that central banks' mandates, objectives, and functions were more limited before the Global Financial Crisis (GFC), but that with the advent of the GFC those mandates got expanded further into areas beyond price stability.

Several developments over the past years have *even further* increased that awareness of nonfinancial risks for the central bank. The focus on topics such as climate change, economic development/employment, financial inclusion, and fintech, have led to central banks becoming public super-institutions—seemingly capable of solving most of a country's economic and financial problems. Clearly, this has also led to central banks moving into areas that might be in the realm of the fiscal authorities—with significant consequences for central bank nonfinancial risks related to those newer areas as well.

This paper focuses on central bank nonfinancial risks specifically related to the surge of technological innovations dubbed "fintech," including the related area of cybersecurity, and how fintech and cybersecurity strengthen the need for enhanced central bank risk management. Central banks need to carefully consider this interplay between the possible upsides of fintech, and the guaranteed downsides of cyber risks, when trying to achieve their (often multiple) objectives.

The paper draws on:

---

[1] This paper predominantly looks at risk management of central banks. However, this includes functions such as microprudential supervision if the supervisor is incorporated into the organization of the central bank.

[2] See Khan, A., 2016, *Central Bank Governance and the Role of Nonfinancial Risk Management*, IMF Working Paper 16/34. Washington, D.C.: International Monetary Fund.

1) Findings from nine (9) central bank technical assistance (TA) cases[3] from the IMF's Monetary and Capital Markets Department (MCM, Central Bank Operations Division) and Information Technology Department (ITD, Digital Advisory Unit); and four (4) country cases (Indonesia, Luxembourg, Sierra Leone, and Ukraine);

2) Informal interactions on fintech with heads of risk management departments of several central bank members of the International Operational Risk Working Group (IORWG);

3) Participation in the EU's Fintech Risk Management Project;[4] and

4) Findings from the IMF's Article IV (AIV) database and from selected Financial Sector Assessment Programs (FSAP).

Section II will provide a definition and overview of "fintech" and related developments relevant for central bank risk management. Next, Section III will examine to what extent IMF technical assistance by MCM Central Bank Operations and ITD/Digital Advisory, as well as IMF surveillance has covered possible links between central bank risk management, fintech, and cybersecurity. Building on this, Section IV analyzes in more detail how specific fintech developments affect central bank risk management (focusing on strategy and policy risk, as well as operational risk). Finally, Section V draws conclusions and recommendations for central banks to consider.

Appendix I lists relevant risk management details of the Bali Fintech Agenda (BFA); Appendix II provides several country case examples.

II. FINTECH—DEFINITION, PRINCIPLES, AND RISK MANAGEMENT

Fintech, in the definition of the Bali Fintech Agenda (BFA), relates to "the advances in technology that have the potential to transform the provision of financial services spurring the development of new business models, applications, processes, and products."[5] Similarly,

[3] Due to the confidential nature of those TA cases, the names of the central banks involved are not mentioned. Instead, the paper has used anonymized findings from the TA reports, discussions with, and feedback from the respective central banks as the foundation for this paper. The TA cases took place between 2018 and 2020. The TA missions were all led by IMF HQ staff from MCM and ITD, and comprised external experts on risk management, strategic planning, governance and organization, from various central banks.

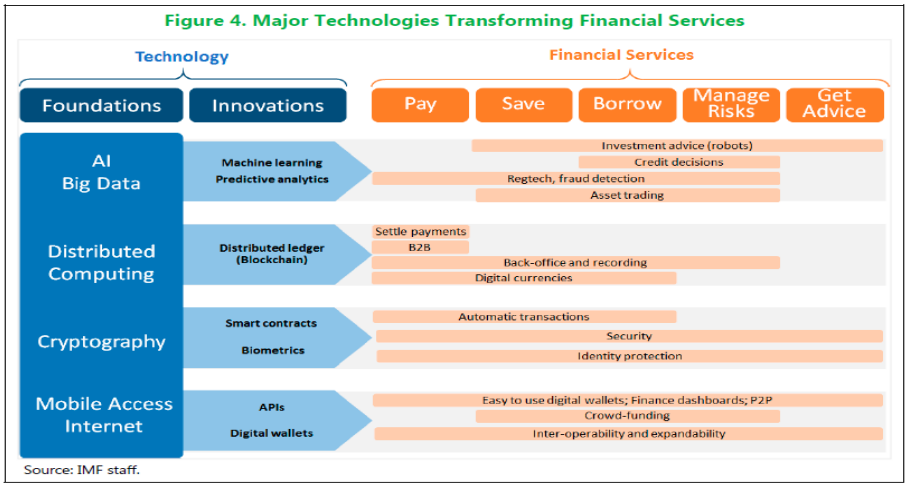
[4] See https://www.fintech-ho2020.eu/. Staff from MCM participated in several meetings of the EU Fintech Risk Management Project, and engaged with participants (academic institutions, central banks, financial supervisors, and fintech firms).

[5] BFA, p. 12.

the Financial Stability Board (FSB)[6] defines fintech as "technologically enabled innovation in financial services 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." Both definitions cover the extensive use of data by (and technological advances to) financial services, and leverage the explosion of Big data on individuals and firms, advances in AI/ML, computing power, lowering capital cost, cryptography, distributed computing and the reach of the Internet. The strong complementarities among these technologies give rise to an array of new applications touching on services from payments to financing, asset management, insurance, and advice. This creates the possibility of entities driven by fintech emerging as competitive alternatives to traditional financial intermediaries, markets, and infrastructures.[7]

Fintech-related technologies have broad effects on a range of financial services. Figure 1 below demonstrates how AI, Big data, Distributed Computing, cryptography, and mobile access internet influence financial services from payments, to saving and lending, risk management, and financial advice (the latter could include components of consumer protection and financial inclusion as well).

Figure 1. Major Technologies Transforming Financial Services



Source: IMF, 2017, Fintech and Financial Services: Initial Considerations. IMF Staff Discussion Note 17/05. Washington, D.C.: International Monetary Fund.

[6] https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/fintech/#:~:text=The%20FSB%20defines%20FinTech%20as,the%20provision%20of%20financial%20services.

[7] IMF, 2017, *Fintech and Financial Services: Initial Considerations*. IMF Staff Discussion Note 17/05. Washington, D.C.: International Monetary Fund.

Risk management has been identified as relevant to fintech developments. The IMF/WB Bali Fintech Agenda (BFA)[8] highlights the necessity for central banks and supervisors to examine risk management components of fintech. BFA Principle IX (Ensure the Stability of Domestic Monetary and Financial Systems, see Appendix I) stresses that fintech "offers central banks the opportunity to explore new services, while having to consider new risks." It focuses on policy aspects relating to Central Bank Digital Currencies (CBDC), payments systems, as well as financial stability aspects, including the lender of last resort-role of central banks.

The BFA includes a specific focus on risk management of fintech. Principle X (Develop Robust Financial and Data Infrastructure to Sustain Fintech Benefits, see Appendix I) stresses that "[e]ffective governance structures and risk-management processes are important to identify and manage risk associated with the use of fintech. The greater reliance on such technologies leads to new operational risks and more interdependencies among service providers… that may threaten the operational resilience of financial and data infrastructures." This includes risks related to outsourcing, as Principle X refers to third-party service providers, and the fact that many of these providers "fall outside the regulatory perimeter," which would require "increased emphasis on managing operational risks and ensuring robust outsourcing arrangements." These risks may reach such significant levels that require the development of a specific vendor risk management framework.

Principles IX and X are focused on fintech-related risks for financial institutions. However, the risk management aspects of the principles hold for central banks to a large extent as well, as the next sections will explore.

III. THE IMF'S INVOLVEMENT WITH "FINTECH" AND RISK MANAGEMENT

The IMF has been involved with "fintech" over the past decades. Though the concept of "fintech" was not necessarily used as such, much of the IMF work in surveillance, policy development, and technical assistance relates to technological developments in and of the financial sector, including of central banks and their risk management.[9]

IMF technical assistance (TA) covers all the areas that the IMF works on. As noted, this paper looks at TA provided by the IMF in the context of central bank operations (central bank risk management, governance, internal organization, and cash currency management) and digital advice (in particular, cybersecurity).

---

[8] IMF/WB, 2018, *The Bali Fintech Agenda*. IMF Policy Paper. Washington, D.C.: International Monetary Fund.

[9] The IMF, of course, also assists countries by providing financial support through loans. As part of these lending operations, the IMF's Finance Department conducts Safeguards Assessments. The Assessments examine, i.a., the internal control framework (including risk management) of the central bank. However, given the highly confidential nature of Safeguards Assessments, this paper does not look at possible fintech and cybersecurity findings based on Safeguards Assessments.

The paper also examines IMF surveillance findings. Surveillance involves the IMF monitoring risks to domestic and global stability. The Fund does so by means of consulting with its member states, which is often referred to as the Article IV (AIV) discussions. These discussions with country authorities focus on exchange rate issues, monetary, fiscal, and regulatory policies, as well as macro-critical structural reforms.

Lastly, the IMF also gauges stability and soundness of the financial sector and assesses the financial sector's potential contribution to growth and development. The IMF does so by means of its Financial Sector Assessment Program (FSAP), of which selected findings are also presented in the paper

In these three modalities—TA, AIVs, FSAPs—attention for fintech and cybersecurity, and to a certain extent (central bank) risk management, is visible and made concrete, as the following subsections will highlight.

A. Technical Assistance: Advice on Fintech in the Context of Risk Management

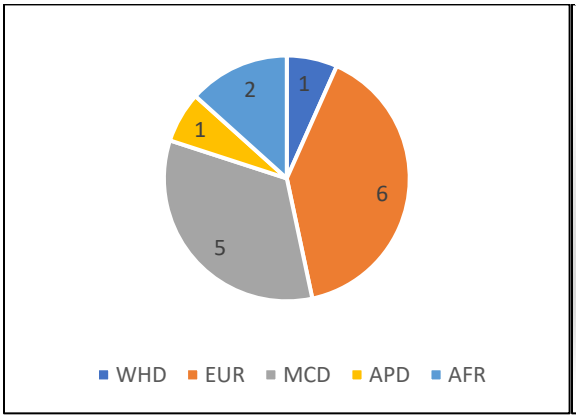
TA by MCM and ITD on fintech and central bank risk management has increased since the publication of the BFA. In the period 2018–2020, MCM (in several cases together with ITD) provided central bank risk management TA, as well as bilateral advice to and discussions with central banks in all regions of the world, with a distinct fintech focus.

As Figure 2 shows, most TA and informal interactions in the period 2018–2020 on fintech and central bank risk management took place with central banks in the European and Middle East and Central Asia regions, and on the topics of (1) central bank risk management in general (including Business Continuity Management, BCM), followed by (2) fintech organization (i.e., relating to the central bank's internal organization of fintech-related activities, for instance, by considering the setting up of a dedicated fintech unit), (3) central bank cybersecurity, and, in two cases, (4) developments of digital payments in the context of central bank risk management and cash currency management.[10]

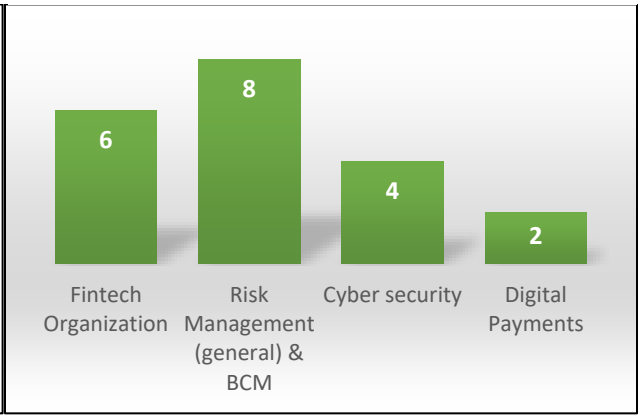
[10] Of course, this is not indicative of IMF TA on digital payments separate from central bank risk management.

Figure 2. Central Bank Risk Management, Fintech, and Cybersecurity

(a) Interactions (missions, advice, discussions) by region (2018-2020)



(b) Main topics of discussion (2018-2020)

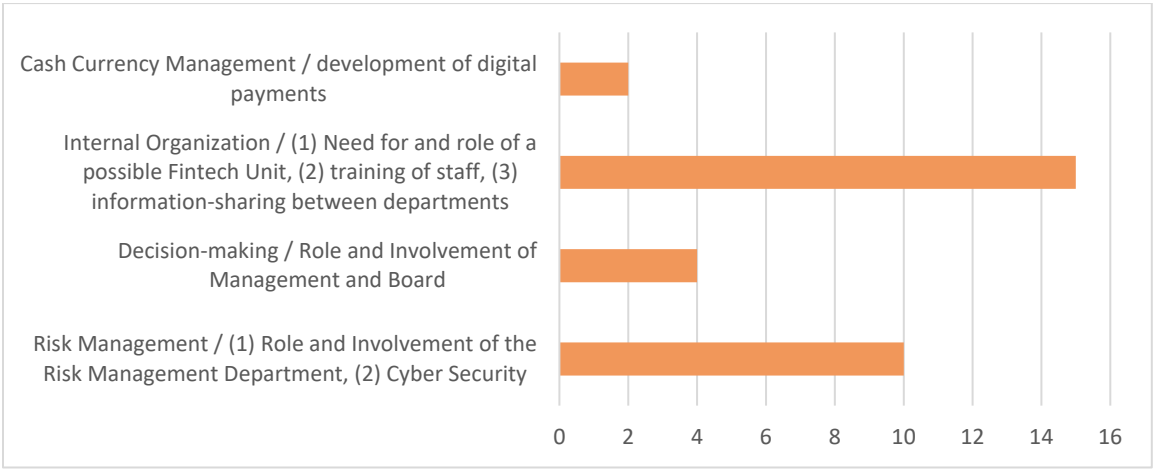


AFR: Africa
APD: Asia and Pacific
EUR: European
MCD: Middle East and Central Asia
WHD: Western Hemisphere

Source: authors.

The main categories of questions raised by the respective central banks related to the following fintech components (see Figure 3 below):

Figure 3. Main Fintech Issues Discussed in the Context of IMF Risk Management TA



Source: IMF staff.

1) **Risk Management: ensuring fintech risks that may affect the central bank are adequately covered by the central bank's risk management department**. In several cases, the central bank risk management departments were not fully aware of emerging fintech risks, for instance, related to cloud computing (see also Section IV (H))—even though risks related to the use of third-parties and outsourcing in general did exist (for instance, related to general procurement and use of service from third-parties). In another case, the risk management department arranged for a presentation by the central bank's fintech department to the IMF TA mission and the risk management department itself. The presentation covered key domestic fintech developments among financial institutions. Subsequently, the discussion between the fintech department and the risk management department allowed for the risk managers to be further informed of key fintech developments, and be able to translate them into developments that might affect the central bank itself. In general, closer cooperation between the central bank's (i) IT department, (ii) fintech department (where applicable), and (iii) financial supervision department (where applicable) proved to be beneficial, as often fintech-related knowledge was already available "in house," but not necessarily available to the risk management department. This also included identifying cyber risks emerging from fintech developments and ensuring sufficiently strong central bank cyber resilience are in place/are being developed.

   Several TA missions also focused on details of central bank security posture, and whether the involvement of third-party vendors would be sound from a central bank risk management perspective. Experiences from other central banks were shared, including on how to set up a central bank Security Operation Center (SOC),[11] conduct cybersecurity assessments (including red, blue, and purple teaming exercises) mainly to examine the SOC's effectiveness, and provide assurance to central bank decision-makers on cybersecurity arrangements.

2) **Decision-making: ensuring the central bank's decision-makers (i.e., senior management and Board) are adequately aware of fintech opportunities and risks** in their jurisdiction and are aware of how these developments could feed into the central bank's strategic planning process and its internal risk management. In most cases, the central bank's key decision-makers (i.e., members of the decision-making body/bodies, such as the governor, deputy governors, and nonexecutive Board members—where applicable) were not fully informed of, or up to date on relevant fintech and cybersecurity developments and how these could affect the central bank's risks (or provide opportunities), and no discussions had taken place in the context of the central bank's risk appetite. Often this turned out to be a more systemic central bank governance issue, as in

[11] SOC is a security operations center formed within an organization to handle security related events and incidents at the technical level. SOC rely on network traffic, node health and application behavior to monitor the network and systems for anomalies and are usually capable of responding and eliminating the threat.

three cases the decision-making body was not at full strength, with in particular nonexecutive Board members' position not yet being filled—even though especially nonexecutive Board members would have a key role to play in identifying strategic developments, including those relating to fintech, cybersecurity, and the role of and effect on the central bank. Additionally, some of these cases also highlighted internal silos, with a fintech department reporting to one specific decision-maker, and risk management reporting to another, without proper information-sharing arrangements.

3) **Internal Organization: facilitating internal central bank discussions on whether there is a need and necessity to have a fintech unit**, roles and responsibilities of such a unit, and place within the internal organization. In three cases, the central bank requested IMF advice on how to set up a fintech department, without it necessarily being clear what such an organizational unit would focus on. In most cases, the fintech department aimed at contributing to financial supervision by identifying fintech developments among financial institutions, examining licensing requirements—including in the context of a regulatory sandbox. In one other case, the fintech department was specifically set-up to contribute to financial inclusion, highlighting less of a focus on upholding prudential requirements, and more on deepening the financial market.

   Other internal organization issues the respective TA missions provided support on, related to ensuring central bank staff (in particular financial supervisors, IT staff, risk management staff) had a proper understanding of relevant fintech developments, and were able to update their knowledge and expertise on a regular basis – in the case of one central bank, it moved to having regular, open meetings with fintech companies at the central bank's premises, allowing them to showcase their products and services, facilitating interaction with central bank staff, and thereby enhancing the central bank's staff's understanding of relevant fintech developments. Cooperation with other involved agencies and donors, including the United Nations and the World Bank, proved to be helpful as well, with fintech experts from their sides providing training to central bank staff in specific fintech areas.

4) **Cash Currency Management: discussions on the interaction between cash currency management and related risks, and the development of digital payments**. In few cases, the risk management department and the currency department raised concerns about moving towards a more cashless society, and/or the increased practical use of digital payments. In one case this related to the use of SIM chips and money stored on those SIM chips, including questions on which agencies would be responsible for overseeing the respective telephone operators. In another case, the central bank presented its case on a (CBDC and how it had identified opportunities as well as risks for the central bank itself. In another example, the central bank was exploring the possibility of issuing a CBDC, and the IMF highlighted a number of operational issues and gaps within the central bank's cyber resilience program to improve internal processes, technologies and skillset needed to maintain a high-level of assurance of their standing infrastructure,

and to include the newly introduced CBDC ecosystem as well. One of the issues highlighted, which was raised by the central bank internal security team, was the lack of a SOC within the central bank to monitor their infrastructure and systems, capable of instantly responding to any threat or incident. Running a SOC capable of monitoring and responding 24/7/365 days to any security issue is fundamental to fintech services specially with more widely accessible systems such as CBDC in comparison to closed traditional payment systems with selective participants (usually commercial banks and credit unions). This is under the assumption that the central bank is maintaining the backend core-system.

Practical examples of IMF TA recommendations on central bank risk management and how fintech and cybersecurity (should) tie into risk management are provided below. Tables 1 and 2 below provide anonymized examples of recommendations from the IMF in two recent MCM TA missions.

Table 1. Example: IMF TA Recommendations on Central Bank Risk Management, Fintech, and Cybersecurity

#	Theme	Recommendation	Actor(s)	Time Frame
1	Risk Management Diagnostic	**Appoint remaining central bank Nonexecutive Board members** (and provide support for their nonexecutive responsibilities), in line with IMF Safeguards Recommendations.	[Governor to highlight the necessity]	As soon as possible
2		**Engage with central bank Nonexecutive Board members on strategic planning** (initially, only focusing on strategic risk assessment, see below).	[Governor to highlight the necessity]	After appointment of remaining Nonexecutive Board members
3	Strategic Risk Management	**Prepare for/conduct a Strategic Risk Assessment (SRA),** built on Operational Risk Management ORM) achievements, complete a multilayered perspective to avoid risk blindsides.	Risk Management Department (RMD)	12-18 months
4		**Develop Enterprise-wide Risk Management** (ERM) to strengthen, streamline and integrate oversight and performance.	RMD	18-24 months
5	Fintech	**Integrate Fintech Unit's (fintech risk) findings** within the central bank's risk management Framework.	RMD, Fintech Unit	1-6 months
6		**Enhance fintech governance/compliance research** with technologists within the RMD.	RMD	6-12 months
7		**Conduct a cybersecurity gap assessment**, addressing: a) Central bank cyber resilience; and b) Early security assurance research/activities for fintech adoption.	RMD	6-18 months

Source: IMF.

Table 2. Example: IMF TA Recommendations on Central Bank Strategic Planning, Risk Management and Cybersecurity

#	Theme	Recommendation	Actor(s)	Time Frame
1	Strategic Planning	Appoint **central bank nonexecutive members** (and provide support for their nonexecutive responsibilities), in line with IMF Safeguards Recommendations.	[Governor to highlight the necessity]	[asap]
2		Adjust the **Strategic Objectives** to express how the central bank intends to deliver the priorities in the Strategic Plan. Undertake a thorough **review of the strategy planning and monitoring procedures** based on the information shared by the mission and re-consider what **strategic planning information** is made public.	Governor (sponsor), Risk Management Department (RMD)	3-6 months 12-24 months
3		Have the **central bank's nonexecutive Board members monitor implementation of the Strategic Plan** at a sufficient frequency and to a sufficient depth, to facilitate timely challenge and support by the nonexecutives.	Board	Ongoing (after appointment)
4	Risk Management	Develop a **Risk Management Framework and Risk Appetite.**	RMD	12-15 months
5		Ensure empowerment and presence of the **risk management function**, including monitoring strategic plan progress and risks, and mandatory participation in the central bank's key forums.	Governor (sponsor), RMD	Ongoing
6		Create further **awareness of risk management** and of the departmental risk champions.	RMD	Ongoing
7		Conduct a **Risk Control Self-Assessment** (RCSA) of processes.	RMD	6-12 months
8		Set up the **incident registration process**.	RMD	12-18 months
9		Incentivize risk management **research and benchmarking**.	RMD	Ongoing
10	Cyber Security	Strengthen the **cyber resilience and security posture**.	RMD, IT Department (ITD)	24 months
11		Build and launch the **Security Operations Center** (SOC) capabilities and perform periodic evaluation exercises.	RMD, ITD	18-30 months
12		Enhance **cybersecurity risk management and security assurance activities** during the evaluation, development or acquisition of new and existing information technology projects and systems.	RMD, ITD	Ongoing
13		Adopt a **cloud computing strategy**.	RMD, ITD	24 months

Source: IMF.

The COVID-19 pandemic has exacerbated possible fintech and cybersecurity risks for central banks even further. Two IMF COVID-19 Special Series Notes[12] highlight specific risk management issues that central banks (could) face in trying to deal with the pandemic and its consequences; another Note highlights the general cybersecurity risks related to working-from-home arrangements. IMF staff recommends that a clear risk management framework (including BCM) is the first and foremost prerequisite for central banks trying to deal with risks related to COVID-19, with a specific focus on nonfinancial risks. Also, "[c]entral banks will need to make adequate preparations prior to return to work (…). This includes maintaining the existing flexible business continuity and risk mitigation arrangements, as well as raising the level of health and safety measures for an extended period of time." Table 3 below provides an overview of the possible COVID-19 risk management measures that central banks could explore, or are already exploring, based on informal discussions with Heads of Risk Management Departments from selected central banks.

Table 3. Example: Overview of Possible COVID-19 Central Bank Risk Management Measures

#	Category	Risk Management Measures	Constraints
1	**Staff-related measures**	• Identifying and sharing best practices in COVID-19 risk management together with financial institutions. • Onsite supervision cancelled. • Reducing reporting requirements (frequency, simplified contents, and term extensions). • Recommendations on fulfilling role in accordance with Government measures (moratory of payments, dividend policy)	• Cross-training of staff for critical functions is complicated in working-at-home environment (suggestion: have junior staff listen in on selected technical discussions).
2	**Board/Management involvement**	• Large-scale issuing of hardware (laptops), including delivering these to staff at home and authorizing use of private laptop in some cases. • Opening IT systems for remote access and implementing the necessary prerequisites/requirements. • Installing additional software (Citrix, Microsoft Teams, OTP applications). • Identify crucial third parties (especially for cloud computing and general IT infrastructure). • Basic telephone lists drafted and distributed among staff in case regular infrastructure fails. • Additional penetration tests conducted to assess IT vulnerabilities.	Support from Board or Management at early stage of the crisis is sometimes difficult, as COVID-19 effects are not fully clear.

[12] IMF Special Series on COVID-19: *Central Banks' "Return to the Workplace" Operational Considerations* (July 22, 2020), *Cybersecurity of Remote Work During Pandemic* (May 6, 2020), and *Central Bank Operational Risk Considerations for COVID-19* (April 29, 2020).

Table 3. Example: Overview of Possible COVID-19 Central Bank Risk Management Measures (Continued)			
		• Increased staff awareness activities, especially relating to phishing (all central banks) and information protection. • Central bank VPN monitored 24x7 by cyber security division.	
3	**Communication**	• Internal: avoiding fake news, boosting morale (videos or messages by Governor and by the Board) providing info on health care services, clear feedback from Board/Management. • External: public communication, as well as sharing information with stakeholders (ministries, other regulators). • In some cases, crisis communication actions were needed after a confirmed case was detected among bank's staff, as well as to avoid fake news.	Difficult to keep up with continuously changing news; central bank needs to be proactive, fast, and accurate.
4	**Interaction with financial sector**	• Identifying and sharing best practices in COVID-19 risk management together with financial institutions. • Onsite supervision cancelled. • Reducing reporting requirements (frequency, simplified contents, and term extensions). • Recommendations on fulfilling role in accordance with Government measures (moratory of payments, dividend policy)	
5	**IT and cyber-security**	• Large-scale issuing of hardware (laptops), including delivering these to staff at home and authorizing use of private laptop in some cases. • Opening IT systems for remote access and implementing the necessary prerequisites/requirements. • Installing additional software (Citrix, Microsoft Teams, OTP applications). • Identify crucial third parties (especially for cloud computing and general IT infrastructure). • Basic telephone lists drafted and distributed among staff in case regular infrastructure fails. • Additional penetration tests conducted to assess IT vulnerabilities. • Increased staff awareness activities, especially relating to phishing (all central banks) and information protection. • Central bank VPN monitored 24x7 by cyber security division.	• Almost no central bank had deployed or tested telework (working-at-home) in a large-scale in the past. • Cyber risk is biggest concern, especially with weak endpoints (e.g., private laptops, including for critical services), and limited data-protection measures. Phishing attacks on staff are on the increase. • Unclear whether IT infrastructure can support this situation in the mid- to long-run/cracks appearing.

Table 3. Example: Overview of Possible COVID-19 Central Bank Risk Management Measures (Concluded)			
6	**Overall risk management**	• Examining if existing legislation and measures are sufficient for (policy and operational) responses. • Increasing monetary policy risk tolerance to allow easier access to liquidity. • Examining overall effects of monetary policy measures on risk exposure of central bank • Reviewing risk appetite. • Strategic risk assessment needed to see if central bank can still achieve its (legal) mandate – need to reprioritize objectives, including postponing larger projects. • Risk Management Department (RMD) plays key role in collecting bank-wide information for Management & Board. In some cases, RMD powers are significantly expanded to collect risk data directly from departments without departmental management involved. • BCM planning were not sufficient (these kinds of extreme scenarios were never included/tested). Some banks had to define new strategies based on worst case scenarios. • Enhanced assessments of critical functions, and staff (when less than 6 people can perform a critical activity). For some central banks critical processes were expanded from the 'normal' 50 to currently 300 – due to predications based on an extended 90-day window for COVID-19 effects • Extension of BCM scope to all central bank activities, including those who were initially considered non-critical. • Development of new internal risk templates to minimize administrative burden on departments.	Legal and reputational risks emerging due to central banks conducting additional (policy) measures, changed public opinion, and effects on financial institutions.
7	**Cash currency management**	• Minimized interpersonal contacts by more shifts, social distancing, additional cleaning/sanitization of buildings and equipment including between shifts. • Quarantining of banknotes between 7 to 15 days. • Still some limited interaction with financial institutions in the form of cash deliveries; no more printing of new banknotes, no more sorting of banknotes and no more flights with banknotes. No sanitization of banknotes was carried out by central banks. • Strategic stock of banknotes in branches is increased to 3 months. • Active encouragement of electronic payments and online transactions (by reducing or eliminating usage fees during the crisis period)	Cash currency management is most sensitive area for new COVID-19 central bank infections.

Source: IMF, 2020, *Central Bank Operational Risk Considerations for COVID-19*. IMF Special Series on COVID-19 Note. Washington D.C.: International Monetary Fund.

B. IMF AIV: Fintech, Cybersecurity, and Risk Management References

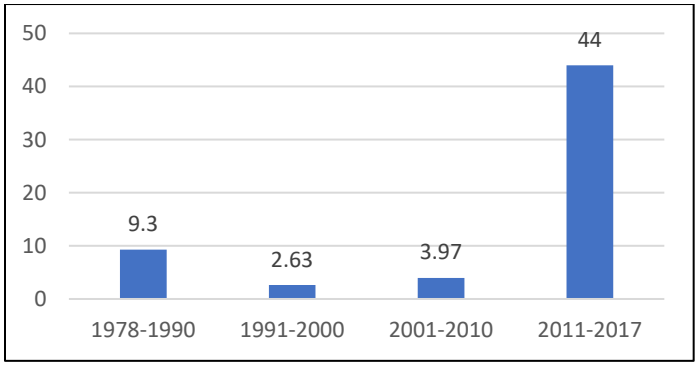
When examining the IMF's Article IV (AIV) database, 1,095 unique hits[13] can be found relating to "technology," spanning the period from 1978 until 2017.

Figure 4 below highlights the number of references per year for different time periods. Clearly, there has been a significant increase in AIV references to technology-related issues in/of the financial sector over the past years, with the period after 2011 showing the bulk of attention for technology-related issues in AIVs.

Figure 5 zooms in on fintech discussions in the one-year period between January 2018 and February 2019—where the majority of fintech issues which are classified as "substantive discussions," followed by the more generic acknowledgement of fintech in the AIV (without further substantive discussion).

The geographical attention for technology-related issues between 1978–2017 is predominantly centered on the African and European regions (Figure 7); in the period January 2018–February 2019 this moved to Asia Pacific and (to a lesser extent) Western Hemisphere (Figure 5). This significantly increased attention coincides with the increase in general attention for "fintech," as Figure 6 demonstrates (Google search for "fintech").

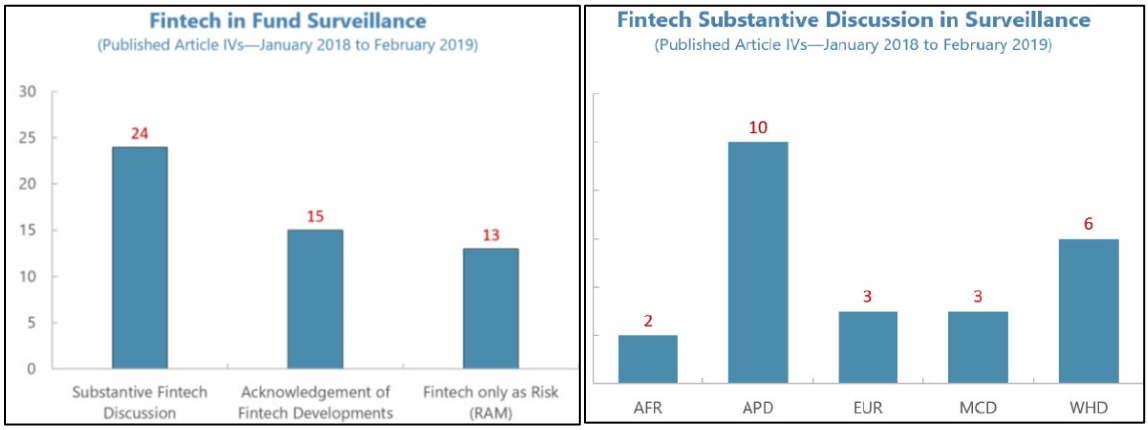
Figure 4. IMF Article IV References to "Technology" (per time period, average per year, 1978–2017)



Source: IMF Staff.

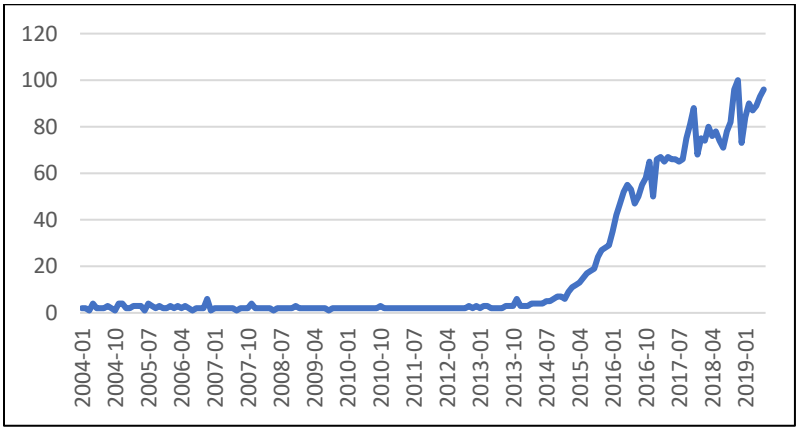
[13] A unique hit relates to an AIV report in a specific time period, for a specific country. One report can contain many references, but the entry is only counted as 1 for the purposes of this paper. Note that the IMF AIV database is an internal database consisting of AIV documents dating back to approximately 1978.

Figure 5. IMF Surveillance and Fintech



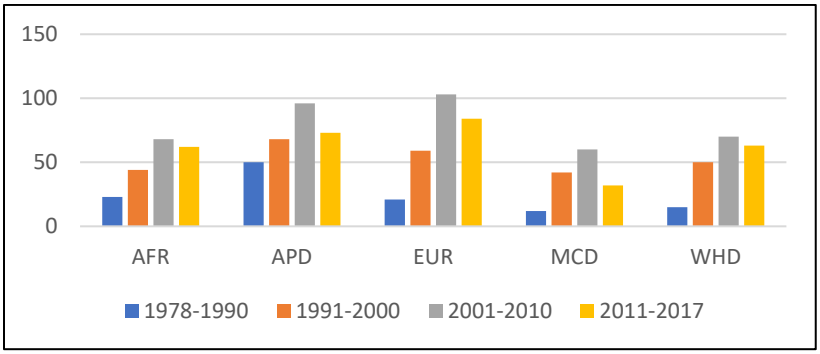
Source: IMF, 2019, *Fintech: The Experience So Far*. IMF Policy Paper, June 2019. Washington, D.C.: International Monetary Fund.

Figure 6. Google Search Interest for "Fintech" (2004–2019)



Source: Google Trends.

Figure 7. IMF Article IV References to "Technology" (per geographical region)



AFR: Africa
APD: Asia and Pacific
EUR: European
MCD: Middle East and Central Asia
WHD: Western Hemisphere

Source: IMF Staff.

It should be noted that "finance and technology" references in the context of AIVs are understandably broader than the current scope of "fintech." The AIV references to finance and technology, as well as cybersecurity, often relate to different sets of findings, such as:

a) General investment/foreign direct investment (FDI) policies;

b) Agricultural technology (including drilling and mining), and other application areas of technology (including space technology); and

c) Fiscal technology (i.e., to improve fiscal operations, including tax revenue collection).

However, within the search results of "finance and technology," several subsets of areas of interest can be identified that could relate to central bank risk management as well, including:

a) **Information (and communication) technology**: references include the building of IT capacity at central banks and Y2K-related risks, which would come closest to the current concept of fintech;

b) **Financial inclusion technology**, which aligns with one of the key goals of fintech often mentioned by central banks—see below;

c) **Digital development strategies**: this includes government-wide strategies, as well as the building of technology hubs (in particular, around the turn of the century), which is similar to jurisdictions like Singapore, UAE, and Hong Kong SAR positioning themselves as fintech hubs and fintech innovation centers.

d) **Telecommunications development**;

e) In occasional cases, explicit references to "**fintech**" can already be found. In the case of one European country reference is made to "regtech" *avant la lettre* (2001), as is the case for "fintech" in another European country (2016); and

f) **Cybersecurity**: out of the 1,095 AIV search hits on technology, only three AIVs could be found with explicit references to cybersecurity. These AIVs all took place after 2015, and generally highlight the role of the authorities in bolstering resilience to cyber-attacks (with one explicit reference to the Bangladesh Bank cyber heist), including in commercial banks.

The IMF[14] notes that the most recent AIV cases where fintech was discussed, relate to links between digital payments and financial inclusion (for instance, Cambodia, Peru, and Tuvalu), as well as "setting up appropriate frameworks and safeguards to develop crypto-assets,

[14] IMF, 2019, *Fintech: The Experience So Far. IMF Policy Report.* Washington, D.C.: International Monetary Fund, pp. 9-12.

including digital currencies projects in small states (the Republic of Marshall Islands (RMI) and Curacao and Sint Maarten).” Additionally, fintech has been brought up in the AIV context regarding China’s fintech industry, and development of financial centers into so-called fintech hubs (such as Hong Kong SAR and Singapore).

On a side note, the links between finance and technology and climate change (risks) should also be noted. In several AIV cases, the links with climate change and the role of the financial sector are made explicit, highlighting how several of the IMF’s overarching policy areas and the accompanying macro-financial risks, are closely related. Examples include considerations on the introduction of low-carbon technologies and noting how the presence of only rudimentary technology has created vulnerabilities to climate change-related issues.

Specific risk management references in the context of “fintech” cover various areas. Most references[15] in the IMF’s AIV database relate to risk management in the context of operational risk for financial sector oversight, that is, in the context of financial supervision. Often, concerns are raised regarding outsourcing of specific activities by financial institutions, and whether third-party risk is managed properly. In those cases where outsourcing aspects of governmental services (including the outsourcing of supervisory functions, and the development of “e-government”) are identified, risk concerns are not often noted explicitly, or possibly overlooked. Instead, the *upsides* of cost-efficiency and higher operational efficiency are more predominant. There is some specific attention for risks of the central bank, especially in cases related to IT, as well as operational risks related to Financial Market Infrastructures (FMIs) and setting up and maintaining infrastructure for RTGS systems.

Central bank-related cybersecurity risks have emerged only more recently. Several AIV cases, predominantly after 2015, refer to “cyber” issues. This relates to initiatives to reinforce central bank cyber-security, especially after the Bangladesh Bank’s “cyber-heist” in February 2016—which is referred to in a couple of cases.

Concludingly, IMF attention for fintech will likely only continue to increase in its areas of surveillance, affecting most of the Fund’s membership. Earlier references in AIVs to finance and technology highlight that IMF staff are aware of opportunities *and* risks that countries—their central banks, supervisors, and other public agencies—might run because of technological developments. Attention has been given predominantly to IT, financial inclusion technology, digital development strategies, telecommunications development, and some initial “fintech” activities. The Fund stresses this increased attention by highlighting that further “advances in AI, digital identification and cybersecurity are enabling new models

[15] Search terms that were used included “outsourcing” (for possible links to outsourcing of IT/technology components of the central bank) and “operational risk” (for possible links to operational risks that the central bank may run related to IT or other technological aspects)

for managing risk for individuals, financial institutions, and regulators."[16] Substantive discussions on fintech in AIVs are increasingly common, and authorities would do well to prepare for these discussions accordingly.

C. IMF FSAP

Attention for the links between risk management, fintech, and cybersecurity in IMF FSAPs is also increasing.

The **Switzerland** FSAP[17] stresses that "[r]isks in the rapidly growing fintech space may not be well understood due to data gaps, resource constraints, and the authorities' liberal approach." It recommends that the Swiss authorities, including the central bank and the financial supervisor, address data collection, analytical capacity, and resources for dealing with fintech-related challenges. This on its turn "should also inform development of fintech-related policies and legislation."

The FSAP on **Singapore**[18] noted that "fintech developments hold the promise of having a far-reaching impact on the Singaporean financial services sector, bringing both opportunities and new risks," for clients, financial institutions, and the financial system as a whole. This could include questions relating to (the applicability of) regulation and the absence of internationally agreed standards, forcing the authorities to "ensure an appropriate balance between opportunities and risks." Though the FSAP mainly talks about *financial institutions*, its statement that "uncertainty surrounding technology" might pose challenges, could likely extend to the central bank (the Monetary Authority of Singapore) as well. Even more so as the main fintech risks are noted as operational and technology-related risks: "Execution risks to implement new strategies and manage business and technology risks are increasingly top risk priorities. Yet a complicating factor are banks' legacy systems with older, slower, and less agile systems increasing banks' inherent risk profile. Additionally, an increasing use and reliance on third-party service providers is evident in the sector" (underlining added). This would, as we have noted already, arguably also apply to central banks, in particular those that have not sufficiently invested in their internal organization, systems, and processes (though it should be stressed that this was not explicitly noted in the Singapore FSAP). Lastly, and importantly, the FSAP also notes that operating a *fintech sandbox* is not without risk to the central bank: "[t]he potential for reputational risk from the regulatory sandbox needs to be monitored. The sandbox is new, and [the Monetary Authority of Singapore] noted its benefits

---

[16] IMF, 2019, *Fintech: The Experience So Far. IMF Policy Report.* Washington, D.C.: International Monetary Fund, p. 9.

[17] IMF, 2019, *Switzerland Financial Sector Assessment Program*. IMF Country Report No. 19/183, June 2019. Washington, D.C.: International Monetary Fund.

[18] See IMF, 2019, *Singapore Financial Sector Assessment Program Technical Note – Fintech: Implications for the Regulation and Supervision of the Financial Sector*. Washington, D.C.: International Monetary Fund.

of facilitating innovation in a controlled environment. The main challenge is to strike a balance between the benefits of fintech firms experimenting in a live environment while mitigating potential downside risks."

In the case of the FSAP on **Canada**[19], IMF staff noted that Canadian authorities were proactive in monitoring fintech developments, including through fintech research which was helpfully conducted to assess the impact on the financial system and the Bank of Canada's core functions. The Canadian Department of Finance, additionally, worked on setting up a new retail payments oversight framework, and examine the possibilities of open banking. Lastly, a so-called "Heads of Agencies Crypto-Asset Working Group was established to coordinate efforts in monitoring developments in crypto-assets with the aim of developing a consistent and clear domestic regulatory framework."

Most recently, in the FSAP on **Korea**,[20] it was noted that "even within an already highly technologically advanced, efficient, and inclusive financial sector, significant benefits can still be reaped from innovation in financial services." However, "new risks could arise in time, such as increasing interconnectedness and complexity in the financial sector, the introduction of greater operational risk, and negative impact on the profitability of incumbent banks."

Figure 8 below provides a schematic overview of the attention for fintech in the selected FSAPs mentioned above, and the specific attention for risks and risk management-related areas.

Figure 8. Selected IMF FSAP References to Fintech

Source: Authors.

[19] See IMF, 2020, *Canada Financial Sector Assessment Program Technical Note – Oversight of Financial Market Infrastructures and Fintech Development*. Washington, D.C.: International Monetary Fund.

[20] See IMF, 2020, *Republic of Korea Financial Sector Assessment Program Technical Note – Technological Change, Legal Frameworks, and Implications for Financial Stability*. Washington, D.C.: International Monetary Fund.

The relevance of IMF attention for finance and technology in AIVs and FSAPs will incentivize further awareness among central banks to ensure adequate understanding and identification of fintech-related risks that they themselves run. Legacy (IT) systems, the involvement of third parties (for instance, in the context of cloud computing—see Section IV. H and Box 2), and already identified nonfinancial risks (operational and reputational, in addition to legal risk), and the need to ensure sufficient resources (which on its turn requires proper strategic planning by the central bank) are key themes.

IV. Fintech and Central Bank Risk Management—Examples

Given the definition of fintech (Section II), and the emerging of attention for fintech in TA, AIVs, and FSAPs (Section III), it is important to examine in more detail *how* fintech developments could possibly affect a central bank's risks and its risk management, by means of examples.

Fintech can hold policy risks related to several core central bank functions. Given the wide range of technologies flagged in Figure 1 above, fintech will likely affect central bank functions such as monetary policy, payments systems regulation, operations, and oversight, financial supervision (and other financial stability functions: macro prudential oversight, resolution, ELA/LOLR), cash currency management, and reserve management, as well as central bank functions in the areas of financial integrity and financial inclusion.

Figure 9 below provides an overview of central bank risks: **strategy and policy risk** (that are inherently the result of the central bank's overall strategy and its policies), **financial risk** (as a result of financial operations), and **operational risk** (based on wide variety of risk categories, including IT infrastructure, cybersecurity, outsourcing, governance, and processes). Tying these together is **reputational risk**—a risk category that results from one or more of the other risks materializing. The subsections below will delve deeper into (i) policy risk emanating from selected central bank functions, as well as (ii) operational risk emanating from the central bank's internal organization, to highlight how fintech and cybersecurity developments might offer opportunities to a central bank, but simultaneously also introduce or exacerbate existing central bank nonfinancial risks. This, on its turn, highlights the continued need for stronger central bank risk management, in particular as many of the highlighted risks overlap: central banks, therefore, should ensure an integrated fintech and cybersecurity analysis, including through the lens of central bank risk management.

Figure 9. Central Bank Risk Landscape

Source: Source: IMF, 2020, *A Survey of Research on Retail Central Bank Digital Currency*, IMF Working Paper 20/104. Washington, D.C.: International Monetary Fund.

A. Monetary Policy & Operations

Various IMF staff have identified fintech-related opportunities in the realm of monetary policy and monetary policy operations—with a particular focus CBDC.[21] This includes effects to increase the effectiveness of monetary policy transmission, increase seigniorage income for central banks, facilitate cross-border payments,[22] and—in the case of a wholesale CBDC—facilitate wholesale payments or improve the effectiveness of existing Real Time Gross Settlement Systems (RTGS). Some IMF staff have also explored whether a CBDC could be designed with attributes like cash or deposits, and whether they could be interest-bearing.[23]

Most authors note that CBDCs carry a form of risk to the central bank as well, in addition to benefits. For digital money across borders, for instance, the IMF finds that foreign CBDCs, as well as Global Stable Coins (GSC) could "raise pressures for currency substitution and worsen vulnerabilities from currency mismatches. They could reduce the ability of local authorities to run monetary policy. [And] they could facilitate illicit flows and make it harder

[21] IMF, 2018, *Casting Light on Central Bank Digital Currency*, Staff Discussion Note 18/08. Washington, D.C.: International Monetary Fund. And: Committee on Payments and Market Infrastructures, 2018, *Central Bank Digital Currencies*. Basel: Bank for International Settlements.

[22] See, for instance, IMF, 2020, *Digital Money Across Borders: Macro-Financial Implications*. Washington, D.C.: International Monetary Fund.

[23] Agur, I., G. Dell'Ariccia, 2019, *Designing Central Bank Digital Currencies*. IMF Working Paper (19/252). Washington, D.C.: International Monetary Fund.

for regulatory authorities to enforce exchange restrictions and capital flow management measures."[24] All of these issues are clearly contingent on the design of the CBDC, and the literature is very much in development.

Other relevant monetary policy aspects include broader issues relating to access to central bank money and its risk implication. That is, the provision of credit facilities, collateral and prefunding arrangements, and operational risk considerations. Central bank examples include, for example, the Bank of England's access provision to TransferWise, as well as access to the non-bank switching company in the Australian National Payment Platform.

B. Financial Market Infrastructures

FMIs[25] play an important role in a country's financial system at large. The 2012 Committee on Payments Market Infrastructures[26] Principles for Financial Markets Infrastructures (PFMI) were drafted precisely to help identify and mitigate risks related to this systemic nature of FMIs. FMIs "facilitate the clearing, settlement, and recording of monetary and other financial transactions [which] can strengthen the markets they serve and play a critical role in fostering financial stability." Given this role, they could also "pose significant risks to the

Box 1. Distributed Ledger Technology Experiments in Payments and Settlements

Distributed Ledger Technology (DLT) is a possible platform for enhancing payment systems by integrating and reconciliating settlement accounts and ledgers. Various central banks have conducted DLT research (and experiments with large-value interbank payments) to examine benefits, risks, limitations, and implementation challenges of DLT in the context of payments and settlements. This includes Brazil. Canada, the Euro area/Japan, Singapore, South Africa, and Thailand. Some central banks and private sector participants have also examined DLT for cross-border payments.

Key risks of DLT, and other technologies, for payments and settlements include liquidity, credit, transaction delay, settlement finality, counterparty, and operational risks. The latter category includes cyber risk incidents. Even though these operational risks are not different from the standard computerized processing, it is the faster (real-time) environment that requires "very fast and highly automated error-handling processes to limit the volume of transactions affected by operational errors." This, on its turn, "calls for improved monitoring systems and error-correction solutions." Additionally, cyberattacks could "compromise data confidentiality, service availability, and systems integrity (…) [and] also affect established settlement finality rules and recovery time objectives."

The potential benefits of DLT therefore require careful consideration from a (central bank) risk management perspective.

Source: Shabsigh, G., T. Khiaonarong, e.a., 2020, *Distributed Ledger Technology Experiments in Payments and Settlements*, IMF Fintech Note. Washington, D.C.: International Monetary Fund.

[24] IMF, 2020, *Digital Money Across Borders: Macro-Financial Implications*. Washington, D.C.: International Monetary Fund.

[25] Which includes payments systems, Central Securities Depositories, Securities Settlement Systems, Central Counterparties, and Trade Repositories.

[26] Previously: Committee on Payment and Settlement Systems, renamed in June 2014.

financial system and be a potential source of contagion, particularly in periods of market stress."[27]

Payments systems operations and oversight are closely linked to fintech developments. The use and operation of (real-time) settlement systems[28] are examined by several central banks from the viewpoint of increasing effectiveness, and/or security by applying distributed ledger technology (see Box 1). Not surprisingly, the Reserve Bank of India (RBI) recently indicated that payment and settlement systems are "technology-based substitutes for currency," tying fintech developments in this area unequivocally to not only its FMI, but to its currency management and monetary policy functions.[29]

The PFMI offer existing guidance on how to deal with fintech-related operational risks. Principle 17 expands on this and puts the key responsibility with the board of directors for defining operational risk (both roles and responsibilities, as well as endorsing the framework). It goes on to specify details on business continuity plans, policies relating to physical and information security, as well as outsourcing risks, and how monitoring should ideally take place. The PMFI highlight similarity with commercial risk management practices, stressing that commercial standards on information security, business continuity, and project management can be helpful for FMIs.

As an example, the RBI stresses in its recently updated Booklet on Payment Systems[30] regarding its FMI oversight framework that the payment landscape "has experienced extensive leveraging of advanced technology in facilitating processing of payment transactions by the PSOs [Payment Systems Operators] as well as their service providers/intermediaries/third party vendors and other entities in the payment ecosystem. On the other hand, the number, frequency and impact of cyber incidents/attacks have increased manifold."

C. Reserve Management

As per the IMF definition,[31] central banks' reserve management relates to ensuring that there are adequate official public sector foreign assets. These need to be readily available to, and

---

[27] BIS, 2012, *Principles for Financial Markets Infrastructures*. Basel: Bank for International Settlement. See p.5.

[28] A common case of a central bank acting as an FMI is the services it provides through the RTGS. In an RTGS, transfers from one bank to another take place in real time and on a gross basis. RTGS' are essential for a smooth and efficient banking system. The central bank can provide the RTGS infrastructure.

[29] RBI, 2018, *Reserve Bank of India releases Dissent Note on Inter-Ministerial Committee for finalization of Amendments to PSS Act*, RBI Press Release, October 19, 2018.

[30] RBI, 2021, Booklet on Payment Systems (January 25, 2021). Mumbai: Reserve Bank of India; accessible via: https://m.rbi.org.in/scripts/PublicationsView.aspx?Id=20315#AP3.

[31] IMF, 2013, *Guidelines on FX Reserve Management*. Washington, D.C.: International Monetary Fund.

controlled by, the authorities for meeting their (pre-defined) objectives. Reserve management is clearly a central bank activity related to core policy decisions.[32] The buying, selling, and managing of the central bank's foreign assets entail risk; not just financial, but also nonfinancial. "Reserve management should seek to ensure that (1) adequate foreign exchange reserves are available for meeting a defined range of objectives; (2) liquidity, market, credit, legal, settlement, custodial, and operational risks are controlled in a prudent manner; and (3) subject to liquidity and other risk constraints, reasonable risk-adjusted returns are generated over the medium to long term on the funds invested."[33] (underlining added)

To contain/mitigate reserve management's operational risks, proper internal governance arrangements are essential. The IMF Guidelines highlight, for instance, the need to "be guided by the principles of clear allocation and separation of responsibilities and accountabilities." The central bank is advised to have "appropriate hierarchical levels", a "committee structure", and a clear separation/independence of the investment side from the risk control/management side to avoid improper incentives. Reserve management also requires checks and balances in the form of internal audits and well-trained staff. Most indicative of the operational risk effects that reserve management activities can have, is the statement that "it is important to identify the level of authority that would reconcile inconsistencies or interferences between reserve management activities and other central bank functions. Unwanted signaling effects from reserve management operations should be avoided."[34]

The IMF Guidelines on FX Reserve Management present[35] several clear examples of operational risks related to reserve management:

a) *Control system failure risks*: There have been a few cases of outright fraud, money laundering, and theft of reserve assets that were made possible by weak or missing control procedures, inadequate skills, poor separation of duties, and collusion among reserve management staff members.

b) *Financial error risk*: Incorrect measurement of the net foreign currency position has exposed reserve management entities to large and unintended exchange rate risks and led to large losses when exchange rate changes have been adverse. This has also occurred when risk has been measured only by reference to the currency composition of reserves directly under management by the reserve management unit and has not included other

[32] Ibid., Article 50: "Reserve management strategies should be consistent with and supportive of a country's or union's specific policy environment, in particular it's monetary and exchange arrangements."

[33] Ibid., Article 8.

[34] Ibid., Section C, articles 24–33.

[35] Ibid., p.26.

foreign currency-denominated assets and liabilities on and off the reserve management entity's balance sheet.

c) *Financial misstatement risk*: In measuring and reporting official foreign exchange reserves, some authorities have incorrectly included funds that have been lent to domestic banks or to foreign branches of domestic banks. Similarly, placements with a reserve management entity's own foreign subsidiaries have also been incorrectly reported as reserve assets.

d) *Loss of potential income*: A failure to reinvest funds accumulating in clearing (nostro) accounts with foreign banks in a timely manner has given rise to the loss of significant amounts of potential revenue. This problem arises from inadequate procedures for monitoring and managing settlements and other cash flows and for reconciling statements from counterparts with internal records.

In all these examples, fintech could assist central banks to enhance their reserve management, for instance, by allowing machine learning applications to analyze financial patterns, identify possibly anomalies (such as related to fraud), and allow for enhanced data reporting to a central bank's first and second lines of defense. The two most relevant fintech applications for asset management in general, as noted in a PWC study,[36] relate to (i) increased sophistication of data analytics to better identify and quantify risk, and (ii) automation of asset allocation. As such, PWC notes that "[m]achine learning technology is transforming risk management by enabling computers to identify patterns in market behavior and analyze transactions almost in real time." It is not unimaginable that central bank reserve and asset managers would similarly benefit from fintech applications.

D. Financial Inclusion

Financial inclusion implies that individuals and businesses have access to useful and affordable financial products and services that meet their needs, and that are delivered in a secure, responsible, and sustainable way. Central banks increasingly have specific roles on, and responsibilities for (stimulating and/or supporting) financial inclusion, as noted above.

Fintech carries significant direct gains for financial inclusion by contributing to increased financial sector efficiency. Fintech could (1) facilitate access to credit, insurance, and pension products, (2) lower costs of cross-border transfers (including worker remittances), (3) stimulate tailored investment products, and (4) strengthen financial literacy and education. Relevant technologies relate to mobile access, API and Internet, Big data and AI, DLT, and cryptography. Indirect fintech gains could be found, for instance, by using DLT payment systems to enhance real-time payments—which could eventually help customers of

[36] PWC, 2016, *Beyond Automated Advice - How FinTech is Shaping Asset & Wealth Management*. PWC Global FinTech Survey 2016.

pay day lenders. Financial inclusion cases using fintech tools in one way or another can be found in different regions of the world.[37] Often, a combination of a high financial exclusion rate with a high cellphone penetration rate allows for leapfrogging in providing financial services to the unbanked and poorest parts of the population.

The IMF[38] (in the context of developments in Asia) stresses that fintech could support "growth and poverty reduction by strengthening financial development, inclusion, and efficiency," supported by strong cellphone penetration in particular (see Zhang and Chen[39] for the case of China in particular). This would allow fintech applications in the areas of micro loans, as well as bookkeeping and accounting tools for Small- and Medium-Sized Enterprises.

Other central banks have indicated that they would want to enhance their decision-making on fintech and financial inclusion. The RBI, for instance, wants to "further deepen digital payments and enhance financial inclusion through FinTech… [by] appoint[ing] a five-member committee under the chairmanship of Shri Nandan Nilekani."[40]

Fintech could enhance financial inclusion by increased loan allocation, and lower rates—but also carries risks, including from a consumer protection perspective. See for instance Bazarbash,[41] who indicates that, in particular, fintech credit "has the potential to enhance financial inclusion and outperform traditional credit scoring by (1) leveraging nontraditional data sources to improve the assessment of the borrower's track record; (2) appraising collateral value; (3) forecasting income prospects; and (4) predicting changes in general conditions." This could lead to significantly shortened credit allocation times and lower loan rates.

However, he also stresses that overreliance on learning from data could lead to opposite effects: the exclusion of creditworthy applicants. Financial institutions and central banks

---

[37] E.g., UAE and Saudi Arabia collaborate on a digital currency for cross-border settlements project, intended to provide "affordable financial services." Papua New Guinea developed its "IdBox" pilot to foster financial inclusion through strengthened personal identification methods. Mobile money, and other mobile applications have been tried and tested over the past decade in many emerging and developing countries (Kenya being the key example)—including mobile data-based credit registries in Latin-America. Financial literacy is enhanced by fintechs providing financial product advice, such as in India, where consumers can get callbacks with free advice on a range of financial services, many of which are often cellphone-based.

[38] IMF, 2018, *Asia at the Forefront: Growth Challenges for the Next Decade and Beyond*. IMF Regional Economic Outlook Asia and Pacific, October 2018. Washington, D.C.: International Monetary Fund.

[39] Zhang, L, S. Chen, 2019, *China's Digital Economy: Opportunities and Risks*. IMF Working Paper, 19/16. Washington, D.C.: International Monetary Fund.

[40] Das, S., 2019, *Opportunities and Challenges of FinTech*, Speech by the Governor of the Reserve Bank of India, NITI Aayog's FinTech Conclave, March 25, 2019.

[41] Bazarbash, M., 2019, *FinTech in Financial Inclusion – Machine Learning Applications in Assessing Credit Risk*. IMF Working Paper 19/109. Washington, D.C.: International Monetary Fund.

should therefore be aware of these risks and address them accordingly—this holds even more for central banks that have an explicit legal mandate on financial inclusion or consumer protection. Berkmen, Beaton, e.a.[42] (for Latin America and the Caribbean) similarly indicate that regulatory frameworks and supervisory practices should "be adapted for orderly development and stability of the financial system, to facilitate the safe entry of new products, activities, and intermediaries and to respond to and prevent stability and integrity risks."

E. Financial Supervision[43]

Closely linked to what is noted above on financial inclusion, the potential effects of fintech on/for financial supervision are similarly substantial. On the one hand, supervised entities are increasingly employing a wide range of fintech tools to ensure more efficient and effective reporting to the supervisor and regulatory compliance in general ("regtech"). On the other hand, financial supervisors themselves are exploring possibilities of using fintech tools to enhance their means and methods of (risk-based) supervision as well ("suptech").

Central banks and financial supervisors have started to recognize opportunities and risks that are linked to these developments. RBI stresses that early recognition of fintech risks and challenges is crucial. Not just to use fintech to the advantage of the supervisor (with RBI "suptech" examples such as their Import Data Processing and Monitoring System, Export Data Processing and Monitoring System, and the Central Repository of Information on Large Credits), but also to enhance the RBI's risk-based supervision in general, with an even stronger basis in data-driven risk analytics, for instance. Risk management is crucial, as Governor Das noted:[44]

> A strong risk culture—in which risk detection, assessment and mitigation are part of the daily job of bank staff—will be central to the success of managing the emerging risks. Similarly, systemic risks may arise from unsustainable credit growth, increased inter-connectedness, procyclicality, development of new activities beyond the supervisory framework and financial risks manifested by lower profitability. Risks for FinTech products may also arise from cross border legal and regulatory issues. Data confidentiality and customer protection are major areas that also need to be addressed.

---

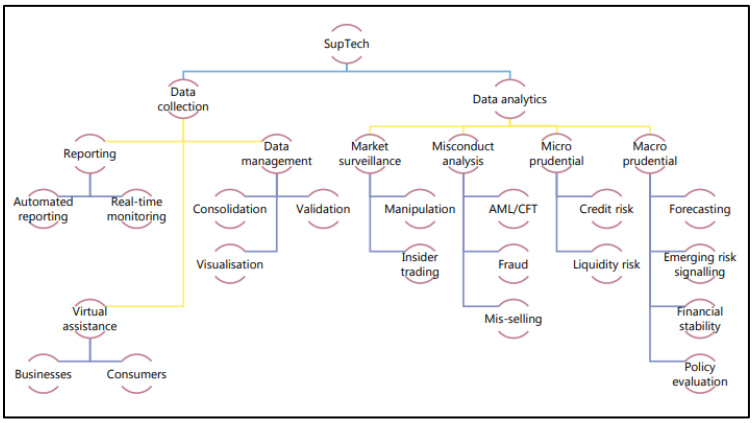
[42] Berkmen, P., K. Beaton, e.a., 2019, *Fintech in Latin America and the Caribbean: Stocktaking*. IMF Working Paper 19/71. Washington, D.C.: International Monetary Fund.

[43] Larger financial stability policy risks (such as related to macro prudential oversight, resolution, and ELA/LOLR) are of course also possible. See, for instance, IMF, 2020, *Digital Money Across Borders: Macro-Financial Implications*. Washington, D.C.: International Monetary Fund.

[44] See footnote 40.

The Financial Stability Institute (FSI)[45] has identified opportunities *and* risks for financial supervisors. The suptech opportunities predominantly relate to data-collection, as well as subsequent data-analytics, with examples spanning real-time monitoring to early identification of insider trading. See Figure 10 below.

Figure 10. Areas of Financial Supervision in which Suptech Applications are Used



Source: FSI.

As far as suptech-related risks go, the list below is based on the eight noted FSI categories of challenges/risks for central banks that are also financial supervisors:

1) *Technical risk*: e.g., computational capacity constraints, as well as lack of transparency on how certain technologies work (this could include algorithmic governance issues). See also further on AI/ML.

2) *Data quality risk*: quality as well as completeness of data from non-traditional sources (such as social media) can create issues. Similarly, the size of data, for instance regarding equity and derivatives markets transactions, could pose a "too big to handle" issue for supervisors.

3) *Legal risk*: enhanced data collection could create additional legal risk, for instance, when data privacy (and legal obligations on data privacy) are violated.

4) *Operational risk*: "[h]eightened operational risks, including cyber-risk, were mentioned underscoring the need for improved risk management in supervisory agencies when using suptech applications." This is specifically a concern for open source and third party and cloud applications: "[i]ncreased third-party risks related to cloud computing and algorithm providers can result when data is transmitted online or is handled by third parties. Data security issues may also arise in the context of

[45] FSI, 2018, *Innovative Technology in Financial Supervision (suptech)—The Experience of Early Users*. FSI Insights on Policy Implementation, No. 9. Basel: Financial Stability Institute. See pp.17–19.

supervisory reporting applications where the supervisors' and the banks' systems are interconnected… A robust risk management and control framework should therefore accompany the use of suptech." In addition, common platform vulnerabilities or back-doors among these third parties or cloud providers may pose a difficult risk to manage due to its complexity and far reach. A recent example is the SolarWinds[46, 47] security incident that impacted many large and reputable organizations including financial institutions[48] and even security service providers.[49]

5) *Reputational risk*: false positives or false negatives because of an increased use of suptech could damage the supervisor's reputation. Lacking transparency in "black-box algorithms" could similarly negatively affect the accountability of the supervisor (ref. Toronto Center, 2018), as well as damage their reputation and trust in general.

6) *Resource risk*: supervisors face additional constraints in finding staff that is sufficiently trained and experienced in dealing with fintech-related issues. Roles such as finding the right use-cases or researching and exploring the technical and financial risks associated with these emerging solutions.

7) *Internal support system risk*: based on the survey of the authors, supervisors can face issues with lacking or insufficient internal support from the supervisor's management and/or Board. This could in part be due to a lack of understanding, as well as the need to incorporate fintech-related issues into the strategic planning cycle of the supervisor and prioritize accordingly.

8) *Practical issues*: examples are mentioned of procurement processes that could take long, which is another form of operational risks for the supervisor.

Fintech developments could also lead to (further) regulatory arbitrage. Lukonga[50] points out that gaps in domestic regulation and supervision could "create opportunities for cross-sector and cross-border regulatory arbitrage. Non-bank payment service providers, such as telecommunication and technology companies, do not immediately fit neatly into the

---

[46] https://www.solarwinds.com/securityadvisory. In the SolarWinds hack, U.S. government agencies (such as the Department of Homeland Security) and companies (including U.S. telecom operators, and Microsoft) were targeted by hackers via third-party vendor that supplied software to those agencies.

[47] https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

[48] https://www.bankinfosecurity.com/us-treasury-suffers-significant-solarwinds-breach-a-15641. U.S. Treasury Suffered 'Significant' SolarWinds Breach.

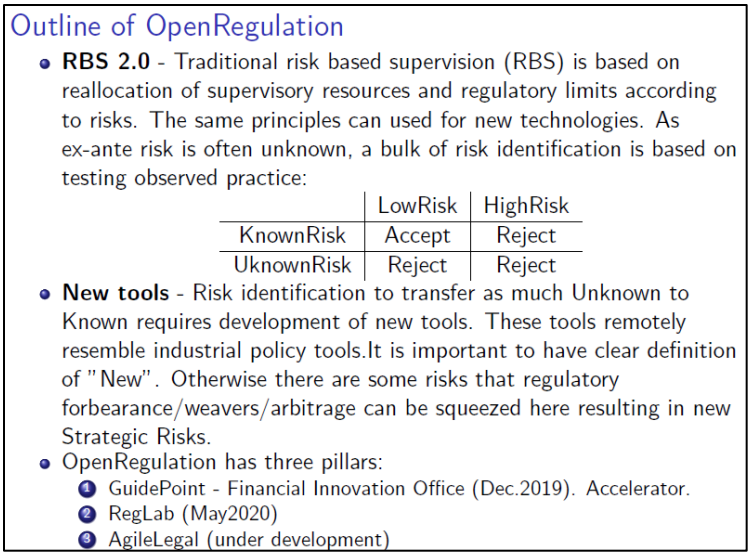
[49] https://threatit.com/articles/lists-of-companies-affected-by-the-solarwinds-hack-published/. Security providers

[50] Lukonga, I., 2018, *Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Region*s, IMF Working Paper 18/201. Washington, D.C.: International Monetary Fund.

jurisdiction of any specific regulatory authority, or there may be ambiguity as to which authority is responsible for the non-banks." An additional issue of regulatory arbitrage could be sparked due to the (significant) cost of implementation of suptech. This might only be feasible for some market participants (such as bigtech/incumbent firms), limiting SMEs to implement suptech solutions. This, on its turn, could also lead to a separation in tech and non-tech supervision, creating an additional regulatory arbitrage environment.

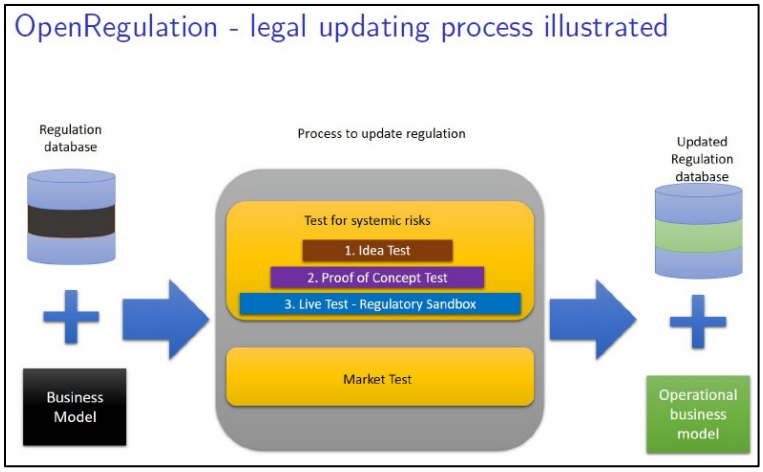
As an example of fintech in the financial supervision context, the National Bank of Georgia (NBG)'s Financial Technology Strategy Department (FTSD) has identified a number of key fintech-related risks to the Georgian financial sector. In specific, it notes that the principle of risk-based supervision can be applied to fintech developments, leading to tailormade tools to emerge. The NBG's approach is dubbed "OpenRegulation," and consists of three main pillars: (i) GuidePoint, (ii) RegLab, and (iii) AgileLegal. All three pillars target fintech innovation and risks in a manner that allows the NBG as financial supervisor to keep track of new and emerging risks – see figure 11 below. This approach, subsequently, feeds into a process that allows the NBG to, as frequently as needed, update its regulatory database. This includes testing of new, updated rules in a regulatory sandbox environment before rolled out to the financial sector in general. See Figure 12 below. As noted in Section III. A above, information on these developments can helpfully tie into a central bank's internal risk management, identifying possible policy and operational risks that the central bank might run.

Figure 11. National Bank of Georgia: Outline of OpenRegulation



Source: National Bank of Georgia.

Figure 12. National Bank of Georgia: OpenRegulation—Legal Updating Process Illustrated



Source: National Bank of Georgia.

F. Financial Integrity[51]

Financial integrity is a high-level goal of the international community. It is a broad concept that covers measures to prevent and combat money laundering (ML), it predicate offences, terrorism financing (TF), and proliferation financing (PF), as well as measures that while may not be specifically covered by the Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) standard, are nonetheless indispensable to support an effective AML/CFT system.[52] These include, for example, measures aimed at preventing and combating specific predicate crimes, such as corruption and tax crime, as well as fostering good governance. Central banks have a responsibility to help ensure that a country's financial sector is insulated from illicit flows and criminal activity. As such, financial integrity is an important aspect of several functions of central banks (supervisory, financial inclusions, and general financial sector oversight), the primary of which are discussed below.

While harboring many potential and actual benefits, fintech developments (especially in the realm of virtual assets (VAs)[53] and virtual asset service providers (VASPs)) raise new challenges for authorities, including central banks, and are accompanied by a number of risks (e.g., related to their frequently anonymous, or pseudonymous, nature. To address these risks,

[51] This subsection was drafted with assistance from Kathleen Kao and Nadine Schwartz (IMF Legal Department/Financial Integrity Group).

[52] IMF, 2018, *Review of the Fund' Strategy on Anti-Money Laundering and Combatting the Financing of Terrorism*, IMF Policy Paper, October 2018. Washington, D.C.: International Monetary Fund.

[53] The FATF uses the terminology "virtual asset" for "a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes". The term is used interchangeably with crypto-assets and digital assets in this paper.

in 2018, the Financial Action Task Force (FATF) —the international standard setting body for AML/CFT—updated its standard to cover VAs and VASPs.[54] Countries are required to identify, assess, and understand the ML/TF emerging from VA and VASP activities in their jurisdiction. Based on that assessment, countries should, on a risk-basis, implement the necessary measures to prevent and mitigate the risks identified. The BFA, Principle VII, pre-empted these responsibilities, noting specifically that "countries should safeguard the integrity of financial systems by identifying, understanding, assessing, and mitigating the Fintech-related risks of criminal misuse and by using technologies that strengthen compliance with AML/CFT measures."

For central banks, these developments will very likely have policy effects and related risks. As noted in subsection E (Financial Supervision), regulatory frameworks and supervisory practices will need to be adapted for the orderly development and stability of the financial system, to facilitate the safe entry of new products, activities, and intermediaries and to respond to and prevent stability *and* integrity risks. New financial intermediaries will impact financial sector oversight in terms of resource and capacity implications. The possibility of such new intermediaries becoming systemically important entities presents financial stability and integrity concerns as these non-traditional players may not be as equipped to handle financial integrity (and other) risks—thereby contributing to (significant) strategy and policy risk of the central bank. Additional legal and reputational risks could increase as well, for instance, when questions arise regarding the validity of the existing legal framework, and the speed and efficiency of, and communication surrounding relevant central bank actions.

In their supervisory role, central banks will need to ensure that they (i.e., decision-makers and staff alike) are up to speed with fintech developments that could affect financial integrity —examples include expertise with and knowledge of crypto-assets (and their attendant risks), as well as of regtech solutions that might be applied by supervised entities relating to (ongoing) client screening, transaction monitoring, supervisory data reporting, and advanced data-analytics on Big data, allowing for more enhanced and cost-effective anomalous pattern detection, including the identification of suspicious transactions. Such an understanding is even more critical for central banks who are the designated AML/CFT supervisor in a country. Pursuant to the standard, financial institutions and intermediaries (both existing and new) are also required to understand and mitigate risks associated with VAs—where a central bank is the designated supervisor, it would be responsible for ensuring that such obligations are met. On the other hand, fintech developments (in the form of suptech) can also assist central banks in the conduct of their supervisory activities (see subsection E).[55]

[54] FATF, 2018, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

[55] BIS, 2018, https://www.bis.org/fsi/publ/insights9.pdf.

Some central banks also house their country's Financial Intelligence Unit (FIU). FIUs generally serve as a national center for the receipt and analysis of information relevant to ML, associated predicate offences, and TF/PF, in the form of suspicious transaction reports (STRs). FIUs are also responsible for analyzing the information received and disseminating the results of their analysis to the relevant law enforcement authorities. In this capacity, FIUs must be knowledgeable about and stay current on the different modalities, mechanisms, and schemes by which ML and TF occur. It is therefore important for FIUs to have an in-depth and up-to-date understanding of fintech developments, products, and services, to inform their analytical work. Fintech could greatly facilitate advanced data-analytics and could therefore be extremely useful to an FIU. However, as noted above with respect to the supervisory role of a central bank, such developments require a certain level of human capacity (in terms of knowledge, expertise, and experience).

The mentioned risks could also emerge from decisions made in the formulation of monetary policy. As noted in subsection A (Monetary Policy), CBDCs and GSCs are recognized as having financial integrity risks and, if not effectively regulated, could contribute to facilitating illicit financial flows. In its recent report to the G20, the FATF identified anonymity, global reach, and layering as being particular ML/TF vulnerabilities for GSCs.[56] The BIS has stated that to mitigate these risks, "providers of stablecoins and other entities that are part of a stablecoin ecosystem should comply with the highest international standards for AML/CFT".[57] Where a central bank has an AML/CFT supervisory role, it would need to ensure that financial intermediaries and other service providers dealing with and/or administering stablecoins are following AML/CFT rules and regulations.

Depending on the specific model issued, the creation of a CBDC might also generate new functions and responsibilities for a central bank (such as holding customer accounts for retail CBDC).[58] These new functions may require that a central bank itself adheres to AML/CFT regulations when conducting its operations and may have larger implications on a country's legal/regulatory framework (e.g., who to supervise the supervisor).

All the foregoing requires a central bank to seriously consider the impact of fintech developments on its functions and activities, as well as the activities of the financial sector and among entities it supervises.

---

[56] FATF, 2020, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.

[57] BIS, 2019, https://www.bis.org/cpmi/publ/d187.pdf.

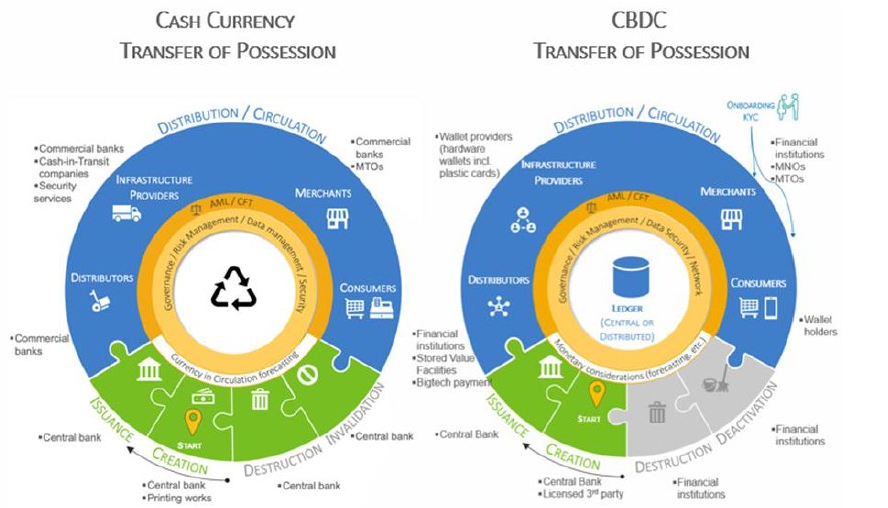
[58] See also, IMF, 2020, *A Survey of Research on Retail Central Bank Digital Currency*, IMF Working Paper 20/104. Washington, D.C.: International Monetary Fund.

G. Cash Currency Management

Cash currency management is one of the oldest functions of central banks. It incorporates aspects related to design and security features of bank notes (and often coins as well), procurement and production issues, logistics (including storage, distribution, invalidation, and destruction), and aspects of modelling and forecasting cash currency demand—see Figure 10 below regarding the cash currency lifecycle and transfer of possession. Most countries have their own currency, and some countries use another country's currency (referred to as "dollarization", given the frequent use of the U.S. dollar,[59] though "euroization" is not uncommon either,[60] nor is the use of the Australian dollar)[61].

Fintech-related policy risks for cash management relate predominantly to the possible use of CBDC. Numerous countries are currently exploring the possibilities of issuing a CBDC, either stand-alone, or in combination with cash—see Figure 13 below. Some countries are simply conducting basic research, others have conducted (and concluded) experiments. Policy risks related to the introduction of a CBDC could stem from a lack of understanding of effects CBDC may have on society, including how this will affect the monetary policy transmission mechanism (see also subsection A). Figure 13 could similarly be applied to the different phases of creation, issuance, distribution/circulation, and invalidation and destruction of CBDC—and the nonfinancial risks related to each of those phases.

Figure 13. Cash Currency and CBDC—Transfer of Possession



Source: IMF, 2020, *A Survey of Research on Retail Central Bank Digital Currency*, IMF Working Paper 20/104. Washington, D.C.: International Monetary Fund.

[59] For instance, in Ecuador, El Salvador, the Marshal Islands, Micronesia, Palau, Panama, and Timor-Leste.

[60] For instance, in Kosovo, Montenegro, and San Marino.

[61] In the case of Kiribati.

Figure 14. Countries Where Retail CBDC is Being Explored

Jurisdictions Where Retail CBDC Is Being Explored (as of May 27, 2020)	
Where central banks are in the advanced stages of retail CBDC exploration	
Bahamas (pilot launched)	Sweden (proof of concept started)
China (pilot launched)	Ukraine (pilot completed)
Eastern Caribbean (pilot launched)	Uruguay (pilot completed)
South Africa	
Where central banks have explored or are exploring issuing retail CBDC	
Australia	Jamaica
Brazil	Japan
Canada	Korea (proof of concept started)
Chile	Mauritius
Curaçao en Sint Maarten	Morocco
Denmark	New Zealand
Ecuador (completed pilot & project discontinued)	Norway
Euro Area	Russia
Finland	Switzerland
Ghana	Trinidad and Tobago
Hong Kong SAR	Tunisia
Iceland	Turkey
India	United Kingdom
Indonesia	United States
Israel	
Where central banks have explored or are exploring issuing retail CBDC (unconfirmed)	
Bahrain	*Lebanon*
Egypt	*Pakistan*
Haiti	*Palestine*
Iran	*Philippines*
Kazakhstan	*Rwanda*
Sources: Central banks or various news sources per hyperlinks above. *Italicized* entries are sourced from news articles. Information has not been verified through official channels.	

Source: IMF, 2020, *A Survey of Research on Retail Central Bank Digital Currency*, IMF Working Paper 20/104. Washington, D.C.: International Monetary Fund.

Operational risks related to possession in particular could be similar for cash and CBDC: both cash and its digital equivalent need to be (1) forecasted (taking into account relevant economic data, including cyclical demand linked to, for instance, agricultural cycles, significant national holidays and other festivities, as well as reasonably predictable shocks, such as adverse weather or even natural disasters), (2) designed while taking into account optical designs (often reflecting symbols of national identity), as well as security aspects to prevent or significantly limit counterfeiting, (3) printed (or, in the case of a CBDC: entered into a database/created as a token), (4) put into circulation, and (5) possibly be invalidated and/or destroyed.

Lastly, a recent IMF Working Paper also highlighted the legal risk that a central bank might run in the case of considering a CBDC, as "[f]irst, most central bank laws do not currently authorize the issuance of CBDC to the general public. Second, from a monetary law perspective, it is not evident that "currency" status can be attributed to CBDC. While the central bank law issue can be solved through rather strai[g]thforward law reform, the monetary law issue poses fund[e]mental legal policy challenges."[62]

[62] Bossu, W., M. Itatani, e.a., 2020, *Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations*. IMF Working Paper (20/254). Washington, D.C.: International Monetary Fund.

In summary, though fintech carries opportunities for central banks, policy, strategy, and operational risks to the financial system *and* for central banks and financial supervisors themselves need to be addressed. As mentioned above, this holds for financial integrity, financial inclusion, as well as of course for financial supervision and other financial stability-related areas where fintech tools might be applied. Proportional regulation should ensure that potential risks associated with fintech are effectively monitored and addressed without unduly stifling innovation and undermining consumer protection and financial inclusion. Legal frameworks will need to adapt to keep pace with innovation and ensure proper calibration of new risks, legal certainty, predictability, and the balance between transparency and privacy. Financial integrity (including AML/CFT) requires specific attention, preventing fintech applications to circumvent or evade current controls, and the usage of new products to criminal ends. Operational risks linked to each of these policy areas could increase in likelihood and/or possible impact.

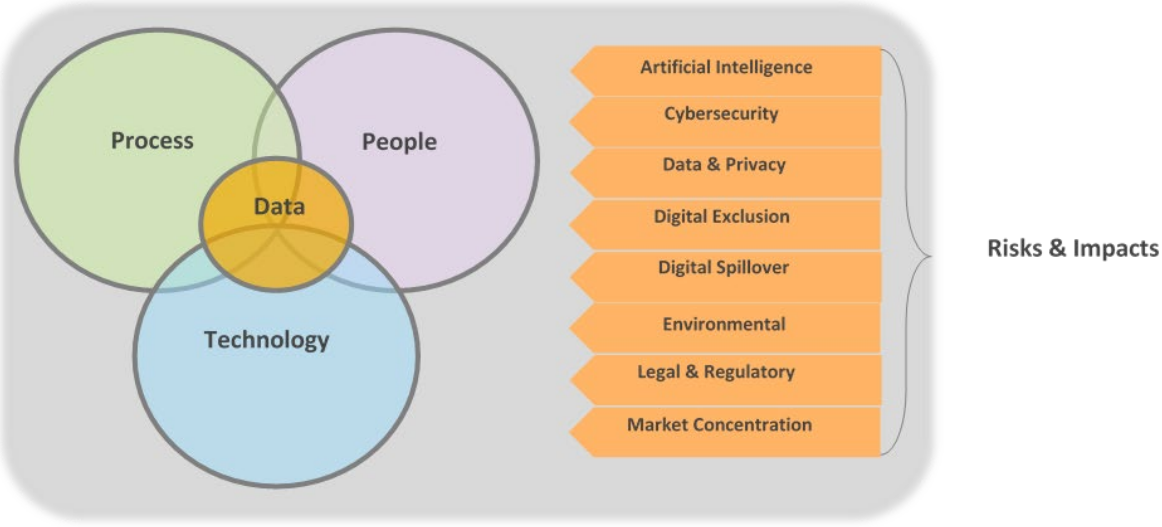
The next subsection will delve deeper into additional *operational* risks that central banks and financial supervisors might run due to fintech- and cybersecurity-related developments.

H. Digital Risks and Central Bank Information Technology

With the advancement of digitalization in the financial industry, managing digital risks, especially cybersecurity, has become a key success factor for digital transformations of central banks. In fact, emerging solutions have introduced new forms of digital risks and concerns with used technologies, new acquired processes, and skills required to develop and maintain complex fintech systems. As a result, without proper rigor and management, digital risks may result in monetary losses, data leakages, and reputational risks, as mentioned above, for central banks and may even impact financial stability of their respective countries.

However, there is more to digital risks than meets the eye. Although crucial, cybersecurity risks are not the only digital risks threatening Fund members—including their central banks—and their financial systems. In addition to (1) cybersecurity risks, digital risks and negative impacts may relate to: (2) artificial intelligence (AI), (3) data and privacy, (4) digital exclusion, (5) market concentrations, (6) digital spillover, (7) inadequate legal, regulatory (including AML/CFT) frameworks, and finally the (8) negative environmental impact technologies may create. Major differences in design, infrastructure and used technologies for each country would result in different risks and impacts and would demand a custom digital risk management and priority plan to reap the benefits of the digital transformations. Digital solutions must account for the risks and impacts across technology, processes, people, and data (see Figure 15).

Figure 15. Digital Risks to IT Systems



Source: Authors.

IT infrastructural issues often go beyond the central bank's sphere of influence. Lukonga[63] stresses that IT outages in general could create significant risks in "countries with unreliable provision of electricity and internet service. The growing trend to shift to digital modes of delivering financial services requires reliable electricity and internet. Unreliable electricity supply remains a significant problem in some countries (Egypt, Lebanon, the West Bank and Gaza, and Yemen), and this can lead to service disruptions as financial institutions rely more on Internet for service delivery."

Similarly, outsourcing could pose operational risks. This relates to reliance on third parties for a central bank's own IT infrastructure (as mentioned above), for instance in the form of private or public cloud computing (see Box 2). Additional legal risks could relate to (the lack of) clear arrangements and Service Level Agreements and the clear allocation of responsibilities to facilitate transparency and accountability. Lastly, it could include aspects of outsourcing of critical capacity and expertise on IT-related issues, such as dependency on external helpdesks, and software engineers as well. This holds for commercial institutions and central banks alike.[64] Some central banks have reportedly started setting-up private cloud services within the central bank community to decrease dependencies on third parties.

[63] Lukonga, I., 2018, *Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Region*s, IMF Working Paper 18/201. Washington, D.C.: International Monetary Fund.

[64] See, for instance, Bowman, M., 2019, *Community Banking in the Age of Innovation*, Speech by Michelle W. Bowman, Member, Board of Governors at the Federal Reserve System, at the "Fed Family" Luncheon at the Federal Reserve Bank of San Francisco, April 11, 2019. In her speech, Bowman emphasizes the need for "outsourcing risk management guidance [to] appropriately reflect the present-day business realities of the banks that we supervise."

Fintech services are introducing new technologies to central banks' infrastructure and their internal operations. In addition to the earlier provided overview of technologies, additional technologies and software such as open-source software,[65] heavy dependency on cloud computing, integration through Application Programming Interface (APIs), Artificial Intelligence/Machine Learning (AI/ML), blockchain/DLT[66] (including the concept of distributed and decentralized architecture and/or authority), Decentralized Finance (DeFi),[67] and Big data are among some of the technologies that will pose even more new risks to central banks. These services and technologies require specific operational techniques with deep technical understanding that needs to be reflected and integrated within the central bank's risk management framework. Only by such an integrated approach can the central bank manage fintech-related risks, in line with its risk appetite.

[65] Open-source software is a type of computer program and a collection of libraries that is written and released under a special license granting anyone the right to use, modify and distribute the software under pre-defined terms and conditions.

[66] Following "DLT" references in the paper are to be read as including "blockchains."

[67] DeFi is short for Decentralized Finance and is a new framework of financial services produced with no, or minimal, intermediaries and relies heavily on source-code and cryptography to enforce governance and fulfillment of agreements.

Box 2. Cloud Computing

Cloud computing can be defined as "off-premise, on-demand computing where the end-user is provided applications, computing resources, and services (including operating systems and infrastructure) by clouds service provider via the internet." *

Clouds can be classified in four distinct types, based on where the location of the cloud is hosted:

1) *Public cloud*: the physical infrastructure is located at the third party's premises. This implies that the user has no clarity regarding the location.
2) *Private cloud*: this is a cloud solution specifically designed for the user. Contrary to common belief, a private cloud does not need to be located at the user's location, but it could also be hosted externally. In either case, the infrastructure is dedicated for the specific user only, and is not shared with other organizations.
3) *Hybrid cloud*: as the name suggests, this is a mix with private components (critical, secure applications that are hosted in a private cloud) and public components (hosted in a public cloud). This is linked to the solution of "cloud bursting", which refers to an organization only using its own infrastructure for normal use, but allowing situations of excessive data use and/or storage to overflow to a public cloud.
4) Community cloud: where the cloud infrastructure is shared between two or more organizations in the same community. Some central banks are exploring the option of creating a private cloud between themselves.

Most cloud providers also offer three different models as follow:

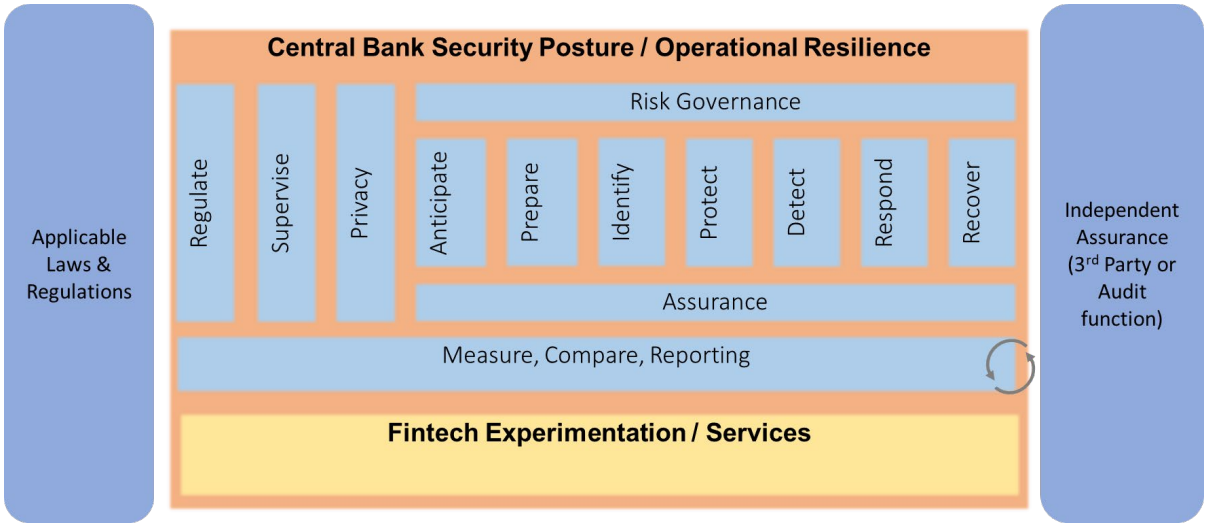
1) *Infrastructure as a service (IaaS):* the cloud provider offers their clients the computer resources such as the actual virtual servers, network devices and the storage. This service model requires more involvement of the client to manage their network and servers.
2) *Platform as a service (PaaS):* the cloud provider offers a platform for their clients to develop and host their applications. This service model requires less client involvement since the cloud provider would manage the backend virtual servers and network.
3) *Software as a service (SaaS):* the cloud provider offers the application to their clients and would manage the virtual servers and networks. This service model requires much less involvement and management from the clients since the cloud provider would manage the environment and develop and maintain the offered applications.

The major cloud providers world-wide are the so-called Big Four: AWS (Amazon), IBM, Microsoft, and Alphabet (Google), raising additional questions on the systemic nature of these providers, and whether more direct oversight would be warranted.

Source: Vikas, S., e.a., 2013, *Private Vs Public Cloud*, International Journal of Computer Science & Communication Networks, Vol. 3 (2), pp. 79–83.

* Note that "mobile cloud solutions" could, for instance in combination with CBDC solutions, also be of interest to explore further, especially as smartphone architecture is enhanced to support mobile cloud-specific applications. See, for instance, Woods, P., 2011, *Towards A Lightweight Mobile Cloud*, Master Dissertation University of Dublin. Dublin: University of Dublin.

Figure 16. Fintech and Central Bank Operational Resilience



Source: IMF staff and NIST Framework.

Cloud computing is an essential component for fintech services to flourish as it provides scalability, elasticity and has the potential to improve business continuity and reduce overall costs. In addition, cloud computing may reduce the operational risks for central banks struggling with on-premise development and maintenance of their own hardware, software, and infrastructure which comes with substantial operational burden and risk. However, leveraging and managing the cloud without careful planning and design security may complicate the central bank's infrastructure and raise ambiguity around liability, security, privacy, and legal regulations on sensitive data, that may vary according to the geographical location. Box 2 shows, by means of example, the different types of cloud computing deployment models and related liability, responsibility, and operational techniques. This is forcing the security industry to shift the security mindset from "perimeter" to "data protection" instead. Central banks should strengthen the management of external dependencies as the pool of cloud-providers and vendors expands. As noted above, this is not different from operational risk related to other forms of outsourcing, with the difference that the central bank might have even more at stage—including its critical infrastructure. Cloud computing will, therefore, also demand more involvement among central bank stakeholders in the early stages of the solution design and requirement gathering with more emphases on threat modeling and early risk management specially by establishing a clear legal arrangement with third party (including cloud) providers that defines responsibilities distinctly in order to facilitate transparency and accountability. This also includes the appropriate means for the central bank to get frequent reassurance and audit attestation of the 3rd party and cloud providers' systems, procedures, and infrastructure. Finally, central banks need to equip themselves with the appropriate business continuity plans to address data portability and continuity of the central bank's services.

Open banking leverages technologies, such as APIs, to enable micro financial services to increase market competition and overall resilience by alleviating the operational risks associated with large corporation's single-point-of-failures or the "too big to fail" risks. However, open banking may exacerbate digital risks – in particular, financial sector cybersecurity at large. This goes against the fabric of financial institutions *and* central banks alike, and decades of centralized closed systems with strong and mature enclave security. Open banking services may suffer from attacks like brute-force[68] due to exposure, unauthorized access through excessive privileges, credential stuffing[69], parameter manipulation[70] and data harvesting.[71] All these attacks may result in disclosure of sensitive (customer) data and fraudulent transactions. Rigorous assurance activities during Open banking development is needed, with stronger authentication schemes and a key role for risk management.[72] Though central banks might not necessarily be exposed to direct risks related to Open banking, it could exacerbate strategy and policy risks of the central bank, as noted earlier.

Big data[73] provides potential in many financial areas, such as real-time analysis and decision-based systems. However, Big data management, data transmission, access control, and the risk of coverage biases (due to inequality of the population representation), and data inaccuracy are challenging and may introduce digital risks to central banks if not designed, implemented, and maintained properly. For example, Big data databases can become a lucrative target for hackers given the vast amounts of data they hold. Unauthorized access may lead to large data leaks. Additionally, Big date software applications are relatively new, and some of it – until recently – lacked basic security features often required by relevant

---

[68] Brute-force, in the context of web security, is an automated and systemic attack against web applications (including APIs) where an attacker would try thousands or even millions of usernames/passwords per second in an attempt to figure the correct username and/or password.

[69] "Credential stuffing" is a cyberattack technique where an attacker uses leaked credential lists (username/passwords or keys) to gain unauthorized access into web applications and APIs using automated programs. This cyberattack takes advantage of the fact that many users reuse their usernames and passwords across multiple web services and applications.

[70] Parameter manipulation is a cyberattack technique where an attacker would manipulate the data sets for web applications in order to fraudulently reduce cost, bypass specific restrictions or accessing unauthorized information.

[71] Data harvesting is a technique where automated programs systematically visit web applications (including web sites and APIs) to extract large amount of data to be used for malicious purposes.

[72] https://www.rsa.com/en-us/blog/2018-10/prepare-for-psd2-understanding-the-opportunities-and-digital-risks.

[73] Big data is a phrase used to explain large volume of data stored in a structured and/or unstructured form. The data could relate to educational, financial, and health information and may hold sensitive information such as Personally Identifiable Information (PII) or sensitive financial and transactional data.

regulations. Lastly, the Big data industry is still struggling in general with balancing the security of metadata and high-demand data[74] with efficiency and usability.

Fintech technologies, such as cloud computing and Distributed Ledger Technologies (DLT, see further), rely heavily on **open-source software and libraries**. Open-source software can enable innovation in many areas including the financial sector. However, open-source requires a different mindset when it comes to the evaluation and maintenance of software, especially with the process of security patching (i.e., the process of continuously developing and applying updates to resolve vulnerabilities or errors in the software). The maturity level of open-source software relies on the adoption rate of the software in the industry. The more the open-source software is adopted, the more issues and vulnerabilities are likely to be fixed given the active communities.[75] Open-source projects are publicity discussed for updates and bug fixing; as a result, security vulnerabilities, with some projects, are published to public forums for verification and fix development. Detailed information of these security issues and steps of exploitation are publicly available. The time it takes to develop and publish these patches varies based on the open-source community and could pose a risk to central banks if the vulnerability is exposed and largely accessible during this period.

Distributed Ledger Technologies (DLT) are becoming an essential component for the modern Internet and fintech services. DLT provide, in some cases, a more efficient solution to, for instance, the double-spending problem[76] of digital assets. They also provide several security features, including consensus and immutability.[77] However, solutions built on top of this network layer suffer from the same software bugs and architecture flaws as other software and systems. In addition, so-called permissionless blockchain in particular suffers from unique attacks, such as the 51 percent attack.[78] Contrary to popular belief, DLT are not *secure-by-default* and still require special attention in the design and solution management—requiring significant attention from a risk management perspective. In fact, encryption key management with DLT based-systems becomes critical as they are the core means to

---

[74] https://cybersecurity.att.com/blogs/security-essentials/9-key-big-data-security-issues.

[75] https://www.zdnet.com/article/open-source-security-this-is-why-bugs-in-open-source-software-have-hit-a-record-high/.

[76] Double-spending is an issue with digital assets in general due to the easiness of copying or reproducing digital information. This would enable a malicious spender to double spend the same digital asset amount across different recipients.

[77] Immutability is a desired feature to maintain integrity within blockchain where agreed blocks are cryptographically structured to prevent malicious tampering of any committed transactions.

[78] A 51 percent attack is a public blockchain-specific attack where an adversary would seek to dominate 51 percent of the network's mining hash-rate. This may result, based on the network's implementation, in double-spending and preventing the confirmation of transactions, which would undermine the blockchain network's integrity.

authenticate users and authorize transactions. For central banks, special attention should be put into the design of any DLT system as zero-day[79] vulnerabilities may intensify the consequences and may impact the central bank's reputation. In addition, immutability of current public blockchains may be problematic to central banks if a transaction was deemed illegal and requires reversing. Researching and investigating these issues and features beforehand will enable central banks to make strategic decisions during the selection of the backend technology to meet their risk profile while being equipped with the features and capabilities that meets their requirements and policies.

Also, with the advent of digital currencies, new fraudulent schemes are emerging to launder money and financing terrorism—as can be seen with the emergence of so-called tumblers, an automated, distributed and/or decentralized mechanism to launder digital currencies. Supposedly, US$1.2 billion was laundered through the use of tumblers in 2018.[80] These schemes, or variations of them, may impact CBDC if AML/CFT techniques and best practices are not well implemented and enforced by central banks and regulatory bodies in their respective countries.

A **smart contract** is another layer added to DLT with the potential to automate financial services and functionalities. Smart contracts also led to the emergence of Decentralized Finance (DeFi), a set of financial services without traditional intermediaries. Although smart contracts may suffer from the same class of security issues as other programs, the consequences for central banks may be worse if these security issues are not fixed aggressively before deployment. Additionally, security best practices (such as defense-in-depth and compartmentalization techniques) should be addressed in the solution's early stages of implementation. Leading smart contract platforms today enforce "immutability," which prohibits any changes to the deployed source-code, a desired feature with permissionless blockchain platforms' difficult-to-fix smart contracts—which may negatively impact central banks (or even the country's financial system as a whole) if such platforms are leveraged and permitted.

AI/ML is another widely adopted technology essential for fintech advancement, with further potential to automate more sectors of the financial system (including the central bank) with efficiency. AI/ML accuracy gains and have proven in many cases to reduce cost and operational overhead. However, AI/ML poses bias risks based on the underline algorithm and the data used to train the AI/ML software. Some authors recently found that leading facial recognition AI/ML algorithms were inconsistent with gender, skin and ethnicity differences

[79] A zero-day vulnerability is a software or hardware flaw that is discovered "in the wild" and has no official fix (or patch) from the hardware or software developer/manufacturer. A zero-day vulnerability can be exploited by malicious users with a high-chance of success, as the application user is unable to fix or update the software.

[80] https://www.ccn.com/1-2-billion-in-cryptocurrency-laundered-through-bitcoin-tumblers-privacy-coins/.

which could result in biased AI/ML decisions based on its use-cases/function.[81] In addition, AI/ML could fail with adversarial (malicious and crafted input) intentional or unintentional settings.[82] This would become more complicated with the black-box problem due to the difficulty to trace back the decision process of an AI algorithm and identify the algorithm's intent—highlighting the need for enhanced transparency, including from the central bank's side when using AI/Ml algorithms.[83] Research is already focusing on AI mitigation and prevention schemes; however, this is still in the early stages and will require new and innovative security modeling of AI components.

Lastly, the separate category of **cybersecurity** risks can be exacerbated by fintech developments. Though cyber-security is distinctly different from fintech developments in general, cyber risks could increase in severity if the central bank is not adequately equipped in terms of IT infrastructure and expertise, and/or if fintech applications are developed and implemented without addressing the additional operational risks linked to those new applications. Bouveret[84] points out that fintech is "particularly exposed to cyber-attacks given [its] reliance on technology," as well as expanding "the range and numbers of entry points into the financial system, which hackers could target." Additionally, fintech could "increase third-party reliance, where firms outsource activities to a few concentrated providers." He stresses that "cyber-risk is an emerging threat for all types of financial institutions, including central banks as well as fintech firms" (see also BFA Principle X, paragraph 55). Figure 17 below demonstrates how cyber risk management can be fitted within the general risk management approach highlighted in the previous section.

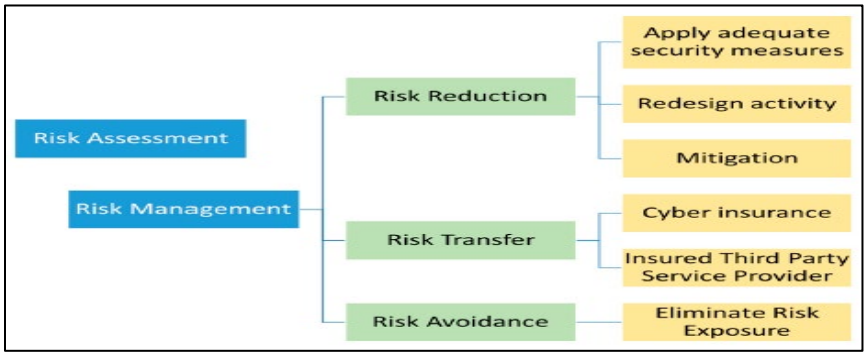
[81] https://dam-prod.media.mit.edu/x/2019/01/24/AIES-19_paper_223.pdf.

[82] https://docs.microsoft.com/en-us/security/engineering/failure-modes-in-machine-learning.

[83] https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf.

[84] Bouveret, 2018, *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*. IMF Working Paper, 18/143. Washington, D.C.: International Monetary Fund.

Figure 17. Cyber Risk Management



Source: Kopp, E., L. Kaffenberger, C. Wilson, 2017, *Cyber Risk, Market Failures, and Financial Stability*, IMF Working Paper 17/185. Washington: International Monetary Fund.

Beside the unique technological and operational risks to central banks mentioned above, more "traditional" risks still exist as well, and may in some cases even be amplified further. This includes inadequate regulatory, supervisory and compliance frameworks, privacy concerns, and cybersecurity risks to the central bank infrastructure, systems, and data. A continued improvement and agility/flexibility mindset should be adopted by central banks to discover any issues, gaps or risks early in the process of exploring the use of fintech, investigating root causes, and possible solution/mitigations, while being capable to adjust rapidly throughout the deployment process.

Fintech in general puts a lot of emphasis on central bank operational resilience[85] and its ability to adapt to the changing landscape by means of policy and regulations. This requires continuously measuring and improving the central bank's overall security posture. On the other hand, adoption of fintech services by the financial sector (and the central bank being part of the financial sector in general) would demand further research and collaboration between the central bank, other regulatory bodies, and specially technologists, to update existing financial policies and regulations to enable safe fintech adoption with minimal risks.

I. Central Bank Internal Organization

Central bank risk governance and organization, including having an operationally effective risk management unit, is a prerequisite for managing the fintech-related risks mentioned in the previous subsections. Not having an independent and dedicated risk management unit within the central bank carries the (operational) risk of not being able to assist business

[85] Cyber Resilience Review (CRR) is a framework example to conduct operational review and examine the cybersecurity controls and processes that requires improvements. The CRR is formed of 10 domains: Asset Management, Controls Management, Configuration & Change Management, Vulnerability Management, Incident Management, Service Continuity Management, Risk Management, External Dependency Management, Training and Awareness, and Situational Awareness.

departments of the central bank, as well as management, with early and proper identification, mitigation, reporting, and monitoring of fintech-related risks. This includes a clear role for the Business Continuity Management (BCM).

Many central banks are struggling with ensuring they have the right staff, with the right skills set(s) to deal with fintech developments. Lukonga[86] points out that "[s]upervisory frameworks and capacities will need aligning with the evolving financial landscape.

Central banks and financial regulators need to upgrade their expertise and internal control mechanism, including operational risk management." The European Commission, for instance, under its Horizon2020 program,[87] is facilitating technical training of central banks/supervisors in all 27 European Union members states and Switzerland on key fintech developments. Its work program includes workstreams, as well as coding sessions, on (1) credit risk in peer-to-peer lending (based on Big data analytics, to enhance loan default prediction rates), (2) market risk in robot advisory asset management (based on AI), and (3) operational risk in payments (based on blockchain, including specific case studies on fraud detection in Initial Coin Offerings, and cyber risk prioritization based on the mapping of attack techniques). The project is managed by the University of Pavia, Italy, with relevant academic institutions in each member country discussing bilaterally with supervisory and regulatory authorities how to set up training for their staff.

The country case examples of Indonesia, Luxembourg, Sierra Leone, and Ukraine provide detailed information on how the respective central banks are dealing with fintech from the perspective of their governance, risk management, and internal operations. This includes central banks that already operate a fintech regulatory sandbox and/or have advanced cybersecurity frameworks. See Appendix II.

V. CONCLUSION

With the advent of fintech, risk management of central banks themselves is increasing further in importance. Though fintech creates opportunities for central banks (/suptech applications, as well as more efficient and effective internal operations), nonfinancial risks for central banks themselves (policy and operational risks in particular) are similarly on the rise.

Policy risks extend to all key areas of central bank operations, varying from financial stability, financial integrity, financial inclusion, payment systems, and cash currency management. Though these fintech-related risks primarily affect supervised institutions, sandbox participants, and other market players, they also affect the risk exposure the central bank itself faces because of its policies (or lack thereof) for those topics and institutions.

---

[86] Lukonga, I., 2018, *Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Region*s, IMF Working Paper 18/201. Washington, D.C.: International Monetary Fund.

[87] See https://www.fintech-ho2020.eu/

Additionally, operational risks relating to the internal organization, including IT (and cyber-security), HR, BCM, could be exacerbated by the increased use of fintech tools as well.

Therefore, central bank risk management needs to form a proper line of defense for fintech-related risks. Though risks related to technology are not new at all, as some of the IMF surveillance findings show, the speed and propensity with which fintech developments are taking place in the financial sector could lead to central banks seriously lagging. Though IT departments and financial supervisors are the first "business units" within many central banks to identify fintech risks, they do so from their respective and limited viewpoints —and not with the view of protecting the central bank. Central banks therefore need to strengthen their internal risk management to include holistic, enterprise-wide assistance with identifying, mitigating, reporting on, and monitoring of fintech-related risks for the central bank. This will also benefit them as the IMF likely increases its attention for fintech-related issues in surveillance and lending operations through its Safeguards Assessments.

Risk governance and a strong risk culture are crucial. These require a strong tone at the top in the central bank. Governors and Board members need to be made aware of the fintech-related risks their organization runs, and how a risk management framework is clearly needed. This would include outreach to and training of central bank staff (not limited to supervisors and IT specialists—though the European Commission's fintech and risk management training program is a good example of how to set up unified, consistent, and focused fintech training), as well as enhancing the understanding of Board members themselves of fintech developments at a more granular level.

We advise five key recommendations for central banks to improve their internal risk management in the context of (emerging) fintech- and cybersecurity-related risks:

1) **Ensure the central bank has a dedicated, independent risk management function**: there should be sufficient risk awareness in the central bank, translated into the establishment of a risk management function that operates independently of business departments, as well as of internal audit. As a second line of defense, the risk management function will help the central bank's management and the business departments to identify fintech-related risks (whether policy or operational), and assist in mitigating of, reporting on, and monitoring of those risks. The risk management function can also integrate all transversal second line of defense risks, such as operational, compliance, data protection or IT/cyber risks. The risk management function (and, ex post, the internal audit function) would also be able to review existing central bank governance structure to determine if there is sufficient oversight of emerging fintech risks. A clearly articulated and communicated risk event escalation matrix could be helpful to ex ante articulate what type of risk events would need to be escalated within what specific time frames, and to whom. Additionally, risk management should ideally also follow up internally by identifying strategic risks in general for the central bank, for instance, by conducting a Strategic

Risk Assessment (SRA). The SRA should identify the key strategic risks, and then the outputs inform and support the strategic planning activity and the prioritization and resourcing of key activity, including programs and projects. This could be the starting point for an overall strategic planning cycle of the central bank. Nonexecutive decision-makers should take an active role in stimulating strategic planning and strategic risk management. Central bank decision-makers (executives and nonexecutives) could liaise more closely with organizations such as the IMF and the IORWG to ensure best practices in central bank risk management are incorporated, including aspects relating to Enterprise-wide Risk Management (ERM).

2) **Ensure updated fit and proper requirements, and facilitate (ongoing) training of central bank staff *and* central bank key decision-makers on relevant fintech issues**: the fast-paced fintech developments spanning a multitude of sectors, functions, and technologies imply that central bank staff are kept up to date at an even higher speed than "normal" financial sector innovation would already require. The same holds for central bank decision-makers, such as governors, executive and nonexecutive Board members. In most cases, these decision-makers will likely lack expertise in, and experience with fintech activities. Ensuring central bank decision-makers are "fit and proper" to deal with fintech in their policies, operations, and internal organization, is crucial. Having them participate in (internal or external) fintech training courses and in events organized by, for instance, the regulatory sandbox, would be helpful. For nonexecutive decision-makers in particular, exposure to fintech issues is critical for their role in central bank strategy-setting, as well as in providing oversight over the central bank's internal control system.

3) **Have clear reporting lines on fintech-issues to central bank decision-makers**: as some of the country examples indicate, central banks could have a dedicated organizational fintech unit, a more (in)formal fintech working group or committee, or other forms of internal collaboration. Regardless of the organizational setup to deal with fintech-related issues, the central bank would need to ensure that reporting on fintech-related risks is not made overly bureaucratic (for instance, by reporting lines to regular management, as well as management of a fintech unit), nor complicated (by separate reporting lines to different central bank decision-makers, and from different units on similar fintech developments). A balance needs to be found by ensuring the existing organization of the central bank can identify, mitigate, report, and monitor fintech developments and risks, but without creating information asymmetries or bottlenecks.

4) **Ensure an integrated fintech approach involving business departments *and* lines of control**: linked to the three points above, a central bank should ensure—ideally as part of its overall mid- to long-term strategic plan—that the organization approaches any (future) fintech developments in a consistent and efficient manner. This implies

an even closer cooperation between existing business departments (in particular, financial supervision), organizational departments (HR.BCM, IT and (cybersecurity), as well as the lines of control (risk management, and internal audit).

5) **Improve cyber resilience and security posture of central bank infrastructure, procedures, technologies, and skillset.** Central banks adopting fintech solutions and services should conduct a security posture assessment of their existing cyber resilience to improve their security posture. The central bank's cyber resilience is measured by the maturity of their internal processes like asset, change, configuration, risk, external dependency, and vulnerability management and could have positive or negative impacts on the central bank's risk management and fintech adoption. Conducting a cyber resilience and a security posture assessment by the central bank (preferable by an independent third-party specialist) would identify gaps that need to be addressed to be successful with the central bank's fintech adoption.

A central bank risk management function should facilitate the improved management of risks related to fintech and cybersecurity developments. In addition to the option of exploring a Strategic Risk Management Assessment, the risk management function could also try to map fintech and cybersecurity risks to specific central bank functions, as well as to the central bank's internal organization. This would involve ex ante identifying the various technologies that are most relevant to the central bank (based on input from, among others, the financial supervision department, if present, and the IT department), and the various functions/powers the central bank has according to its mandate. Through discussions with the central bank's management and the business departments, the risk management function should be able to provide a basic risk matrix that would serve as input for further discussions within the central bank. See an example listed below.

Lastly, central banks should avoid dependencies on external parties, as some of the fintech and cybersecurity examples have shown. However, given the fast-evolving nature of risks in these areas, central banks should nonetheless consider seeking external fintech and cybersecurity expertise from external experts, in pre-identified areas and within a specific timeframe. This could involve TA from the IMF or the WB, peer review input from IORWG members, bilateral feedback from other central banks, or discussions with other key international organizations, such as the BIS and its Innovation Hubs.

Figure 18. Fintech and Central Bank Risk Management—Example of a Risk Matrix

Function	MP	FS	FX RM	FMI	FI/CP	AML/ CFT	Org.
Technology							
Cloud Computing							
API/Open Banking							
Big data							
Open Source							
Smart Contracts							
AI/ML							
Internet of Things							

MP	Monetary Policy/Operations
FS	Financial Stability
FX RM	Foreign Exchange Reserve Management
FMI	Financial Market Infrastructures
FI/CP	Financial Inclusion/Consumer Protection
AML/CFT	Anti-Money Laundering/Countering Financing of Terrorism
Org.	Internal organization of the central bank

APPENDIX I. BALI FINTECH AGENDA

Principles IX and X:

IX. Ensure the Stability of Domestic Monetary and Financial Systems

Explore applications of fintech innovations to central banking services, while safeguarding financial stability, expanding if needed safety nets and ensuring effective monetary policy transmission.

Rapid fintech developments are reshaping financial markets and their structures. Fintech is progressively blurring the boundaries between intermediaries and markets, as well as between digital service providers moving into the financial space, nonbank financial companies, and banks. These developments could affect central banks' capacity to implement monetary policy and the ability of supervisory agencies to safeguard financial stability, raising both challenges and opportunities.

The potential impact of fintech on monetary transmission and the effectiveness of policy needs further consideration. In many countries, monetary policy is transmitted by changing the marginal price of liquidity—central bank reserves—available to large commercial banks, which in turn is transmitted to lending and deposits rates, as well as inducing a repricing of bonds, the exchange rate, and other assets. Fintech innovations can change any segment of this transmission. The balance-sheet channel could be affected by how households and firms react to new financial products or delivery methods, while the bank-lending channel could be reshaped by changes in the composition of bank financing. Fintech may alter the risk-taking behavior of both bank and nonbank intermediaries with implication for monetary transmission. Fintech could also affect the role of banks in payments and could thus affect their need for central bank liquidity. Policymakers will need to think through the impact of specific fintech innovations, and—if necessary—adapt operational frameworks of monetary policy to ensure effective transmission.

Fintech offers central banks the opportunity to explore new services, while having to consider new risks:

a) Some central banks are considering the possibility of issuing CBDCs, reflecting such issues as the rapid decline of cash use in their systems, maintaining demand for central bank money, reducing the cost of maintaining printed cash, and improving financial inclusion by reducing transaction costs. The design of CBDCs by central banks could have implications for the sources of commercial bank funding in the future—an issue that would call for careful examination.

b) Some central banks are exploring new fintech applications to improve and expand access to payments systems. Applications, such as DLT, are being examined closely to ascertain their capacity to increase the efficiency and resilience of payments systems.

c) Safeguarding financial stability could increasingly become a challenge. Fintech could impact the nature of systemic risks. For example, fintech-enabled multiple payment systems could improve the resilience of payments flows and reduce counterparty risk but could also become conduits amplifying risks at times of stress. Similarly, the determination of what constitutes a systemically important entity, from a stability perspective, may need to be expanded not only to a wider set of nonbank financial institutions but also, possibly, to entities providing critical fintech infrastructure.

d) Central bank support and the role of the LOLR in times of crisis might need to be re-examined. Fintech activities could lead to a decentralization and shift of activities outside the perimeter of the traditional banking sector. Although such shifts are not a new phenomenon, the speed and intensity with which these developments take place raise issues for central banks, financial supervisors, and other agencies to consider—including any potential need for adjustments to their legislative and regulatory frameworks may be needed.

e) Implications for other financial safety net arrangements might need to be considered as well. This could include analysis of the nature of "deposit" insurance, as well as its scope and coverage, and issues relating to crisis management and resolution of systemic fintech firms.

Principle X. Develop Robust Financial and Data Infrastructure to Sustain Fintech Benefits

Develop robust digital infrastructure that is resilient to disruption and that supports trust and confidence in the financial system by protecting the integrity of data and financial services.

Robust financial and data infrastructure is necessary to provide operational resilience and to preserve confidence. Strong standards of operational resilience help market participants and infrastructures to withstand and rapidly recover from disruptions, thus supporting confidence in the continuity of services and preserving the "safety and soundness" and the integrity of the financial system.

Fintech innovation increases IT dependencies and operational risks that should be carefully managed. Effective governance structures and risk-management processes are important to identify and manage risks associated with the use of fintech. The greater reliance on such technologies leads to new operational risks and more interdependencies among service providers (financial institutions, technology providers, and others) that may threaten the operational resilience of financial and data infrastructures. Financial institutions are increasingly partnering with or providers. In such cases, the associated risks for those operations and delivery of the financial services remain with incumbents. As many third-party providers fall outside the regulatory perimeter, increased emphasis on managing

operational risks and ensuring robust outsourcing arrangements is key to preserving financial stability.

Economies of scale may increase concentration risks. Economies of scale may motivate greater consolidation among financial firms or third-party service providers, increasing interconnectedness, and accentuating the potential for concentration and network risk. The provision of key infrastructure services by one or a few dominant players raises risks (both domestic and cross-border) that would need to be carefully managed and addressed by information-sharing, cooperation, and macroprudential policies as needed.

Cybersecurity is paramount. Cybersecurity is a vital element of overall operational resilience, recognizing that financial services infrastructures are only as strong as the weakest link. Increased digitalization of finance encouraged by financial innovation places even more pressure on the importance of strong cybersecurity. It is thus important that cybersecurity be fully integrated into the development of new processes from the start. Robust standards are needed to achieve a minimum level of cyber resilience across the entire financial services supply chain to maintain the safety and soundness of the financial system and integrity of data.

Robust business continuity and recovery plans are essential. A key component of strong resilience is the ability to withstand and rapidly recover from operational disruption. This necessitates robust back-up systems, incident response plans, and arrangements that are regularly tested with realistic failure scenarios.

The increased digitalization of finance increases the need for strong frameworks to protect individual and institutional data. As more entities gain access to large volumes of personal and proprietary data, efforts to gain improper access to this information will increase. Robust data governance frameworks are essential to sustain the trust and confidence of users and to deliver the benefits of fintech. Important components of such frameworks include: (1) clarity of data ownership; (2) safeguards to protect data confidentiality, availability and integrity, while encouraging appropriate regulatory information sharing; (3) privacy considerations; and (4) the ethical use of data. Processes will be needed to ensure that data controllers and processors implement effective data protection mechanisms and retain accountability for data breaches.

The following steps may be helpful for authorities to strengthen operational resilience:

a) Encourage financial firms and technology providers to embed cybersecurity and operational risk management into an enterprise-wide risk-management framework and to promote technical standards on cyber and information security. Build upon industry standards issued by SSBs [Standard-Setting Bodies] to set expectations for operational risk management and governance that include monitoring of compliance with applicable regulatory requirements when introducing new products.

b) Promote robust outsourcing arrangements that address technology dependence and apply strong disaster-recovery and business-continuity principles and standards for digital infrastructure. Market players should have robust processes for due diligence, risk management, and monitoring of any operation outsourced to a third party. Contracts should outline the responsibilities of each party, agreed service levels, and audit rights.

c) Monitor and manage domestic and cross-border concentration risk, because economies of scale could lead to large financial or technology firms becoming increasingly important in the provision of key infrastructure services, thus increasing vulnerability to systemic disruption.

d) Ensure that robust data-governance frameworks are in place to address issues of data ownership, privacy, confidentiality, integrity, availability, and the ethical use of data. Priorities are the protection of consumer and institutional data and the integrity of the financial services industry infrastructure.

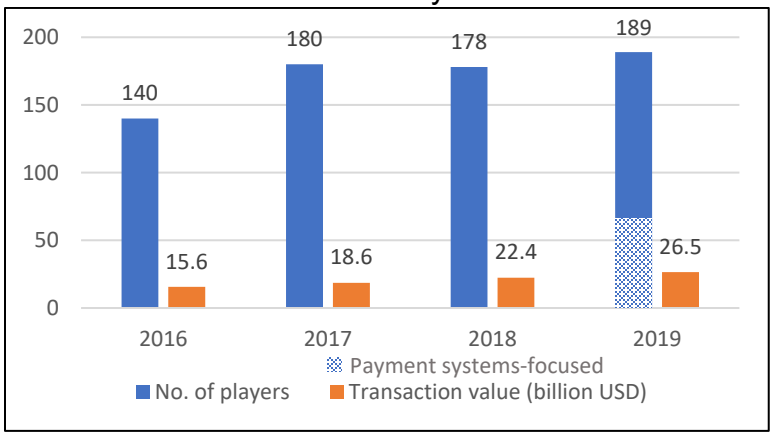
e) Additional capacity and specialized skills may be needed to supervise operational and cybersecurity risks.

APPENDIX II. CASE EXAMPLES[1]

A. Indonesia

Fintech in Indonesia has been growing. The fintech industry in Indonesia has shown an upward trend during the last several years, dominated by peer-to-peer (P2P) lending, and followed by payment system service. The transaction value grew by 18.3 percent from US$22.4 billion in 2018, to a predicted value of US$26.5 billion in 2019—most of which (95.67 percent) comes from digital payments.[2] According to the Indonesia Fintech Association (Aftech), the number of fintech players in Indonesia grew rapidly from 140 players by 2016, to 189 players by February 2019. Among those players, 34 percent focused on payment systems. See Figure 1 below.

Figure 1. Fintech in Indonesia/Players and Transaction Value



Source: Bank Indonesia.

Fintech is seen through the lens of the central bank's objective of payment system stability. For Bank Indonesia (BI), the country's central bank, these developments warranted the need for active involvement with fintech in Indonesia. The BI has a mandate to regulate and maintain the stability of payment system and to achieve an efficient, safe, and reliable payment system by considering the expansion of financial access and consumer protection. As such, BI has five main roles: regulator, licenser, operator, facilitator, and supervisor of the payment system.

[1] This section is based on input provided by the respective central banks. Note that the examples are not illustrative for developments in all central banks, but only serve as illustrations for the approaches of the specific countries/central banks. The three examples were included due to the pro-active approach of these central banks in sharing their fintech-related risk management experiences in the central banking community and with the IMF.

[2] https://www.statista.com/outlook/295/120/fintech/indonesia

Additionally, fintech is seen as potentially influencing financial stability as well. The fintech business in Indonesia is classified into five categories: (i) lending and capital raising, (ii) market support, (iii) payment, clearing, and settlement, (iv) investment and risk management, and (v) insurance. As such, BI works closely with the Indonesian financial supervisor (Otoritas Jasa Keuangan, OJK). This allows BI to strike the right balance in creating policies that simultaneously nurture digital innovation, while also preserving financial stability and integrity.

In organizational terms, BI established a function under the Payment System Department to facilitate its work in the fintech area. It has nine full time employees with a varied set of experiences, expertise, and backgrounds, ranging from economist, accountant, mathematician, to legal, and IT experts—this is a reflection of the complexity of "fintech" and the topics generally included under its header.

Additionally, the regulatory sandbox is a controlled environment for innovative products. It provides a safe and secure environment for experimenting with fintech products, services, technology, or business models that are created to nurture innovation—while also safeguarding consumer protection, risk management, and prudential principles. The duration of participation in the sandbox is limited to six months, though extension for another six months is possible. Requirements for participation include registration at BI, payment systems-related business, innovative products, benefits to customer, non-exclusive and scalable businesses, with risks identified and mitigated.

BI has set up a regulatory sandbox's expert panel, comprising experts from the regulation, licensing, information technology, risk management, law, and supervision units. This expert panel has the responsibility to assess risks of potential fintech participants in the regulatory sandbox. To control fintech-related risks, BI requires all fintech payment systems to be registered at BI, and it limits collaboration by licensed providers with unregistered fintech companies. BI also requires all fintech companies to comply with Indonesia's AML/CFT Act and relevant regulations and requires fintech companies to report any suspicious transactions. As crypto-currencies are not legal tender in Indonesia, payment service providers (including fintech companies) are currently prohibited to process transactions using crypto-currencies.

B. Luxembourg

The Central Bank of Luxembourg (BCL) closely follows and carefully analyzes fintech developments, though it does not have a separate fintech unit. Fintech developments that affect the central bank are dealt with in various departments depending on their respective areas of expertise. This most notably includes market infrastructure and payment systems and oversight, financial stability, economics and research, market operations, as well as in the BCL's own operational risk management and IT. The BCL Governor recently tasked a staff member of the BCL's European and Internal Coordination Unit to actively follow fintech developments and to ensure effective coordination throughout the bank. Similarly, an internal working group on Blockchain/DLT provides a forum to discuss fintech-related developments

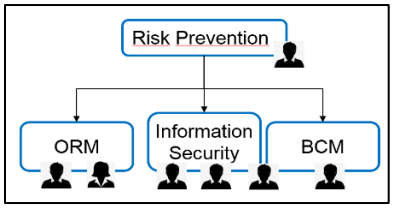
across departments. It should be noted that prudential supervision of fintech service providers is undertaken by Luxembourg's financial supervisor, which is a separate entity.

From a payments system perspective, the BCL monitors fintech developments at the European level. The BCL's Market Infrastructure and Payment Systems Unit follows fintech—and DLT in particular—at the level of Eurosystem committees and work groups. It examines function, operational reliability, and legal setup vis-à-vis the users (what rights do users have). A similar approach is followed at local level vis-à-vis the analyzed initiatives. In this context, cybersecurity, auditability and traceability, and IT management are evoked but without competence and capacity from this unit to adequately assess the responses.

The BCL's current approach to fintech is to rely on decentralized expertise throughout the organization. For the BCL, the objective of this approach is to rely on the expertise of each unit in their area of competence, while adding an additional coordination layer to ensure an efficient communication and information flow, as well as a comprehensive view and understanding of the diverse fintech developments, their interlinkages, and impact.

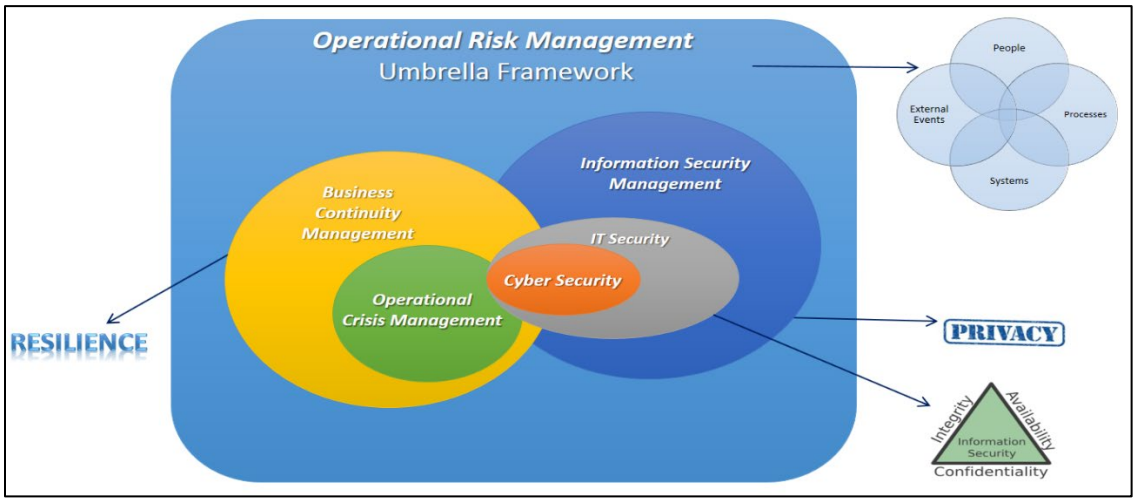
BCL's internal risk management function consists of the Risk Prevention Unit, which deals with ORM including BCM, information security (cybersecurity) and compliance. See Figure 2 below. As the BCL's second line of defense, the Risk Prevention Unit needs to have the necessary skillset to embrace and assess more technical disciplines such as IT, information security, as well as emerging and potentially disruptive technologies. Figure 3 provides an overview of the BCL's operational risk management umbrella framework.

Figure 2. BCL Risk Prevention Approach



Source: Central Bank of Luxembourg

Figure 3. The BCL Operational Risk Management Umbrella Framework



Source: Central Bank of Luxembourg

The Risk Prevention Unit is involved in analyzing potential (future) fintech-related risks to the central bank as well. At this stage, the BCL does not yet use fintech for its own benefit, and technology such as DLT and AI/ML is not used in supervisory tasks, nor does the central bank use cloud services. Nonetheless, these technologies are analyzed by the BCL's internal Risk Prevention Unit. The Risk Prevention Unit is also actively involved in the assessment of cyber-risks to the BCL. Additionally, new technologies are discussed in various Eurosystem groups as well, before use cases are further developed. The BCL also participates in the OECD Financial Markets Group, and its newly set up Expert Group on Finance and Digitization.

From a risk management perspective, the BCL sees possible disruptive consequences of fintech. The Risk Prevention Unit assesses risks related to disruptive technologies, in particular those associated with Luxembourg's startup ecosystem, such as cloud computing and mobile computing. The BCL is currently considering more officially defining its risk appetite for different risk domains like cyber risks, fraud risk, third-party risks, or technology risk—including fintech.

The BCL sees the necessity to address technology risk given rapid changes and strong interconnectedness. It defines technology risk as "any potential for technology failures or incidents to disrupt the business, such as breaches of agreed service availability, loss of data integrity or data corruption, architectural risk that exposes significant single points of failure, or an inability to recover technology enablers supporting critical processes. It is the risk of the inability to operate critical processes within a reasonable timeframe due to technology failures." The BCL covers some explicit fintech elements such as cloud computing, cybersecurity, and mobile computing. As evolution of technology is advancing rapidly and will further accelerate, the rate of change associated through the interconnectedness, mobility

and complexity in the future, the BCL feels it must respond quickly by reshaping and improving its current operational risk management practices and technical means.

Practical examples include implementing a Governance, Risk, and Compliance (GRC) solution. The Risk Prevention Section is currently implementing a GRC software solution for fostering the operational risk management process at the central bank. The third phase of the project would incorporate elements such as cyber or IT incidents feeding directly the GRC solution. The BCL considers this as a viable option, given the presence of the necessary technical background and skillset is at the second line of defense level. The Risk Prevention Section collaborates with the BCL's operational security to implement security assessment tools that could feed into the GRC tool in the future.

BCL risk management will be able to improve operational resilience in the context of fintech. Given that risk management is a second line of defense, BCL's risk management will be able to translate technical incidents, weaknesses, and risks into business terms and risks for the central bank. Expanding risk management to cover fintech-related developments will allow the BCL to respond more quickly to technical weaknesses at the business level, and thereby guarantee higher operational resilience of the central bank.

In the (near) future, the BCL expects the following developments to allow fintech to contribute to internal risk management of the central bank:

1) Improved automation and computerization of the ORM process by implementing an advanced software GRC solution;

2) In the BCL Management Team: interfacing the GRC tool with IT technical solutions;

3) Improved translation of cyber and technical risks into business terms and risks – which would result in quicker response times, and higher operational resilience;

4) Better targeted and increasingly empowered risk assessments of operational risks, including cyber and technical risks by the second line of defense;

5) Significant improvements in the accuracy, efficiency, and security of processes across payments, clearing, and settlement;

6) Additionally, contributing to identifying the best options for mitigating risks and the respective strategies;

7) Real-time information on all types of risk;

8) Mitigation of the effects of cyber-attacks (internal or external), by continuous monitoring of the data environment; and

9) Continuous monitoring and auditing of processes and systems that are vulnerable to threats. The process should include alerting, responding, and eradicating threats.

Additionally, the BCL is studying the following topics for possible future application, if deemed appropriate:

1) Improvement of fraud detection by measuring and monitoring anomalies and abnormal activities (internal and external fraud, cyber-attacks; possible applications in the context of SWIFT payment messages to avoid cases like Bangladesh Bank by means of scanning all transactions, false payments, false invoices, etc.);

2) Data mining, including the application of statistical and artificial intelligence tools for data-analytics, allowing assessment of risk of internal fraud, management fraud, occupational fraud, and to support fraud audits;

3) Detection front office behaviors, and observe emerging behavioral patterns to predict latent risks, and detect links between employees;

4) Detection of money laundering by analyzing large datasets;

5) Control of operational risks by using effective Workflow Management;

6) Analyzing the best ways to protect systems through AI/ML analysis;

7) Process-automation to accelerate the pace of routine tasks, minimize human error, and make processes in general more efficient and more secure;

8) Setting-up of early-warning systems by defining Key Risk Indicators, Key Performance Indicators, Key Control Indicators enriched by appropriate models for detecting abnormal behavior and constructing legitimate events;

9) Identifying patterns, by using tools in complex data structures involving non-linear relationships in particular;

10) Applying simulation models for the analysis of more complex problems;

11) Modelling complex phenomena based on experts' perceptions by modeling uncertainty and related events and enable the development and forecasting exercises through simulations;

12) Automation of the classification of risk events;

13) Automation of taxonomies and risk libraries by standardization, centralization, and elimination of redundancies;

14) Allowing for automatic links between historic incidents with the corresponding risk event(s) to prevent similar risks in the futures; and

15) Combining loss data with risk reports to ensure improved prediction of risk events, and therefore a more accurate prediction of future losses.

In terms of challenges, the BCL has identified the following key issues to be tackled:

1) The availability of suitable data;

2) Data held in separate silos, different systems;

3) Data kept as informal knowledge; and

4) Transparency and ethics (regulatory compliance).

C. Sierra Leone

The Bank of Sierra Leone (BSL), which is Sierra Leone's central bank, actively manages the country's regulatory sandbox. The BSL's Regulatory Sandbox Program was set up to enable innovative fintech products, services, and solutions to be deployed and tested in a live environment, within specified parameters and timeframes prior to launch into the market. The sandbox helps facilitate the BSL's understanding of emerging fintech issues and supports evidence-based approaches that advance the goals of financial inclusion and maintaining financial stability. The mandate of the sandbox is derived from the Sierra Leonean Banking Act (2011) and from the Other Financial Services Act (2001). These give the BSL the authority to issue regulations and guidelines. The BSL Regulatory Sandbox (the "Sandbox") framework stipulates eligibility criteria, licenses, and regulatory requirements for the participation in the Sandbox. Participants must be tested and licensed or rejected licensing within the testing period.

The Sandbox involves numerous organizational elements within the central bank. Within the BSL, the Sandbox is managed by a Sandbox Steering Committee consisting of representatives from the following departments: Banking Supervision, Other Financial Institutions Supervision, Financial Stability, Legal Affairs Division, and Financial Inclusion Unit. The Sandbox Steering Committee provides policy direction and oversight of the Sandbox Program, including recommendations to the governor on granting or rejecting licensing of projects accepted in the sandbox. The Sandbox Steering Committee is supported by a project implementation team called the Sandbox Team, which consists of experts from Banking Supervision, Financial Stability, and Other Financial Institutions Supervision Departments. The BSL's risk management unit is currently not a member of the Committee or the Team. The Sandbox Team is housed in the Other Financial Institutions Supervision Department, but all its internal and external correspondences are channeled through the Chairman of the BSL Regulatory Sandbox Committee (Director of Other Financial Institutions Supervision Department of the BSL), who reports to management and governor

of the BSL on regular basis. As need arises, the Sandbox Team may invite experts from other departments within the BSL, including the BSL's risk management unit, as well as from outside the BSL.

From a risk management perspective, the BSL has identified key risks to the central bank and the financial sector. As the Sandbox operates in a live environment (i.e., involving actual customers using the product(s)), test failures may result in financial loss or other risks to participants, their customers, and the financial system—including the BSL. As such, the Sandbox incorporates appropriate safeguards, including:

- Issuance of licences for a period of twelve months to identify and manage potential risks and contain the consequences of failure;
- Conducting a thorough "Fit and Proper Persons" assessment on all would-be Board Members and top management staff to ascertain their integrity, sources of funds and suitability to manage fintechs within the Sandbox;
- Requesting participants to sign a written agreement with their service providers and a disclosure to their customers that the solutions offered to them is under testing in the Sandbox; and
- Requiring Sandbox participants to get the consent of customers before they would use their personal data in order to protect consumer's privacy.

A so-called monitoring tracker and testing plan is used to assess the risks and measures put in place to mitigate risks and the impact to customers that may arise from:

- Any test failures;
- Fintech developments;
- Regulatory requirements to be relaxed or modified;
- Testing methodology;
- Control boundaries; key metrics and outcome indications; and
- Data security requirements, KYC processes and AML/CFT safeguards.

D. Ukraine[3]

[3] This section is in part based on the research paper written by Roman Hartinger (e.a.), Head, Division for Innovative Projects (Payment Systems and Innovative Development Department) of the National Bank of Ukraine.

The National Bank of Ukraine implemented a pilot project on retail CBDC issuance called E-hryvnia during 2018.

As a part of this project, the NBU analyzed international experience on CBDCs, studied related legal issues and macroeconomic effects, and drew up optimum versions of business models for e-hryvnia circulation.

Along with theoretical studies, the NBU project also conducted case studies. While testing a blockchain technology platform, the NBU issued a limited amount of e-hryvnias into circulation. Transactions involving e-hryvnias could be initiated via either web-wallets or mobile apps for Android and iOS. Transactions were tested by task forces consisting of NBU staff, volunteer companies, and World Bank experts, which provided advice to the NBU as technical assistance[4].

BACKGROUND:

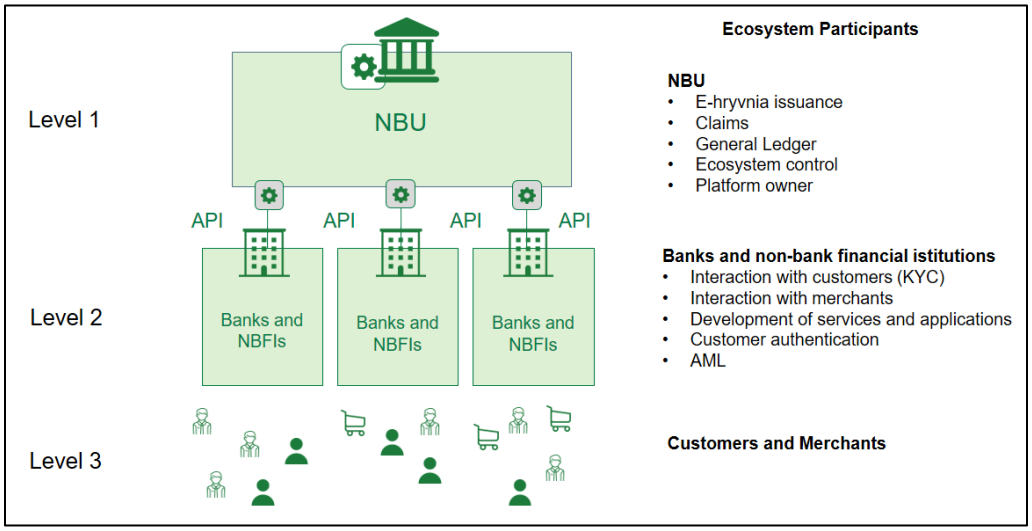
Financial inclusion is one of the seven strategic objectives set in the National Bank of Ukraine's (NBU) Strategy.
According to the World Bank's estimations, 37 percent of adults in Ukraine do not have a bank account and are therefore not involved in the financial system.
It is an important objective for the Ukrainian payment market and the financial inclusion agenda to introduce an affordable, cheap, secure, and functional instrument for retail payments by individuals.

Thereby, research and development activities on CBDC were committed in the Strategy of Ukrainian Financial Sector Development until 2025..

Within the project framework, the NBU team was considering the launch of e-hryvnia in the Ukrainian payment market under one of two alternative models of issuance: centralized or decentralized.
The centralized model (Figure 4) implies that the NBU is the only issuer of e-hryvnia and the only owner and operator of the blockchain platform. E-hryvnia is the direct claim on the NBU. Banks and non-bank financial institutions are agents that conduct e-hryvnia distribution, provide users with access to the platform via internet resources, and offer customers additional services, such as secure key storage, mobile applications, and user-friendly presentation of information on customer transactions, etc.

[4] The results of the pilot project are published in the pilot project research note https://bank.gov.ua/news/all/e-hryvnia.

Figure 4. NBU e-hryvnia Centralized Model

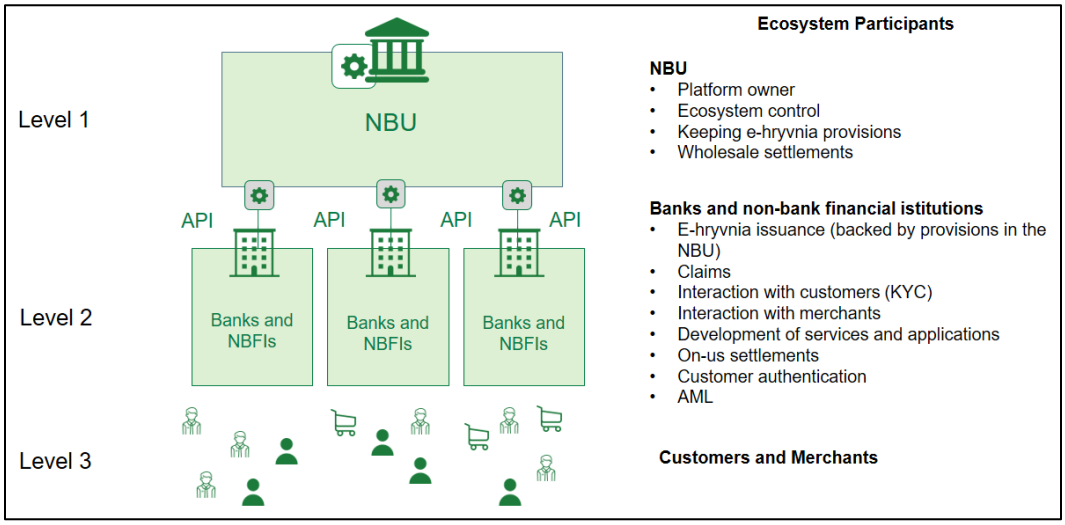


Source: National Bank of Ukraine.

The decentralized model (Figure 5) assumes that banks and non-bank financial institutions are entitled to issue e-hryvnia, backed by provisions in the NBU. E-hryvnia is the claim on these banks and non-bank financial institutions, which operate all retail payments. This model is similar to what the IMF defines as synthetic CBDC.[5]

For the purposes of the pilot project, the centralized model of e-hryvnia issuance was chosen as a simpler, more comprehensible, and transparent model.

Figure 5. NBU e-hryvnia Decentralized Model



Source: National Bank of Ukraine.

[5] IMF, 2019, *The Rise of Digital Money*. IMF FinTech Note No. 19/01. Washington, D.C.: International Monetary Fund.

Two working groups were established to implement the pilot project, namely:

1) **Internal working group**, consisting of the NBU's structural units: Payment Systems and Innovations Department (project leader), Strategy and Reforming Department, Information Technologies Department, Security Department, Accounting Department, Operational Department, Legal Department, Monetary Policy and Economic Analysis Department. The project manager and the project team reported to the Change Management Committee of the NBU on a regular basis.

2) **External initiative group**, consisting of the Ukrainian IT and payment markets' participants who volunteered to take part (they developed the blockchain technology platform and performed service (agent) functions in the pilot project).

The pilot project allowed the project team to identify the following risks and ways to minimize them:

1. The implementation of e-hryvnia may be disruptive for the Ukrainian payment ecosystem. E-hryvnia has the potential to become a competitor to existing retail payment instruments and means of payment, such payment cards, electronic money, payment orders. As a result, it may change the ecosystem of Ukraine's payment market and reassign the current roles of market participants instead of replacing cash and including more population into financial system.

2. Considering that the pilot project had a limited list of transaction types and a limited range of users, as well as the minor quantity and volumes of executed transactions, the project did not fully uncover the instrument's attractiveness and the potential level of involvement of Ukraine's population in using it. Thus, it is hard to predict the number of Ukrainian citizens to become e-hryvnia users if the decision to implement e-hryvnia at a national scale is taken.

3. In case of the centralized model, the NBU would perform non-specific functions for a central bank such as interacting with individuals (including KYC, disputes resolution, AML/CFT).

4. Implementation of e-hryvnia in Ukraine's payment market should be in line with the possible implementation of other innovative payment instruments, including instant payments and new Open Banking instruments to avoid the overlapping of these projects.

5. There is legal uncertainty for the implementation of e-hryvnia as it should be regulated by law. As the full-scale implementation of e-hryvnia in the Ukrainian payment market would require amendments to both Ukrainian legislation and NBU regulations, the pilot project was hold in the framework of the electronic money regulation.

6. Significant investments and time are required to modernize the payment infrastructure for a new instrument like retail CBDC, that may be unjustified as Ukrainian payment

services market is characterized by high level of competition, concentration, and established infrastructure.

7. Risk of the proper technology choice: distributed leger technology (DLT, blockchain) can be used as a platform for the issuance and circulation of e-hryvnia. However, the main advantages of this technology, namely: the lack of a single trust center and the possibility of checking any transaction by any person are not used in case of the centralized model of e-hryvnia. Also, for the national level system, private version of the blockchain protocol cannot be used since its updating in accordance with the development of the basic protocol is virtually impossible.

The NBU is currently considering the possibility of issuing e-hryvnia not just from the supply side but also through market demand analysis. At present, the Project Team is focused on exploring the possible areas of usage and potential demand for e-hryvnia. The NBU is considering the following use cases for e-hryvnia:

1) Instrument for retail cashless payments by individuals (P2P, P2B);

2) Instrument for social welfare payments (G2P);

3) Instrument for securities settlements (B2B);

4) Instrument for wholesale (interbank) settlements inside the country (B2B);

5) Instrument for cross-border settlements (cooperation with other central banks) (B2B, P2P, P2B); and

6) Interest bearing instrument (not as means of payment).

In December 2020, the NBU initiated a Survey on Potential Demand and Consumer Motivations in a form of a questionnaire. The questionnaire includes 30 questions from the perspective of the above-mentioned use-cases and addressed to six target groups of Ukrainian experts: Retail Business and Innovations/Corporate Business/Financial Markets/Digital Transformation of Public Authorities/Virtual Assets.

In 2020, the NBU presented the Draft Law of Ukraine on Payment Services intended to regulate the operation of the Ukrainian payments and transfer market. Among others, the draft law contains the definition of CBDC, as well as changes to the existing Law of Ukraine on the National Bank of Ukraine in the part of the NBU's function to issue digital currency. Currently, the draft law is being revised by the Parliament and voting is expected in 2021.

The NBU continues to research the possibility of issuing its digital currency, taking into account the results of the pilot project, the current needs and motivations of the financial market, and the ongoing economic development prospects.

REFERENCES

Bazarbash, M., 2019, *FinTech in Financial Inclusion – Machine Learning Applications in Assessing Credit Risk*. IMF Working Paper 19/109. Washington, D.C.: International Monetary Fund.

Berkmen, P., K. Beaton, e.a., 2019, *Fintech in Latin America and the Caribbean: Stocktaking*. IMF Working Paper 19/71. Washington, D.C.: International Monetary Fund.

BIS, 2009, *Issues in the Governance of Central Banks – A Report from the Central Bank Governance Group*. Basel: Bank for International Settlements.

BIS, 2012, *Principles for Financial Markets Infrastructures*. Basel: Bank for International Settlement.

Bouveret, 2018, *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*. IMF Working Paper, 18/143. Washington, D.C.: International Monetary Fund.

Bowman, M., 2019, *Community Banking in the Age of Innovation*, Speech by Michelle W. Bowman, Member, Board of Governors at the Federal Reserve System, at the "Fed Family" Luncheon at the Federal Reserve Bank of San Francisco, April 11, 2019

Chamoun, E., R. van Greuning, 2018, *Effectiveness of Internal Audit and Oversight at Central Banks: Safeguards Findings – Trends and Observations*. IMF Working Paper 18/125. Washington, D.C.: International Monetary Fund.

Das, S., 2019, *Opportunities and Challenges of FinTech*, Speech by the Governor of the Reserve Bank of India, NITI Aayog's FinTech Conclave, March 25, 2019.

FATF, 2012, *International Standards On Combating Money Laundering And The Financing Of Terrorism and Proliferation - The FATF Recommendations*. Paris: FATF (recommendation 29).

FSI, 2018, *Innovative Technology in Financial Supervision (Suptech) – The Experience of Early Users*. FSI Insights on Policy Implementation, No. 9. Basel: Financial Stability Institute.

IMF, 2013, *Guidelines on FX Reserve Management*. Washington, D.C.: International Monetary Fund.

IMF, 2017, *Fintech and Financial Services: Initial Considerations*. IMF Staff Discussion Note 17/05. Washington, D.C.: International Monetary Fund.

IMF, 2018, *Asia at the Forefront: Growth Challenges for the Next Decade and Beyond*. IMF Regional Economic Outlook Asia and Pacific, October 2018. Washington, D.C.: International Monetary Fund.

IMF, 2018, *Casting Light on Central Bank Digital Currency*, Staff Discussion Note 18/08. Washington, D.C.: International Monetary Fund.

IMF, 2019, *Fintech: The Experience So Far*. IMF Policy Paper, June 2019. Washington, D.C.: International Monetary Fund.

IMF, 2019, *Review of the Fund's Strategy on Anti-Money Laundering and Combating the Financing of Terrorism*. IMF Policy Paper, February 2019. Washington, D.C.: International Monetary Fund.

IMF, 2019, *Staff Proposal to Update the Monetary and Financial Policies Transparency Code*, May 2019. Washington, D.C.: International Monetary Fund.

IMF, 2019, *Switzerland Financial Sector Assessment Program*. IMF Country Report No. 19/183, June 2019. Washington, D.C.: International Monetary Fund.

IMF/WB, 2004, *Financial Intelligence Units: An Overview*. Washington, D.C.: International Monetary Fund.

IMF/WB, 2018, *The Bali Fintech Agenda*. IMF Policy Paper. Washington, D.C.: International Monetary Fund.

ISO 31000, http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170

Kearns, A., *The organisation of risk management in central banks*, in Sullivan, K., M. Horáková (eds.), *Financial Independence and Accountability for Central Banks*, 2014. London: Central Banking Publications.

Khan, A., 2016, *Central Bank Governance and the Role of Nonfinancial Risk Management*, IMF Working Paper 16/34. Washington: International Monetary Fund.

Khan, A., 2017, *Central Bank Legal Frameworks in the Aftermath of the Global Financial Crisis*, IMF Working Paper 17/101. Washington: International Monetary Fund.

Kopp, E., L. Kaffenberger, C. Wilson, 2017, *Cyber Risk, Market Failures, and Financial Stability*, IMF Working Paper 17/185. Washington, D.C.: International Monetary Fund

Lukonga, I., 2018, *Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions*, IMF Working Paper 18/201. Washington, D.C.: International Monetary Fund.

PWC, 2016, *Beyond Automated Advice - How FinTech is Shaping Asset & Wealth Management*. PWC Global FinTech Survey 2016.

RBI, 2018, *Reserve Bank of India releases Dissent Note on Inter-Ministerial Committee for finalization of Amendments to PSS Act*, RBI Press Release, October 19, 2018.

RBI, 2019, *Opportunities and Challenges of FinTech*, Speech by Governor Das, March 25, 2018, at the NITI Aayyog's FinTech Conclave.

RBI, 2021, *Booklet on Payment Systems* (January 25, 2021). Mumbai: Reserve Bank of India; accessible via: https://m.rbi.org.in/scripts/PublicationsView.aspx?Id=20315#AP3.

Shabsigh, G., T. Khiaonarong, e.a., 2020, *Distributed Ledger Technology Experiments in Payments and Settlements*, IMF Fintech Note. Washington, D.C.: International Monetary Fund.

Vikas, S., e.a., 2013, *Private Vs Public Cloud*, International Journal of Computer Science & Communication Networks, Vol. 3 (2), pp. 79-83.

Woods, P., 2011, *Towards A Lightweight Mobile Cloud*, Master Dissertation University of Dublin. Dublin: University of Dublin.

Zhang, L, S. Chen, 2019, *China's Digital Economy: Opportunities and Risks*. IMF Working Paper, 19/16. Washington, D.C.: International Monetary Fund.