FINANCE, COMPETITIVENESS & INNOVATION INSIGHT

Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit and Deposits

WORLD BANK GROUP

1818 H Street NW
Washington, DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

Photo Credits: Shutterstock.com

TABLE OF CONTENTS

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

This report has been prepared by Charles Taylor (consultant), Aquiles Almansi and Aurora Ferrari (World Bank). The authors gratefully acknowledge inputs and suggestions received from Alfonso Garcia Mora, Harish Natarajan, Matei Dohotaru, Yira Mascaro, Pierre Laurent Chatain, Erik Feyen, Matthew Saal, Mahesh Uttamchandani, Marco Nicoli, Holti Banka, Katia d'Hulster (all World Bank) and Jan Nolte and Froukelien Wendt (IMF). Lastly, we thank Ann Redmon for editing this publication and Aichin Lim Jones and Amy Quach for design and production services.

EXECUTIVE SUMMARY

This report reviews progress in prudential regulatory practices related to three basic fintech products—transaction accounts, credit, and payments. It examines advanced and emerging markets and developing economies and, based on that examination, highlights four priority areas for strengthening regulation.

Four technologies are driving fintech forward: application program interfaces, artificial intelligence, distributed ledger technology, and cloud computing. Mobile technology has facilitated the expansion of fintech products. Fintech can bring many benefits, although it is also associated with new acquisitions and partnerships, new competitors, and new processes and business models and thus with potentially disruptive structural change. Old boundaries are dissolving between segments in the financial sector and between finance and the rest of the economy.

Much uncertainty persists about future fintech prudential risks so, unsurprisingly, many jurisdictions are spending resources to monitor developments and engage with industry. Sandboxes, where firms can test innovations under close regulatory scrutiny, are becoming commonplace. Licensing practices are evolving to encourage or require innovators to come within the perimeter, improving the ability of regulators to understand fintech risks over time. Supervisory approaches are also maturing gradually and with significant differences between countries. Capital and liquidity requirements, for example, seem to vary widely from country to country. Supervisors are themselves embracing fintech through supervisory technology (suptech).

One trend is deceptively familiar—the increasing dependence of financial firms on information technology outsourcing. For a long time, regulators have approached outsourcing risks by setting governance standards for the outsourcing firms, but this traditional approach becomes increasingly less effective when firms buy hardware and software as a service. Cloud suppliers continuously move the source of these services around their networks, so there is no longer a place for a customer (or a regulator) to go to monitor and mitigate their risks. The in-house capability of financial firms is diminishing in relation to the capability of suppliers. Making matters worse, if something goes wrong, and a cloud computing company fails, outsourcers have become so dependent on cloud providers, and that industry is so concentrated globally, that practical options for switching are few.

One area of growing prudential concern is the safety of customer funds held by the likes of telecommunications firms that provide e-money services. Should the safety net that bank customers enjoy be extended to customers of these firms too? Some countries have explicitly ruled this out, some have approached it by requiring e-money firms to make back-to-back deposits in central banks or banks, and some are looking into having e-money providers join deposit insurance schemes. The details of most of these approaches are still being worked out, and key questions remain to be addressed. A particularly thorny one is how to address a nonbank e-money provider that fails so that customer assets are protected and continuity of services is ensured.

For many jurisdictions, fintech has increased the importance of working with domestic and foreign regulators. The blurring of lines between the financial sector and other industries, the rapid dissemination of fintech developments, and the reach of global technology firms have contributed to this. Established regulatory forums such as the Financial Stability Board (FSB) and the Basel Committee have been monitoring fintech developments. Fifty agencies from more than 20

jurisdictions participate in the Global Financial Innovation Network.[1] There they share information, coordinate approaches, and explore the topics for mutual recognition of standards

Financial regulators are making strides to improve their understanding of fintech and to address potential associated prudential risks, but four areas remain worrisome:

- Oversight of cloud computing service providers: Regulators in different sectors and jurisdictions cannot oversee these giant providers by themselves. Any corruption or disruption of their services is likely to be systemic.
- Capital and liquidity levels for fintech firms: These vary a great deal according to jurisdiction and are only loosely related to risk. Sufficient capital and liquidity can absorb losses and encourage providers to take risk management seriously.
- Extension of safety nets to resources held by nonbank e-money providers: In several jurisdictions, it is hard to say whether e-money safety nets are robust. The details of what happens when an e-money firm fails are unclear. Bankruptcy law may need to be changed.
- Embracing suptech: This presents opportunities to manage the ever-increasing data flows from regulated entities, improve analysis and take advantage of big data. But is also presents risks related to the capacity of supervisors, operations, and data similar to those that regulated institutions face.

No major jurisdiction except Mexico has seen the need for a fundamental rethink of its financial legislation to cope with fintech. Time will tell whether regulatory coordination and cooperation and a patchwork of fixes will be enough to address future fintech prudential risks.

INTRODUCTION

This report is a stock-take of the state of prudential supervision and regulation of fintech. It focuses on prudential questions related to three basic products—transaction accounts (deposits and e-money accounts), credit, and payments—because they are foundational for all markets and essential for the deepening of the financial systems of emerging markets and developing economies. The report identifies types of existing regulatory approaches, as well as emerging key questions, but does not attempt to identify best practices, because the regulatory developments analyzed are too recent to draw conclusions. The report is targeted at policy makers.

The report adopts the Bali Fintech Agenda definition of "fintech": "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."[2] Of those technological advances, the report examines artificial intelligence (AI) (including machine learning (ML)), application programming interfaces (APIs), distributed ledger technologies (DLTs), and cloud computing. These basic technologies are already affecting the financial sector thanks in part to mobile technology, which has greatly facilitated the expansion of fintech products. Other technologies that may matter in the future, such as quantum computing and wearables, are not covered here.

Against this definition of fintech, the report focuses on the effects that fintech has on market developments (including benefits and risks) and attendant implications for existing prudential regulatory, supervisory, and resolution concepts and practices. It takes a comprehensive view of prudential regulation, which refers to macroprudential regulations addressing risks to the financial system as a whole and microprudential regulation addressing risks to institutions or individual markets. Regulations should ensure that institutions' risks are well managed and that they have enough capital and liquidity.[3] Then, in the event that they nevertheless fail, there should be a way to resolve the institution without disruption to the system or cost to the public. In the case of markets, microprudential regulation is aimed at ensuring transparent price discovery and smooth clearance and settlement of transactions.[4] Cybersecurity is not included in this report because it is addressed in a separate publication.[5]

The universe of publications that have been analyzed consists mainly of English-language materials that governments around the world and financial regulatory agencies have published. The team has also used materials published by international financial institutions, standard-setting bodies, law firms, foundations, consultancies, and academics. The authors also interviewed officials and experts from Australia Brazil, Canada, China, Colombia, Mexico, the European Union, Switzerland, the United Kingdom, and the United States.

The jurisdictions analyzed include emerging markets and developing economies and advanced economies. Fintech market developments are not necessarily associated with degree of market development. For example, e-money providers are large and systemic in some emerging markets and developing economies, whereas they are small in mature markets. Therefore, fintech prudential experiences are relevant for countries of all income groups.


0.4
1.5
3.4
3.5
7.9
2.5

UNDERSTANDING THE CHALLENGE

Fintech Growth

"Technology has always played an important role in driving change in the financial sector: from the telegraph to the ATM" (Hauser 2017), but since the global financial crisis, the pace of change has accelerated, and the effect of new technologies has spread across a wider range of financial activities than ever before.

For example, the market for outsourcing of processes and decisions by financial sector firms is growing fast. Worldwide public cloud service revenue is estimated to grow from $182 billion in 2018 to $331 billion in 2022. Revenues for cloud system infrastructure as a service (IaaS), which are the most relevant for financial institutions processing their core banking systems and storing critical data in the cloud, are estimated to grow from $31 billion in 2018 to $77 billion in 2022.

When examining the effect of fintech on different segments of the financial services sector, the payments industry stands out. From 2013 to 2017, total electronic transactions globally grew by 50 percent. The pace of growth differs in different economies, with Emerging Asia, Middle East and Africa experiencing faster growth in noncash transactions (figure 1) than other countries.

Fintech has also affected other segments of the financial sector. The extension of credit by fintech increased from $11 billion in 2013 to $419 billion in 2017 (figure 2). There are differences in the rate of growth of fintech platforms, with markets in China, the United States, and the United Kingdom experiencing the greatest growth in recent years, albeit from a low base. (Fintech lending accounted for approximately 13 percent of overall new lending in the first half of 2018 in China, and in the United States, credit volumes accounted for 4 percent of overall net loan origination in 2016.)

China has emerged as a global leader in fintech growth. Credit via peer-to-peer lending increased from $5.5 billion in 2013 to $358 billion in 2018, and although growth has slowed in the past year owing to regulatory tightening, average year-over-year growth over the whole period remains high. In 2016, 30 percent of fintech firms valued at more than $1 billion were in China. Payment platforms associated with e-commerce and social media dominate the fintech space in China. For example, Ant Financial (formerly Alipay), the largest payment service provider, supported 451 million active users in 2015 and processed on average 153 million transactions a day, slightly ahead of VISA in 2016, at 150 million.

Basic Technologies and Deriving Fintech Solutions

Four technologies underlie many of the applications that have driven fintech growth: APIs, AI, DLTs, and cloud computing:

- APIs are definitions, protocols, and tools that specify how different pieces of software should interact. Standardized APIs help connect disparate systems and separate organizations, allowing them to share data and analytics. APIs allow development of computer programs such as personal financial management tools that access different financial accounts (Dias 2017). They are essential for open banking, because they make it easy to share personal and product data securely among financial institutions.

- AI computer programs are capable of performing tasks such as problem-solving, speech recognition, pattern recognition, visual perception, and decision-making and providing expert advice without human intervention. A central technology underlying AI is ML, which refers to the way computer programs can be algorithmically refined

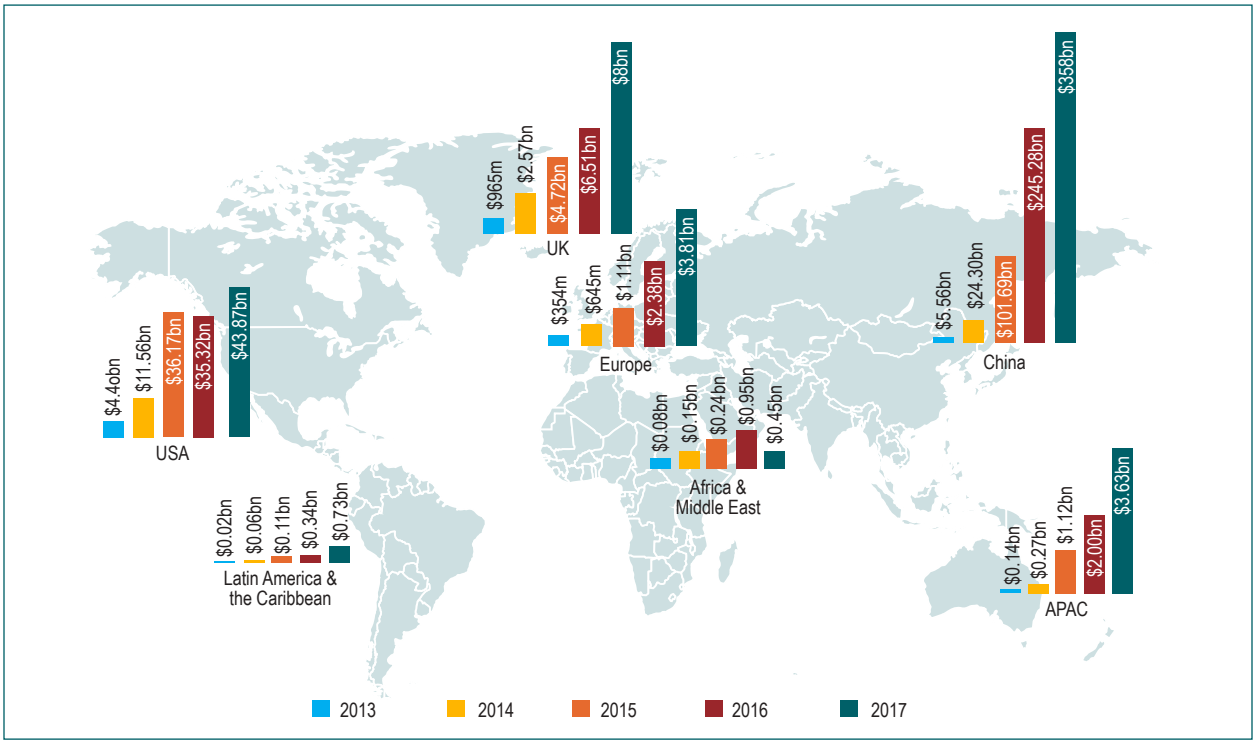
Figure 1: Growth of Number of Worldwide Noncash Transactions, According to Region: 2013-2017

	CAGR (2013-17)	Growth (2015-16)	Growth (2016-17)	
Global	10.8%	10.4%	12.0%	
Latin America	5.4%	3.4%	8.3%	Developing
Middle East and Africa	15.9%	19.0%	19.3%	Developing
Emerging Asia	34.6%	27.6%	32.5%	Developing
Mature Asia-Pacific	10.5%	10.4%	11.0%	Mature
Europe (including Eurozone)	7.9%	8.4%	7.6%	Mature
North America	5.4%	5.1%	5.1%	Mature

Note: Middle East and Africa includes Turkey, South Africa, Saudi Arabia, Africa and Middle East, Russia, Other CE countries and Other MEA countries. Other CE countries includes Bulgaria and Croatia. Other MEA countries includes Algeria, Kenya, Nigeria, Egypt, Israel, UAE, and Morocco; Latin America includes Argentina, Colombia, Venezuela, Chile, Peru, Uruguay, Costa Rica, Bolivia, and Paraguay in other Latin American countries; Emerging Asia includes China, India, Hongkong and other Asian countries including Malaysia, Thailand, Indonesia, Philippines, Taiwan, Pakistan, Sri Lanka, and Bangladesh; Mature APAC (Asia-Pacific) includes Japan, Australia, South Korea, and Singapore; NA (North America) includes the US and Canada; Chart numbers and quoted percentages may not add up due to rounding..

Source: Capgemini Research Institute, 2019.

Figure 2: Fintech Platform Growth: 2013-2017



Source: Cambridge Center for Alternative Finance 2019

to improve outcomes. In recent years, increases in data processing and storage power have boosted AI and ML (Dias 2017). With cloud computing, AI has supported the emergence of lending (or peer-to-peer (P2P)) platforms.

- DLTs propose, validate, and record data in many places at the same time so that all participants in a DLT system always have valid and identical versions of the data (Committee on Payment Clearing and Settlement 2017; Dias 2017).[6] Unlike traditional databases, distributed ledgers are not centralized, although they may be managed by a single party.

- Cloud computing refers to the practice of using a network of remote servers, typically accessed over the internet, to provide information technology (IT) services. Public clouds that are operated and owned by a third party are typically pay-as-you-go and are available on demand, offering scale, efficiency, and flexibility. They often have functions distributed over multiple locations. Clouds may also be limited to a single organization (private cloud) or a combination of public and private (hybrid cloud). The largest public cloud is Amazon Web Services**.** Financial firms can purchase different levels of service from cloud providers. The basic level of service is IaaS, in which a vendor provides pay-as-you-go access to storage, networking, servers, and other computing resources in the cloud. The next level is platform as a service (PaaS), in which a service provider offers access to a cloud-based environment in which users can build and deliver applications, and the provider supplies underlying infrastructure. With software as a service (SaaS), a service provider delivers software and applications over the internet, that users subscribe to and access via the web or vendor APIs. The highest level is business process as a service, in which a firm outsources many of its business processes to a cloud provider. Cloud computing is increasingly becoming a necessary foundation for other disruptive technologies such as AI. This report focuses on prudential considerations regarding IaaS, which is the most relevant for financial institutions processing their core banking systems and storing critical data in the cloud.

An indirect outcome of the development of API, AI, and cloud computing is that large volumes of unstructured (e.g., emails, internet traffic) and structured (e.g., databases) data, so-called big data, can be stored, exchanged, and analyzed.

Fintech Benefits and Risks

These technologies are affecting market outcomes. Fintech can spur competition; recent research shows that, the less competitive the banking sector is, the greater fintech credit by new players is (Claessens et al. 2018). Financial services and products should be cheaper than they would have been otherwise as a result of cost-saving innovations. Advanced analytics may aid in customization. Big data and the use of ML and AI may make it easier for financial firms to identify specific market segments and to understand their customers' needs more precisely. In addition, know-your-customer regulations may be "automated through ML and advanced analytics; similarly, transaction monitoring for suspicious transactions or sanctions" (Institute of International Finance 2016).

Fintech should increase contestability (the ease with which new firms can enter and leave a market). Open-data policies, which require institutions to ensure that customers have control of data about them, should make it easier to switch from one institution to another. Also, aggregators drawing on sources from different specialist firms should be able to challenge existing universal banking brands with a variety of competitive services, decreasing the value of brand and consumer loyalty. This could result in much better access to financial services.

Nevertheless, the emergence of the basic technologies (API, AI, DLT, cloud) with their attendant positive implications for market developments are not without risks. Table 1 provides an overview of where the technologies presented above may affect prudential risks.

In particular:

- **Levels of uncertainty about the future.** There is a good deal of uncertainty about the effect of fintech on financial stability in the medium and long term. Table 1 illustrates this with the number of data points where the effect of basic technologies could be positive or negative. For example, the effect of APIs on the risk of systems failure: APIs that replace manual or patched-together systems may make interactions more reliable in normal circumstances but, in abnormal times, act as a conduit for contagion. Likewise, consider the effect of AI on reputation risk. To the extent that the analysis of many forms of consumer data supports inclusion and better credit assessments, it reduces risks, but it has not been tested in a downturn, when it may make a procyclical contraction in credit worse. These uncertainties provide a powerful justification for the emphasis that many jurisdictions are placing on monitoring, engagement, and creation of test environments or sandboxes (discussed further below).

- **The technology whose effect is most uncertain is cloud computing.** Consider, for example, the effect of cloud computing on the risk of systems failure. Higher standards of IT management for critical outsourced systems in smaller financial institutions may reduce that risk while at the same time increasing governance challenges, making risk mitigation more difficult. This vulnerability is further explored in the section below on outsourcing.

Table 1: Prudential Risks and Fintech

	Institutional Instability										Market Instability		Network Instability		
	Solvency Risks									Liquidity Risks	Liquidity Risks	Operational Risks	Contagion Effects		Positive Feedback Loops
	Credit (1)	Market (2)	Operational						Reputational	Funding Liquidity Risk			Lost Confidence Due to Asociation	Lost Confidence Due to Exposures	Fire Sales
			People	Processes	IT/Systems										
					System Failure	Cyber	Compliance								
							Data Privacy	Data Privacy							
Artificial Intelligence	>	>	>	>	x	<	<	x	x	–	x	x	<	<	<
Distributed Ledger Technolllogies	>	>	>	>	x	>	<	x	x	–	–	>	–	–	<
Application Programming Interface	–	–	>	>	x	<	<	x	x	–	–	–	<	<	<
Cloud Computing	–	–	x	x	x	x	x	x	x	–	–	–	x	–	–

Source: World Bank staff

[1] Net losses due to loan or exposure impairment or write-offs.

[2] Net losses due to changes in asset market values includes interest rate, fx, equity, commodity risks. Also includes risks specific to options and derivatives.

> = fintech may well reduce prudential risk; < = fintech may well increase prudential risk

>< = it can go wither way; - = fintech likely to have minimal impact on prudential risk

- **Other than cyber risk and fire sales, the category of risk that fintech most affects is compliance risk.** The concern is largely to do with data integrity and security, topics covered in the subsequent section on data governance.
- **AI and APIs may amplify network instability.** In addition to the risk of APIs acting as a conduit for contagion effects, AI may exacerbate contagion because it is a critical technology behind high-frequency trading and other trading and investment strategies that may increase volatility. APIs may facilitate customer switching, making deposits unsticky and, therefore, an unreliable source of funding for institutions holding customer funds. For these reasons, safety nets for nonbank financial institutions, which act as a bulwark against any general loss of confidence and reduce switching risks, are included in the report.

Effect on Market Structure and Attendant Prudential Considerations

The technological developments described in section below on test environments are changing the structure of the financial sector in three ways.

First, they are leading to an increase in outsourcing of activities and decisions. Outsourcing of activities is not a new phenomenon in the financial services industry; outsourcing of data processing and storing of data has existed for many years. What is new is that outsourcing leads to having no physical access to the stored data or its processing. Furthermore, there is a high concentration of providers of outsourced services. Fintech is also leading to outsourcing of decisions, which mathematical algorithms ultimately make, rather than human beings, who often must have specific qualifications to make such decisions and must follow specific protocols laid out in manuals or other formal documents specifying the parameters to be considered in the decision-making process and what is or is not allowed (e.g., customer discrimination).

Second, these technologies are creating the opportunity for nonfinancial firms to provide basic services. New entrants may disintermediate established institutions. Big technology firms such as Facebook in the United States and Alibaba in China have large customer networks and are positioned to take share in several financial markets, including payments, savings, and insurance. Two other examples are that greater efficiencies in international remittance transfers arising from fintech may mean that a significant revenue source for existing banks is going away and that DLT innovations in back office processing may disintermediate prime brokerages. The playing field may be uneven, with new entrants not subject to the same level of regulatory scrutiny as established institutions. Although this is no more than old-fashioned regulatory arbitrage, it challenges the structure of the industry and, from a regulatory point of view, challenges the common approach of regulating institutions rather than activities.

Third, established providers such as banks are reacting to the threat of new competition by buying or partnering with fintech developers. For new technology entrants, these alliances give them access to consumer deposits or related account data, payment systems, credit origination, and compliance management (Brainard 2017).

These market trends raise fundamental questions for regulators and supervisors regarding regulatory perimeters and fragmentation. Although regulators have traditionally monitored activities that fall outside their remit, with a view to expanding the regulatory perimeter if necessary, the speed of fintech innovation means that adequate coverage of activity and institutions today is no guarantee of adequate coverage tomorrow.[7] In many jurisdictions, types of institutions rather than types of activities define the regulatory perimeter, and technology firms that provide financial services are often outside the perimeter. Conversely, innovative start-ups and technology firms may not know when their products or services will be subject to financial regulation.

The increasing outsourcing of activities and decisions of financial institutions is testing existing supervisory practices. Are bank management and boards able to exercise oversight on cloud providers? Who should supervise cloud providers? How can algorithms making decisions be overseen to ensure certain regulatory criteria are included in the decision-making process?

Along with the regulatory perimeter, the other prominent theme in published documents about fintech regulation is the challenges that regulatory fragmentation creates. For regulators, these are challenges of coordination. For industry participants, these are the challenges of navigating many regimes if their activities span multiple subsectors or countries.

The problem may be particularly acute for jurisdictions with multiple agencies responsible for regulation and supervision. For example, "the distributed nature of U.S. regulatory authorities means that multiple agencies may have a stake in considering certain fintech matters. It also means that new guidance and programs will often come from multiple agencies and in some cases may have narrower application than comparable measures from jurisdictions with more centralized authorities" (Tsai 2017). Fintech payment and lending firms in particular say that complying with fragmented state requirements is costly and time consuming (US GAO 2018). The United States is not unique in this regard.

Fragmentation is also a challenge internationally. Technologies are often portable, and fintech companies look for ways to exploit economies of scale by selling their services internationally, which increases the need for international coordination and cooperation between supervisors on the regulatory treatment of cross-border technology companies, among other things. Greater international cooperation may be beneficial for all parties (Basel Committee on Banking Supervision 2017)."

APPROACHES TO REGULATION

To stay abreast of fintech development and ensure that firms are brought within the perimeter when necessary, authorities around the world have created arrangements to monitor and engage with the fintech community. These arrangements range from holding regular meetings to creating innovation hubs. Several jurisdictions have also created sandboxes—live test environments to observe new firms, products, or processes outside of the regulatory perimeter. Authorities have also modified the regulatory perimeter to take into account fintech developments. Some jurisdictions have used the existing framework and applied it to fintech; others have created new types of licenses with different prudential requirements. Supervisory practices are being developed for newly licensed fintech companies, and existing supervisory approaches are being applied to outsourcing to fintech firms. Supervisory practices overall are taking advantage of technological developments, a phenomenon called suptech. No jurisdiction has modified the existing resolution framework to take into account fintech developments, but some are experimenting with ways to include nonbank deposit payments of fintech firms in their safety nets. Lastly, domestic and international cooperation arrangements, ranging from exchanges of information to harmonization of frameworks, are emerging.

Monitoring and Engagement

At any point in time, regulators need to know how fast fintech is developing. They need to know where processes have been created or eliminated and where they have been streamlined so they can understand the implications for adding value in different parts of the financial sector and for emerging risks.

Jurisdictions around the world are engaging with the industry in different ways. For example, in the United States, regulators are reaching out through so-called "office hours," which means that they travel from city to city to meet fintech company executives and explain regulation to them.[8] In France, in 2016, the prudential authority in charge of banking and insurance supervision (Autorité de Contrôle Prudentiel et de Résolution (ACPR)) and the securities markets regulator (Autorité des Marchés Financiers) created the Forum FinTech, which gathers financial sector regulators, the Minister of Finance, and financial sector participants (fintech and more traditional segments) to share what they know about questions, concerns, and risks related to fintech. The Hong Kong Monetary Authority has set up a "Fintech Supervisory Chatroom to provide feedback to banks and tech firms at an early stage of their fintech projects" (HKMA 2016).

Innovation hubs are another, often government-led, effort that can help prudential supervisors engage with the fintech industry and stay abreast of fintech development. There are more than 30 innovation hubs around the world, primarily in North America, Europe, the Gulf countries, and Asia (box 1). In eight jurisdictions, the regulator or central bank is the host. Stated objectives of innovation hubs vary, from promoting innovation to financial inclusion and risk mitigation. Bahrain, Cyprus, Estonia, Hong Kong, Malaysia, Singapore, and the United States have all identified risk mitigation to consumers and the markets as a major objective of their hubs.

Test Environments

Many regulators have decided to create test environments for fintech through sandboxes—formal regulatory programs that allow market participants to test new financial services or business models

with live customers, subject to some safeguards and oversight, usually for a limited time. More than 31 authorities have created regulatory sandboxes in the last few years, nine are in process of creating one, and nine are planning to (box 2).

Broadly speaking, sandboxes may focus on testing products or policies. Sandboxes testing products aim to establish the commercial viability of the product, and those testing policies aim to assess whether particular rules or regulations should be changed based on specific use cases. The sandbox becomes the final step in a regulatory continuum, which begins with informal guidance on regulatory uncertainties and ends with a test to determine whether the business model or an existing rule

Box 1: Existing Innovation Hubs and Hubs Linked to Regulators

Innovation Offices

Australia	Hong Kong	Netherlands
Austria	Hungary	Norway
Bahrain	Iceland	Poland
Belgium	Indonesia	Romania
Canada	Ireland	Singapore
Cyprus	Italy	Spain
Denmark	Japan	Sweden
Estonoa	Latvia	Switzerland
Finland	Liechtenstein	Thailand
France	Lithuania	UK
Germany	Malaysia	USA

Innovation Hubs Linked to Regulators/Central Banks

Abu Dhabi
Bahrain
Dubai
France
Hungary
Portugal
Singapore
South Korea

Source: UNSGSA FinTech Working Group and CCAF 2019.

Box 2: Operational, Forthcoming, and Proposed Sandboxes

Operational Sandboxes			Forthcoming Sandboxes	Proposed Sandboxes
Abu Dhabi	Japan	Russia	Bermuda	China
Australia	Jordan	Saudi Arabia	Brazil	EU
Bahrain	Kazakhstan	Sierra Leone	India	Fiji
Brunei	Lithuania	Singapore	Indonesia	Israel
Canada	Malaysia	Switzerland	Jamaica	Japan
Denmark	Mauritius	Taiwan	Kenya	Malta
Dubai	Mozambique	Thailand	Mexico	South Korea
Hong Kong	Netherlands	UK	Norway	Sri Lanka
Hungary	Nigeria	USA	Spain	Uganda
India	Philippines			
Indonesia	Poland			

Source: UNSGSA FinTech Working Group and CCAF 2019.

or regulation needs modification. The Monetary Authority of Singapore (MAS) has been a pioneer in this approach to evolving policy.

Licensing

Authorities are addressing the challenges that fintech poses to the regulatory perimeter in different ways. Generally, common law jurisdictions have been able to apply existing legislation and adapt old procedures for chartering or licensing, whereas in civil law jurisdictions, it depends on institutional structure. If there is a unified financial regulator, it is easier to accommodate fintech licensing internally. If different regulators are responsible for different parts of the financial system, it is harder, and new legislation can be needed.

The United Kingdom is an example of a common law jurisdiction. Although it has separate prudential and conduct regulators, most accommodations needed for fintech could be made administratively within the Bank of England, the Prudential Regulation Authority, and the Financial Conduct Authority. At the other end of the spectrum is Mexico, a civil law country with a divided regulatory structure, which had to pass new legislation in March 2018 to achieve its fintech policy objectives.

In between the United Kingdom and Mexico are common law and civil law countries that have used a combination of measures to establish appropriate definitions of fintech through small changes to existing primary legislation (e.g., Switzerland) or adapted rules or introduced secondary legislation for licensing in various ways (e.g., Australia).

Before they define a perimeter, jurisdictions need a definition of the term "fintech."[9] Some have chosen to enumerate covered activities, whereas others have defined fintech in terms of specific technologies and their potential effect. The FSB definition of fintech has been influential: fintech is "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."[10] Most national definitions of fintech approximate the FSB definition in practice.

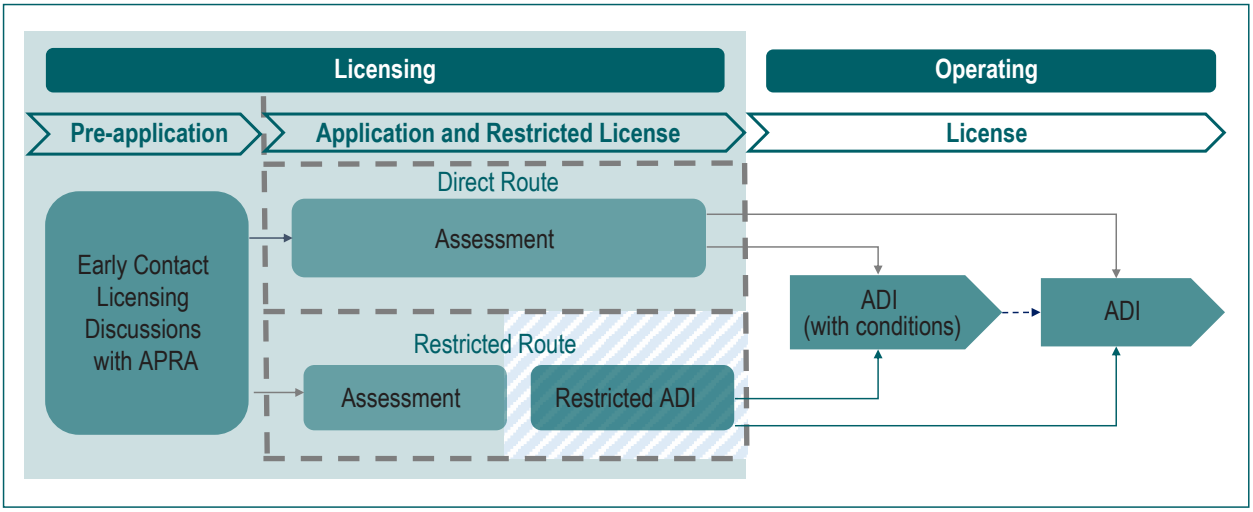
With a fintech definition in hand, jurisdictions have adopted a one- or two-perimeter model. Under the one-perimeter model, all fintech firms must register with the authorities so that they can be monitored. Under the two-perimeter model, all fintech firms must register and be monitored, and a subset must also be licensed and supervised. Two approaches have emerged to the two-perimeter model: one in which the subset is defined in terms of activities or size and another in which it depends on how long a firm has been registered.

China is a leading example of the one-perimeter approach. Since 2015, China's Ministry of Finance has defined its internet finance regulatory perimeter by enumerating specific activities, including payment services, lending (P2P and online microfinance), crowdfunding, fund sales, insurance, trust services, and consumer finance delivered over the internet. Firms engaged in this sort of activity must register (Chinese Ministry of Finance 2018). It is expected that the Chinese perimeter model will evolve into one of the other forms.

The European Union illustrates the first approach under the second model. The European Banking Authority (EBA) recently stated that crowdfunding, consumer credit, robo advice, financial intermediation services, comparison services, and credit reference services must all be authorized—defining its inner perimeter where firms are licensed and supervised. Firms engaged in money broking, portfolio management, or portfolio advice need only be registered—defining a second outer perimeter. Firms that simply provide technology to financial firms, such as point-of-sale system providers, regulatory technology firms, and technology support companies, do not need to register or be licensed and so are outside both regulatory perimeters.

Australia's temporary restricted license for authorized deposit-taking institutions (ADIs) is an example of the second approach under the second model. The Australian Prudential Regulation

Figure 3: Australia Restricted Authorized Deposit-Taking Institution Framework



Source: APRA n.d.

Authority (APRA) limits the powers and size of fintech start-ups that receive this license. It lasts for a maximum of two years, constituting a transitional phase for a new entrant in obtaining a full ADI license. APRA assesses each applicant's structure, ownership, governance, and business plan. Fit and proper standards are the same, but capital requirements, shareholding concentration standards, IT requirements, and organizational requirements are lighter than they are for a full ADI license. Applicants also have to say how they expect to graduate to a full ADI license and, in the interim, must have an exit plan.

With respect to types of licenses, regulators have developed four approaches for e-money providers based largely on the relative roles of banks (or narrow banks) and nonbanks, such as telecommunications companies (Gates Foundation 2019). Table 2 summarizes these approaches and their various advantages and disadvantages and provides examples of e-money providers for each type of approach. Licensing requirements for lending or P2P platforms vary from country to country. A recent World Bank technical note examined registration—one step in the licensing process—in the United States, United Kingdom, China, and Indonesia. In these jurisdictions, registration seems to be complicated, sometimes involving multiple authorities, multiple steps, capital requirements, membership in a local industry association, and certification from the International Organization for Standardization for information security (table 3).

To obtain a license, fintech firms have generally had to meet specific conditions, and then, to keep their license, they must operate within specific rules that are enforced through some level of supervision. The types of rules are broadly similar across jurisdictions and closely follow those used for banks. For example, the European Central Bank has set out rules for license applications for fintech credit institutions that mirror those for regular European banks.

There are differences between rules for banks and those for fintech. Capital and liquidity requirements, as well as permitted and prohibited activities, stand out. The paragraphs below highlight the features of fintech that may require a different approach or calibration.

- **Governance arrangements:** A management body comprising people who are competent and experienced is required. Typically, the founders of a fintech company need qualifications and experience that are very different from those

Table 2: Approaches to Licensing E-Money Providers

Licensing Model	Nonbank Functions[1]	Advantages	Disadvantages	Examples	
				Country	Services
Bank only	None	• Banks already licensed and supervised • Risk management and anti-money-laundering and countering financing of terrorism systems in place • Can lead to other services	• Business case for expansion may be weak • May lack understanding of poor and rural markets • Few examples of helping with financial inclusion	Bangladesh South Africa	bKash FNB eWallet
Narrow bank	None	• Clarity on licensing and supervision	• Prudential requirements for all banks may not fit narrow banks well	India Pakistan	Paytm Payments Bank EasyPaisa Telenor Microfinance Bank
Bank based but nonbank led	Branding and delivery	• Clarity on licensing and supervision	• Tight supervisory control of, for example, new products and services, changes to account limits • Indirect communication between nonbank and banking supervisors	Cameroon Uganda	MTN MoMo Airtel Money, MTN Mobile Money
Nonbank special purpose vehicle	All except safeguarding	• Common in high adoption jurisdictions • Direct communication between nonbank and banking supervisors • Separate legal entity can help in governance, supervision, and resolution	• Strain on supervisory capacity • Mobile network operators may restrict competition • Unclear legal authority of banking supervisors over nonbanks • Interagency coordination	Brazil China Nigeria Tanzania United States	Payment institutions Alipay FirstMonie (bank), Paga (nonbank) M-Pesa PayPal

Source: Gates Foundation forthcoming.

[1]Possible functions include license to issue e-money, direct communication, contractual agreement with customer, branding of e-money service, delivery of e-money service, safeguarding of customer funds.
Note: Brazil requires technology companies with non-fintech businesses to set up a local fintech subsidiary. Not all countries fit neatly into this typology. For example, the UK Financial Conduct Authority has different payment and e-money licensing requirements based on size, with more demanding associated regulations as size increases. Thresholds are at average monthly turnover in payment transactions below $3.3m (€3m), between $3.3m and $5.5m, and above $5.5m (https://www.fca.org.uk/firms/authorisation-registration-emoney-payment-institutions).

Table 3: Features and Requirements of National Peer-to-Peer Platform Registration Processes

	United States	United Kingdom	China	Indonesia
Multiple agencies	Federal and state	Financial Conduct Authority only	Federal and local	
Steps in the process			Multiple steps	Two-step process
Capital requirements	None	Minimum requirements	None	Minimum requirements
Association membership				Yes
International Standards Organization 27001 certification			Yes	

Source: World Bank staff

required for effective bank leadership. For a start-up, much-less-elaborate governance arrangements may suffice—simpler procedures and smaller numbers of people involved—provided they are transparent and effective.

- **Ownership and control structure:** Shareholders in start-ups must have considerable financial resources from the outset to avoid excessive leverage as they grow. Broadly speaking, the same is true of a fintech firm as a bank, although requirements are calibrated to different short- and long-term liquidity and capital requirements.

  For fintech firms that are part of a larger established technology company, most countries require that company to set up a subsidiary. Kenya is a notable exception. Segregation of the financial sector activity in a subsidiary is critical should the parent or subsidiary fail. If the technology firm is an international one, a local subsidiary—or at least a supervisable local presence—is often a requirement.

- **Fit and proper owners and managers:** Owners and managers must be of good character. This standard is often the same for fintech firms and banks. It is hard for applicants to prove a negative—that they have never done anything wrong—but evidence of good standing is typically part of fintech licensing requirements.[11]

- **Capital, liquidity and solvency:** There should be enough assured resources to cover initial losses, finance growth, and possible strategic shifts that can be necessary in the early stages of any business (ECB 2017). Details on the level of initial and ongoing capital required for e-money providers and lending platforms in different jurisdictions and attendant observations are provided in Table 4. With respect to the source of initial capital, many fintech companies have foreign sources of capital. This may be challenging for countries that have foreign exchange controls.

- **Business strategy and plan:** There must be a well-thought-out business strategy and plan (including plans for any future acquisitions). In addition, some jurisdictions such as Australia require firms to have a nondisruptive resolution or exit plan.

- **Internal controls and risk management arrangements:** Strong, well-documented core risk management processes are necessary. In banks, these include processes to score loan applicants, approve new loans, manage collateral, and manage nonperforming loans. Requirements for fintech firms can emphasize strong processes for cybersecurity and outsourcing risk management and data governance backed up by good audits.

- **Consent of other supervisors:** Consent of any other supervisors is important for banking supervisors—for example, for listing a bank on a stock exchange subject to separate regulation, although for fintech firms, particularly e-money providers, other agencies may need to be involved, such as those responsible for IT, industry development, telecommunications, or communications.
- **Permitted and forbidden activities:** Banks and fintech firms should engage only in permitted activities. For banks, these typically include lending, payments, and deposit taking but may also include other services such as custodian and trust services. For other activities such as securities trading on their own account, permissions and prohibitions vary according to jurisdiction. For fintech firms, permitted activities are typically more narrowly defined—payments, but not lending for e-money firms and facilitating P2P lending and maybe some borrower research for platforms—although permissions may be broader for fintech firms than banks in one respect; a parent may be permitted to engage in commerce, as is the case for Alipay, for example, which is a subsidiary of Alibaba, a company active in the e-commerce, retail, internet, and technology sectors.

It is too soon to see how these special licensing arrangements are going to work. In Switzerland, for example, the fintech license has been available only since January 2019. The Swiss Financial Market Supervisory Authority is assessing the first applications, so it is too soon to say how many will be granted. Similarly, in Mexico, the first licenses were due to be filed by late September 2019. The authorities received 85 applications: 60 for electronic payment institutions and 25 for platforms. The Comisión Nacional Bancaria y de Valores (CNBV) has six months to grant a license. During that time, it can go back one time to give the fintech firm a month to modify its application. The largest firms will be probably ready, but smaller firms with limited resources and those who did not take the filing process seriously may not be able to file properly and in time. The situation will become clearer after the CNBV has completed its reviews.[12]

At the U.S. Office of the Comptroller of the Currency (OCC), which announced a special-purpose fintech charter with fanfare in July 2018, there had been no formal applications as of June 2019 (OCC 2019).[13] (Litigation from several states that challenges the OCC prerogative to supersede their regulation has compromised the potential for this sort of license (Ballard Spahr LLP 2018).) Even in Singapore, where the MAS has been active in promoting fintech in a variety of ways, it was not announced until July 2019 that MAS would award its first five digital banking licenses—two retail full banks and three wholesale—and started accepting applications in August.[14]


D45CB84CA
HELP
https://www.
D45CB84CA

APPROACHES TO SUPERVISION

Fintech is affecting supervisory practices in three dimensions. First, prudential regulators have developed supervisory practices for recently created fintech firms such as e-money providers and lending platforms. Second, supervisors have adapted existing supervisory practices to oversee and mitigate micro- and macroprudential risk emerging from increasing outsourcing of processes and decisions by financial firms. Third, to manage ever-increasing data flows from regulated entities and more difficult analytical challenges and to take advantage of big data, regulatory and supervisory agencies have started using fintech internally. This is referred to as suptech, which represents an opportunity but also presents risks.

E-Money Providers and P2P Platforms

Although supervision covers many aspects, this section focuses on capital and liquidity, which firms need to operate, as well as the ability of supervisors to ensure that fintech companies comply with the almost universal requirement of fund segregation.

It is difficult for financial authorities to set objectively justified capital requirements for fintech services, and there has been little international cooperation to set international standards. E-money providers or payment services are a case in point. Table 4 summarizes the capital requirements for e-money providers in four sorts of regulatory regimes:

- Bank-only schemes, in which a banking license is needed to provide e-money services
- Narrow banking schemes, in which banks must set up a narrow bank specifically to provide e-money services
- Banking-based but non-bank-led schemes, in which a nonbank firm takes the lead in branding and delivery, but a banking relationship is the means through which the resources of customers are safeguarded and the relationship with the regulators is maintained
- No-bank special purpose vehicle schemes, in which a bank is involved only in safeguarding customer funds

Table 4 illustrates that there are large differences in capital requirements during licensing and later on as operations develop. Capital requirements are based on different ratios with regard to deposits, liabilities, risk-weighted assets, and, in the case of Bangladesh, an absolute number.

Capital requirements for lending platforms are also uneven. Only one-third of jurisdictions worldwide had minimum capital requirements, and one-fifth required P2P to hold capital proportionate to the total amount invested in the lending platform (WBG and University of Cambridge 2019). China and the United States, for example, had no capital requirement, the United Kingdom had a requirement of 0.2 percent of the total value of loaned funds up to £50 mm (USD64 million), with the marginal rate declining to 0.05 percent above £250 million (USD320 million) (World Bank 2019 b).

One useful way to think about capital requirements for e-money providers and P2P platforms (and other sorts of fintech services) is that many if not all of their risks are operational, and operational risks tend to be heterogeneous and fat-tailed, and applicable data for estimating loss distributions tend to be scarce. For operational risks, there are some useful points of reference. First, the Basel Committee has an operational risk capital standard for smaller banks that requires them to hold operational risk capital equal to at least 12 percent of operational revenues or operational expenses, whichever is greater. ("Smaller banks" are defined here as banks with operational revenues and expenses of less than Euro 1 billion;

most e-money providers are likely to fall well below that threshold.) Second, the Committee on Payments and Market Infrastructures–International Organization of Securities Commissions (IOSCO) Principles for Financial Market Infrastructure have a requirement that unencumbered capital be at least enough to cover fully loaded operational expenses for 6 months, to allow for an orderly closure.

It would be useful to know how e-money and P2P capital compare with these two capital requirements. It seems likely from table 4 that there would be a wide dispersion in national capital adequacy regimes for these sorts of fintech firms, but there are other considerations. For example, the length of time it takes to close down a network without causing instability depends on whether there are alternative service providers and whether the obligations (financial or operational) of their customers can be transferred to those competitors cheaply and smoothly. For telecommunications operators in rural areas, transferring e-money accounts effectively might be difficult. Likewise,

Table 4: Minimum Capital Requirements for E-Money Providers

Country	Type	Initial Requirement (USD)	Ongoing Requirement
Brazil	SPV	54,000,000	Greater of 2% of monthly transaction value or 2% of liabilities
Hong Kong	SPV	3,200,000	Unspecified
India	Narrow bank	13,700,000	15% of risk weighted assets
Mexico	Narrow bank	11,100,000	8% of risk weighted assets
Bangladesh	Bank only	5,300,000	USD10,700,000
Columbia	SPV	2,200,000	2% of deposits
Myanmar	SPV	1,900,000	Unspecified
Malaysia	SPV	1,200,000	8% of liabilities
Ghana	SPV	1,000,000	Unspecified
Sri Lanka	SPV	872,000	Unspecified
Peru	SPV	722,000	2% of liabilities
Brazil	SPV	470,000	Greater of 2% of monthly transaction value or 2% of liabilities
EU	SPV	400,000	2% of liabilities
Tanzania	SPV	219,000	Unspecified
Kenya	SPV	200,000	Unspecified
Rwanda	SPV	116,000	Unspecified
Uganda	Bank-based but nonbank led	Unspecified	Unspecified

Source: Gates Foundation forthcoming. For Hong Kong: "https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/retail-payment-initiatives/Explanatory_note_on_licensing_for_SVF.pdf."

Notes: USD0.13 = HK$1.
Nonbank special-purpose vehicle (SPV) in this case refers to nonbanks whether or not they are a special purpose vehicle

if a P2P platform gave its customers any ongoing services after the initial match between lender and borrower, those services could last for several years—the duration of a loan. In both cases, 6 months might not be enough to achieve a smooth resolution.

In banks, capital and liquidity requirements go together. For e-money and P2P platforms, liquidity requirements may be much lower, depending on precise institutional and contractual arrangements. Some major jurisdictions such as the United States and the United Kingdom do not have liquidity requirements for e-money providers. This makes sense when an e-money provider is required to associate any funds held for its customers with a segregated account in a commercial bank, because the liquidity requirement naturally falls on the bank. That is, any quick demand for funds from e-money customers could be met by drawing down the segregated account. Then the only additional liquidity requirement needed from the e-money provider would be what might be needed to cover any operational lag between changes in e-money accounts and the corresponding segregated bank account.

There may, nevertheless, be a case for a bank that has a large liability to an e-money provider to set aside some extra liquidity itself against the risk that the e-money provider fails and all its customers demand funds at the same time. In the case of P2P platforms, similar considerations apply. Only if the lending platform services loans or guarantees the timeliness of debt service payments can a significant liquidity requirement arise.

Once again, bank regulatory standards may be a useful point of reference. The liquidity coverage ratio of banks operating in jurisdictions that have adopted Basel promotes short-term resilience. Banks must have assets that can be converted into cash quickly and easily to meet liquidity needs for a 30-calendar-day liquidity stress scenario.[15] They are also subject to a net stable funding requirement, which means that they must have enough capital and liquid funds available over a one-year time horizon to meet the liquidity requirements that their liabilities generate.

These standards are based on cash flow forecasts under different circumstances. To ensure that those forecasts are accurate, supervisors must understand their business models in some detail, so there is an associated supervisory capacity challenge.

With respect to fund segregation, e-money and P2P platform operators are required to hold segregated accounts to back e-money liabilities in banks or, more rarely, in their central banks (China and Brazil being the most notable examples). Should the provider become insolvent, this account represents the first line of defense for customers, especially if the account is ringfenced from claims by creditors. Therefore, supervision of segregated accounts is critical. Supervision of such accounts takes place in three ways.

- The provider must report the total amount of e-money issued and a statement from the bank where the segregated funds are held.
- The above plus a system-based check on a limit set in the e-money issuance system on the maximum e-money that can be issued. This is how most e-money providers monitor their own compliance. The system will not allow them to issue more e-money than what is configured in the system.
- In addition to the system-based checks, some jurisdictions require independent validation by a certified audit company.

In practice, supervisory arrangements for segregated accounts are weak. Existing supervisory practices for custodian banks and security houses could provide some guidance here. Such institutions are subject to inspections that include analysis of the sample of individual accounts and of transactions to assess their integrity.

Outsourcing

IT outsourcing is not a new phenomenon (box 3), but the regulatory framework and supervisory practices have not kept pace with technological change. The increasing variety and complexity of outsourced IT services and the changing nature of third-party providers pose new conceptual challenges to financial regulators and the institutions they supervise. Computer hardware and software have been changing rapidly, altering the nature of the services that organizations can—and in some key respects must—outsource to third-party providers.

Cloud services have complicated regulation and supervision as services move offsite and providers become more concentrated. Mainframe computers that all members of an organization could access from multiple terminals and the desktop computers and servers that started replacing them in the 1980s were products that financial institutions could acquire and keep in their facilities. These were under their control and, consequently, within reach of bank supervisors and other authorities. It is now possible to share computer resources with remote data centers, including those outsourced to cloud providers located anywhere in the world.[16] Furthermore, the cloud industry is concentrated in a handful of mostly unregulated "big technology" providers, posing additional challenges for financial sector regulators.

The evolution of software poses even more-daunting conceptual challenges. Computer applications run on a shrinking handful of standard operating systems. Not only do the 500 most powerful supercomputers in the world run on Linux today, but something similar is also happening in the cloud. Most virtual computers on Amazon EC2, for example, run on Linux.[17] Meanwhile, 89 percent of desktop and laptop computers run on Windows. Another challenge is the growing complexity of software. The latest version of any application or operating system builds on layers of software developed over many years by thousands of frequently unrelated programmers. Linux is an example of such complexity; more than 15,000 developers from thousands of companies have contributed to developing the Linux kernel since 2005, accumulating nearly 25 million lines of code in 14 years.[18] Estimates for the proprietary Windows 10 operating system exceed 50 million lines of code.[19] The supply of core banking systems has exhibited a similar trend toward concentration in a handful of increasingly complex software.[20]

For individual banks to rely on a few specialized cloud providers makes sense and can even reduce microprudential risks owing to the much higher

Box 3: Early Information Technology Outsourcing in the Financial Sector

In September 1955, just one year after delivery of the world's first business computer (Remington Rand's UNIVAC-1), Bank of America unveiled the electronic recording method of accounting (ERMA) to process checks and automate account management. At around the same time, in partnership with General Electric and the Stanford Research Institute, Bank of America also developed magnetic-ink character recognition (MICR), the string of numbers we see at the bottom of checks that enables ERMA to read bank documents. The American Banking Association adopted MICR as the industry standard in 1956, and it remains the global standard. Since then, the financial system's reliance on computers to handle all kind of processes has been increasing continuously. Bank of America did not develop ERMA and MICR on its own; it relied on the technical expertise of third parties such as General Electric and the Stanford Research Institute. As financial institutions have adopted more information technology in their operations since 1955, they have had to rely on numerous—including many unknown—third parties, outsourcing an increasing variety of information technology services.

Source: World Bank staff.

technological competencies of the cloud services providers, but at a macroprudential level, the challenges are significant. For example, if the cloud provider is compromised, there may be no ready alternative provider to turn to. In other words, risk mitigation may be a challenge. Even if there is an alternative, it is possible that a cloud service provider failure would lead to several financial institutions looking for back-up at the same time, causing problems.

Regulators have sought to adapt existing frameworks to address some of these challenges. EBA (2019), Guidelines on Outsourcing Arrangements,[21] MAS (2016), Guidelines on Outsourcing,[22] ACPR (2013), Guidance: Risks Associated with Cloud Computing,[23] BIS (2012), and Principles for the Sound Management of Operational Risk[24] are key documents. BIS (2012) notes that, "use of technology related products, activities, processes and delivery channels exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks. Sound technology risk management uses the same precepts as operational risk management." Furthermore, BIS (2012) states that the board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring effective risk management.

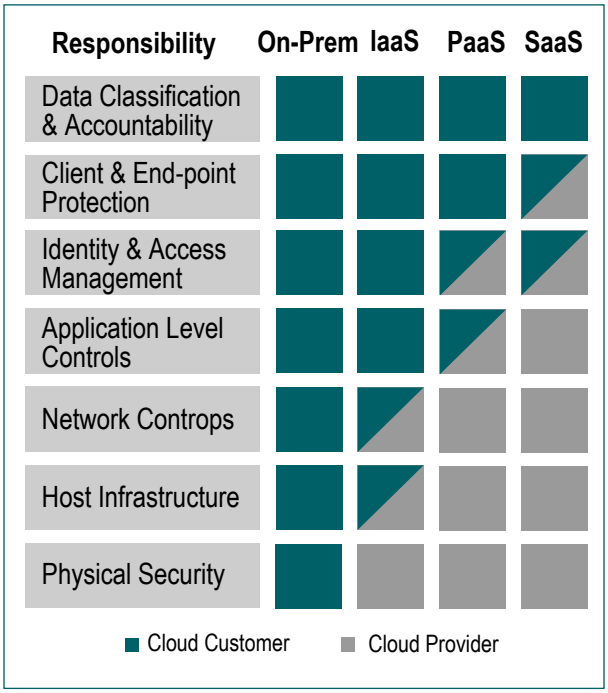
Whether the usual corporate responsibilities are appropriate to address the ever-increasing reliance on technology developed, and increasingly operated, by third parties is unclear. EBA (2019) points out that the main focus of those responsibilities should be "on the outsourcing of critical or important functions, including that the availability, integrity and security of data and information is ensured." Consequently, to fully understand the outsourcing of which IT services would require special attention from the board and senior management of financial institutions, it is necessary to define those "critical or important functions."

Regulatory definitions of critical and important functions focus on those in which a defect or failure would have a material effect on an institution's operations, profitability, or compliance. Several conceivable IT services, such as processing transactions and storing customer information at a third-party provider, would seem to squarely meet the definition of a material outsourcing arrangement, but some technology-intensive services are already expressly excluded from outsourcing regulations. EBA (2019), for example, excludes market information services (e.g., provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch); global network infrastructures (e.g., Visa, MasterCard); clearing and settlement arrangements between clearing houses, central counterparties, and settlement institutions and their members; global financial messaging infrastructures subject to oversight by relevant authorities; correspondent banking services; and acquisition of services that the institution or payment institution would not otherwise undertake (e.g., electricity, gas, water, telephone line).

A crucial question is whether a separate or distinct regulator covers the service in question (e.g., utilities). Providers of cloud services such as Amazon EC2, Microsoft Azure, Google, and IBM, hosting millions of virtual computers in networks of globally distributed data centers, only some which customers fully design and administer, already look like public utilities. Hence, it seems natural to ask whether existing outsourcing regulations are adequate to regulate the reliance of financial institutions on their services, which might need a more nuanced regulatory framework.

Microsoft[25] has suggested an allocation of responsibilities between customers, such as banks and other financial institutions, and their cloud service providers. This may help financial sector authorities decide the risks of which outsourced IT services can a financial firm be expected to control, and which ones must be supervised by an appropriate State agency, as it already happens with utilities and other outsourced services. Microsoft's suggested allocation of responsibilities on several critical dimensions of IT services, as opposed to those that the supervised institution operates on its systems on its premises, depends on the cloud

Figure 4: Proposed Allocation of Responsibilities Between Cloud Customers and Providers



Source: Microsoft 2017
Note: On-Prem, On Premises, namely when cloud services are not used; IaaS, infrastructure as a service; PaaS, process as a service; SaaS, software as a service.

service delivery mechanism: IaaS, platform as a service, and software as a service.

Another concern of many regulators, for any type of cloud services, is the extent of physical access to the data stored with third-party providers. This has already led some major jurisdictions, such as the European Union, to restrict where the data can be stored, but given the nature of cloud services, imposing similar restrictions at a national level could make it impossible for financial institutions to take advantage of technological change in most countries. Furthermore, preserving logical access encrypted data would seem to be far more important than just physical access to it.

Supervisory Technology

Suptech is the use of innovative technology by supervisory agencies to support supervision, especially in the areas of data collection and data analytics, which have traditionally required considerable human resources. Another area in which suptech is used is automated data dissemination; this is not analyzed here because it is not widely used in data collection and analysis.

Despite the high initial investment required to adopt suptech tools, the benefits of using them are considerable and include enhanced effectiveness, better identification of risks (particularly systemic ones), lower costs over the medium and long term (for regulatory agencies and financial institutions), and greater ability to process information. Especially in the area of data analytics, the new technologies can support effective implementation of risk-based supervision and forward-looking risk identification, potentially alleviating supervisory capacity constraints.

Although the benefits of suptech are clear, there are also associated risks. These can be grouped into three categories:

- Technical risks: ranging from difficulty finding and retaining in-house expertise to difficulty integrating suptech solutions with legacy systems, including in most cases, limited internal capacity to manage implementation of complex IT projects
- Data risks: from data privacy risks in using alternative data such as social media or commercially sensitive raw data from regulated institutions; includes unreliability or poor quality of some big data types such as social media
- Operational risk: cybersecurity and outsourcing risks, especially from cloud computing and algorithm providers

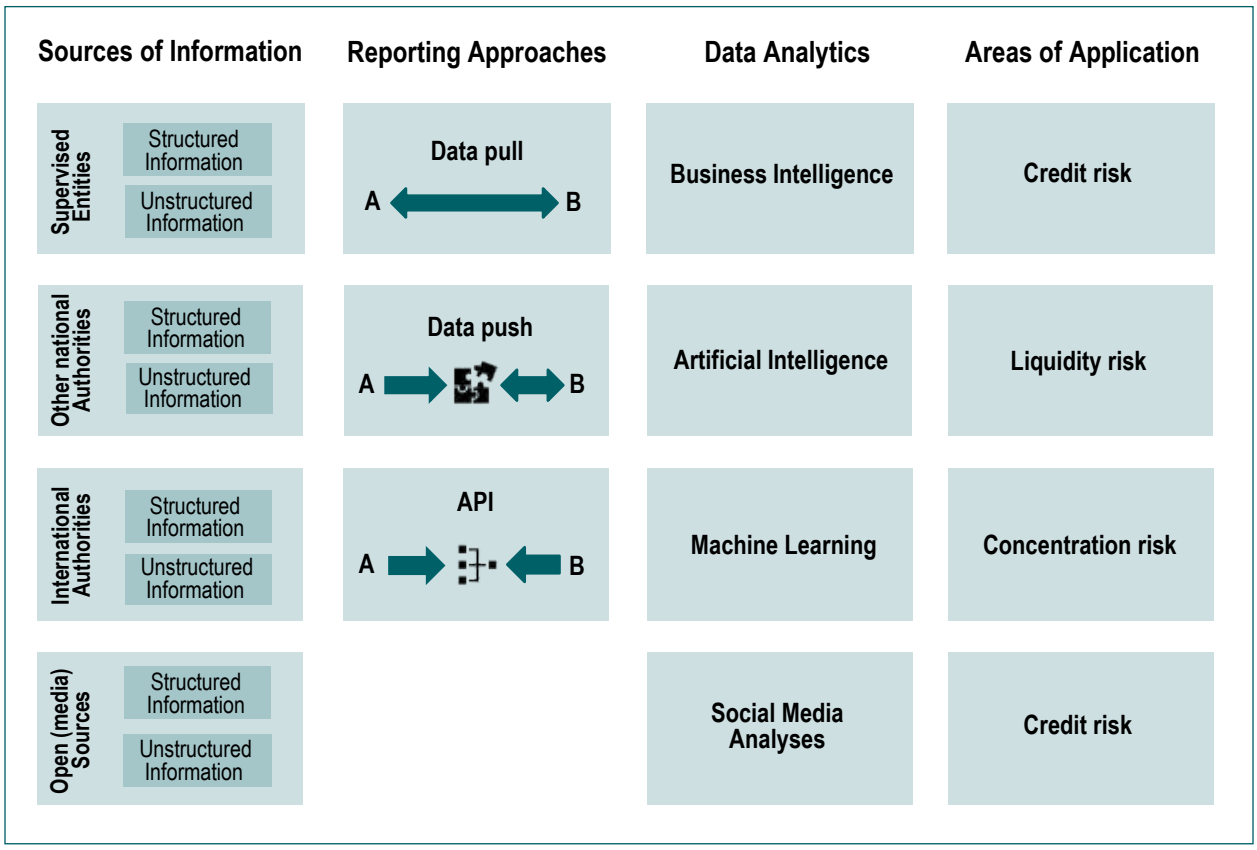
Given the novelty of suptech, mitigation of these risks by financial supervisors is at an early stage, although risk mitigation measures for regulatory

agencies are likely to be similar to measures that the same agencies are requiring of market participants. For example, regulations on outsourcing for market participants are likely to be applicable to regulators as well when trying to mitigate outsourcing risks.

Data collection tools are used to reduce the reporting time and increase the quality of data collected from different sources thanks to advanced validation techniques. Four models have emerged with respect to data collection: data pull, data push, a combination of pull and push, and API. A schematic representation of the different approaches in data collection, as well as areas of application, is presented in figure 5.

The National Bank of Rwanda has implemented data pull, extracting data directly from the IT core systems of the supervised institutions. Because this model has been implemented only recently, it is too early to identify advantages and disadvantages with certainty, although the following observations can be made. Implementing the data pull approach is much more complex and correspondingly more expensive than implementing other suptech data collection approaches. This complexity derives from the fact that all pulled information needs to be mapped to the sources from the core banking system of each bank. Any changes to the core banking system require adjustment of data source mapping. Any new products or changes to the existing ones would probably require adjustment of data source mapping. In some jurisdictions, if primary data are incorrect, it may be impossible to hold bank management accountable, because the information will be extracted directly by the supervisor and not provided by the reporting entity.

Figure 5: Data Collection Approaches



Source: World Bank staff

The Central Bank of Austria (OeNB) uses a combination of data push and pull. This approach entails creation of an intermediary layer between the reporting entities and the supervisor that is responsible for the entire process. In Austria, banks created a company (AuRep) to which they upload all financial and prudential information that the supervisor requires. As soon as the information is validated and uploaded in AuRep's data warehouse, OeNB can extract it for its own needs. Extraction of data from the AuRep data warehouse by the OeNB is technically similar to the data pull approach.

The data push approach has advantages and disadvantages. First, for the intermediary model to be efficient, all reporting entities must be part of the reporting framework. Otherwise, there will be a redundant infrastructure for the process at the level of intermediary company (for entities that are part of this framework) and at the level of central bank (for entities that are not part of this framework). Second, although this approach is costly for the industry, reporting financial institutions can benefit from the reporting framework and use nonconfidential system data from the data warehouse to identify and monitor market developments and establish benchmarks for different business indicators. Third, the intermediary layer can spare significant resources of the supervisor that otherwise would have to be allocated to the reporting infrastructure.

Lastly, the Central Bank of the Republic of the Philippines is implementing the API approach, which does not require human intervention. The Philippines central bank has developed an API for banks to automatically report highly granular and near-real-time data. The tool offers back office functions such as automated validation, data visualization, and report customization. Following the successful test of the prototype, the Philippines central bank is planning to introduce the API. An advantage of this approach is that costs are much lower than in the data push and data pull approaches.

The next frontier of suptech is issuance by supervisors of machine-readable regulations in the form of software (code) that the financial institutions' systems then run. Implementation of this reporting approach requires a high level of technological development in the supervisory authority and the financial industry. A number of authorities are exploring this approach (MAS and Financial Conduct Authority among them), and it is still too early to assess the effect on the financial industry and its supervisors, especially with respect to reporting costs and data quality.

Data analytics tools that have application in the prudential supervision sphere are business intelligence, AI, social media analysis, and ML. These tools allow supervisors to effectively use unstructured information, which in the past used to be processed manually with high human resources costs and a high incidence of errors. These tools are essential to identify intentional wrongdoing (e.g., hidden related-party transactions, market manipulation) that require processing of a significant amount of structured and unstructured information by supervisors.

Business intelligence tools are by far the most popular suptech tools used for data visualization and data drilling (drill down and drill through). These tools allow supervisors to process a significant amount of structured data quickly and transform it into a user-friendly visual information to support risk identification and supervisory decisions. The areas where supervisors most commonly use business intelligence tools are oversight of credit risk, liquidity risk, and payment systems.

Financial sector authorities have recently started using social media analysis tools, which are designed to extract and process media and social media information and highlight useful information. The Bank of Italy, for example, uses information extracted from tweets as a meaningful signal of inflation expectations.

APPROACHES TO RESOLUTION

One of the challenges that the entry of fintech companies into retail banking and the large scale of fintech outsourcing pose is what to do when one of these companies fails. In most jurisdictions, fintech companies are subject to general corporate bankruptcy law. The primary objective of general bankruptcy frameworks is maximization of the value of the firm, rather than protection of depositors, which is the primary objective of deposit-taking institutions.[26] Furthermore, best practices would suggest that, at the start of a general bankruptcy proceeding, the assets of the insolvent company would be frozen under a stay of proceedings, meaning that customers would not be able to access the stored resources immediately.

With respect to e-money providers or P2P platforms, the legal frameworks of some countries recognize that customer assets that payment system and P2P platform participants collect are not part of the company estate. In common law countries, the customers' assets are separated by requiring that the segregated account be a trust account. India, Hong Kong, and the United Kingdom have similar provisions. Civil law countries have used other instruments (e.g., fiduciary, custodial, or escrow accounts) to set up mechanisms with features similar to those of trust accounts. Peru and several other Latin American countries have set up such mechanisms. Turkey requires e-money providers to hold funds in a trust fund account; in the case of insolvency, the funds are to be used to compensate customers regardless of their priority in the bankruptcy process.

If e-float and platform resources are ring-fenced from claims by creditors, provided the insolvency representative[27] of the e-money provider authorizes access to the customer assets by other than telecommunication companies or P2P platform staff and that the records of the subaccounts are in good order, the e-money holders or P2P platform customers can access their funds, although in most cases, customer assets are part of the telecom company or P2P platform estate.[28] As a result, customers are general creditors, and access to e-money and P2P platform funds will not be allowed until creditors higher than e-money holder or P2P platform customers in the hierarchy are satisfied. Even assuming that e-money holders or P2P platform customers will receive the amount corresponding to the value of e-money or amount lent, this could take a long time. Given the longer timeframe of corporate bankruptcy, especially in jurisdictions where e-money providers are systemic, it would seem appropriate to require a nondisruptive exit plan, but only half of jurisdictions globally require it for P2P platforms (WBG and University of Cambridge 2019). Such requirement is also not mandatory for most e-money providers.

Another area that presents new challenges for resolution is cloud outsourcing. This industry is characterized by a high level of concentration, with four providers serving most of the global financial sector industry. Although these providers perform functions similar to those of a utility, they are subject to general bankruptcy, with no consideration for public safety or the public good. Instead, the interests of their creditors drive bankruptcy decisions for cloud services providers. Furthermore, given the small number of providers operating globally, the considerable challenges of cross-border bankruptcy are also worrisome.

Should a cloud provider fail, EBA and MAS stipulate that financial sector supervisors must continue to have access to stored information and require banks to have in place alternative arrangements, but depending on the type of service model stipulated in the contract between the financial institution and the cloud provider, continuity and transfer may not be possible. Transfer to another provider

may not be possible if the cloud provider provides platform as a service and the platform used by the competitors is different. If the financial institution has a software-as-a-service-type contract, the financial institution may not technically be able to transfer the service to another provider, and there may be legal restrictions in using the intellectual property of the former provider with a new provider. Lastly, owing to the concentration of cloud services providers, if the failure of a provider affects several institutions, it may be unclear whether the one or two alternative providers are capable of stepping in to support all of the affected institutions instantly and simultaneously.

Following the global financial crisis, a great deal of attention was paid to resolution regimes for financial institutions, especially banks. Much less attention has been paid to the resolution of outsourcers, beyond requiring banks to have alternative arrangements in place. As safety nets become more important on the retail side, it may be timely to consider how financial regulators should work with regulators in other sectors and with bankruptcy authorities to avoid systemic consequences if an important fintech firm collapses operationally or financially.

APPROACHES TO SAFETY NETS

A few regulators are asking whether some sort of safety net or insurance similar to deposit insurance for banks should cover deposit-like products that fintech firms such as e-money providers offer. Such a scheme would be activated if the fintech firm failed and there were no back-to-back segregated bank accounts (direct approach). When back-to-back segregated bank accounts are required, the scheme could be activated if the bank in question failed (pass-through approach). Coverage by deposit insurance for deposit-like products is particularly relevant for jurisdictions where e-money providers have systemic importance and the failure of such providers could undermine confidence in the financial system as a whole.

In most countries, deposit insurance is restricted to the customers of banks that belong to a government-backed deposit insurance scheme. These schemes typically guarantee depositors that, if their bank fails, they will not lose their deposits. This protection is usually limited so that customers with large account balances may suffer some losses if their bank fails. Limits are sometimes different for different sorts of customers and accounts.

In countries where deposit-like products that nonbanks offer are sizeable, three approaches have emerged (Izaguirre and Grace 2015; Izaguirre and Grace n.d.):

- The **exclusion approach** specifically excludes from the deposit insurance scheme any deposit-like products from a nonbank provider. Examples of countries using the exclusion approach are the Philippines, Turkey, and Switzerland. Normally, a country with an established deposit insurance scheme does not have to change the law to exclude e-money that nonbanks provide because the insurance they offer is available only to bank depositors anyway, but when a country first introduces deposit insurance, it must decide whether to extend insurance to nonbanks.
- With the **direct approach**, deposit-like products that nonbanks offer are insured. Colombia (box 4) and Mexico have adopted this approach, creating new specialized categories of regulated financial institutions that may offer deposit-like products provided they become members of the national deposit insurance scheme. The law prohibits nonmembers from offering deposit-like products.
- The **pass-through approach** extends insurance coverage to digital deposit-like products even when the provider is not a member of the deposit insurance system. The United States has been implementing pass-through arrangements for a long time for trusts and has extended this arrangement to e-money providers. Malaysia and the Czech Republic have adopted this approach; Nigeria, Kenya, and Rwanda are in the early stages of adopting this approach; and Tanzania is considering following this example. In these countries, any nonbank provider must hold customer funds in a trust account (or account with similar features) with an insured depository institution. This trust account would protect customers in case of failure of nonbank providers. In Nigeria, nonbank providers must also have fidelity bond insurance for losses caused by fraudulent acts of their staff (e.g., if staff do not deposit the float at an insured institution). The deposit insurance scheme would instead protect customers should the bank fail. In addition, the deposit insurer does not apply the usual coverage limit to the custodial account. Instead, the limit applied is the sum of the amounts individual e-money customers would have had insured if they had been direct customers of the bank. This would provide some protection for customers from a failure of the bank.

Each of these approaches has its advantages and disadvantages. The exclusion approach provides clarity and is easy to implement but does not

Box 4: Colombia Deposit Insurance for Sedpes

In 2014, the Colombian government introduced a new type of financial institution: sedpes. These licensed institutions can provide only electronic deposits and savings and payments. They are not allowed to provide retail credit but can on-lend the resources they collect from customers to banks. The Colombian financial supervisors supervise sedpes, which are subject to lighter prudential requirements than banks owing to the tight restriction on their activities. Deposit insurance for which the sedpes must pay cover sedpes deposits. If a sedpes fails, depositors are reimbursed from the pool of sedpes deposit insurance contributions. If a sedpes fails because the bank to which it on-lent deposits failed, sedpes depositors would be protected through a pass-through provision of the bank's deposit insurance scheme.

Source: Interview with Fogafin.

protect potentially vulnerable and unsophisticated customers of nonbank financial institutions. The inclusion approach provides protection and clarity regarding regulatory prerogatives, but it may increase compliance costs, inhibit financial innovation, and impose demanding responsibilities on regulators. The pass-through approach provides some protection, perhaps without inhibiting innovation so much, although operating costs may increase, as the requirement for e-money operators to hold a fidelity bond insurance in Nigeria illustrates. The pass-through approach requires regulators to enforce the custodial account rule, making the deposit insurance scheme more expensive than the exclusion approach, and it may not be as easy as the exclusion or inclusion approach to implement.

The operational challenges of the pass-through approach are yet to be fully tested, so for example, if a nonbank e-money provider failed, could the bank holding the trust account identify exactly who owned which e-money accounts and how much each customer had in them? If the bank failed too, could the deposit insurer do the same thing? Moreover, even if a bank or a deposit insurer could identify the beneficial owners, how would it release funds to them if they are in remote areas of the country or otherwise have little contact with the formal economy?

DOMESTIC AND INTERNATIONAL COORDINATION

The overlap between the financial sector and other sectors such as IT and telecommunications is significant and evolving, meaning that coordination between financial sector regulators and with nonfinancial sector regulators is essential. Middle- and low-income countries identify intergovernmental coordination as a greater obstacle than higher-income countries (WBG and University of Cambridge 2019). Furthermore, the "internet of finance" does not respect borders between jurisdictions, and gaps in regulatory coverage at these borders can create opportunities for regulatory arbitrage, as the targeting of initial coin offerings (ICOs) to retail investors through online distribution channels by parties often located outside an investor's home jurisdiction illustrates (WBG 2018; Gifford and Chang2016). This makes international cooperation crucial.

There are obstacles to intergovernmental coordination. First is the sharing of information. This is a particularly acute challenge between financial sector and non-financial sector regulators and between foreign jurisdictions, especially for administrative law countries, where information exchanges may have to be codified in law to be effective, whereas a less formal sort of coordination, such as memoranda of understanding (MoUs), may suffice in common law countries. Lack of international standards also hampers coordination among jurisdictions.

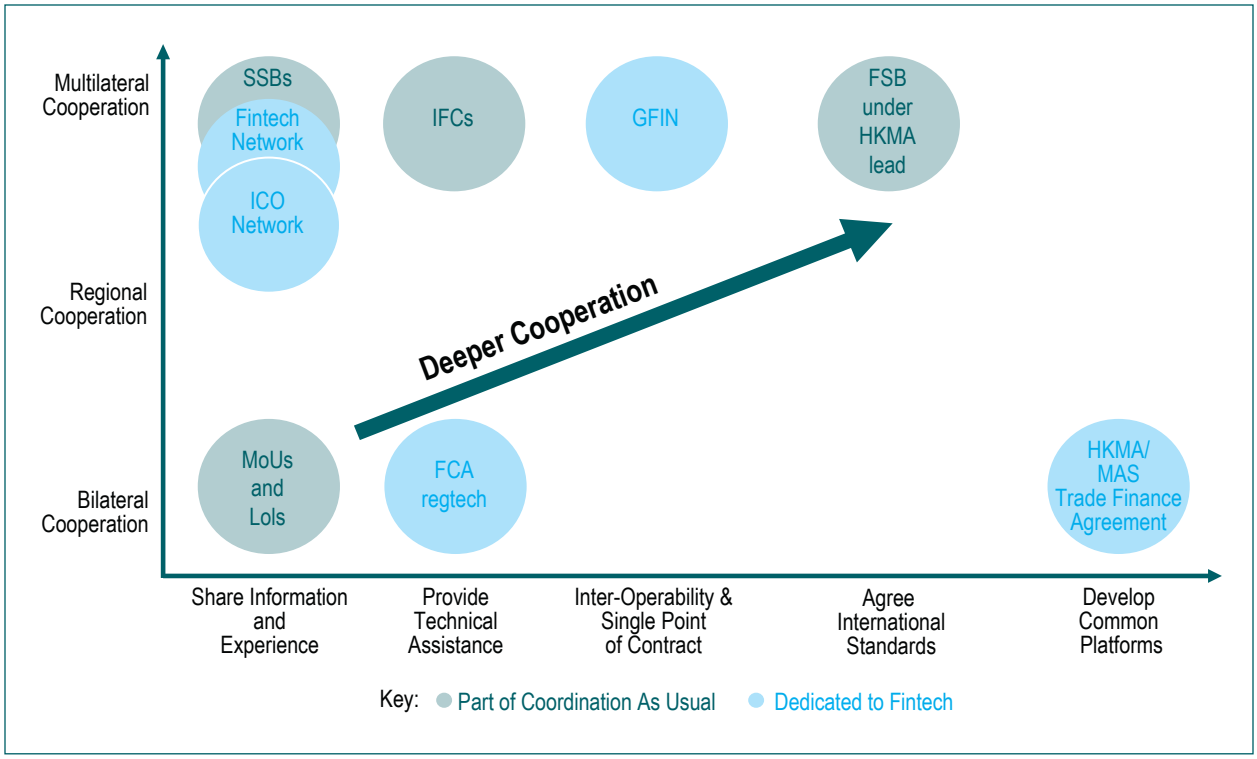
Some countries use existing committees and other permanent groups for domestic coordination. For example, in the United States, there are two standing formal coordination mechanisms among the federal financial regulators: the Financial Stability Oversight Council (FSOC) and the Federal Financial Institutions Examination Council. Both take up fintech issues from time to time and have set up working groups to address particular fintech issues. Set up by the FSOC in 2017, the Digital Assets Working Group is an example. It examines questions related to digital assets and DLT, including financial institutions' exposure, cybersecurity and operational risks, and illicit activities. In other jurisdictions, senior-level coordination results in creation of timebound taskforces to develop proposals or write milestone reports. For example, in the United Kingdom, the Treasury set up the Triparty Cryptoassets Task Force with the Bank of England and the Financial Conduct Authority. In the United States, the Treasury issued a major report on nonbank financial companies, fintech, and innovation in 2018, after extensive consultation with all federal financial regulators.

At the operational level, it has become common for governments to create at least one fintech unit in one financial regulator. In addition to being a point of contact for fintech firms and other outside parties, these usually have interagency coordination responsibilities, which generally include information exchange. In civil law countries, their ability to coordinate policy usually must be statutorily endorsed. In common law countries, less-formal arrangements may suffice for them to coordinate policy development and, beyond that, supervision of established firms adopting new financial technology and new fintech firms.

With respect to international cooperation, different models are emerging. Figure 6 plots existing international coordination arrangements along two axes. The extent of coordination is along the horizontal axis, and the vertical axis defines the scope of cooperation, ranging from bilateral to regional to multilateral.

Sharing of information and experience: Standard bilateral information-sharing arrangements used for other aspects of financial regulatory cooperation are being used to coordinate on fintech. Bilaterally,

Figure 6: Existing Models of International Cooperation



Source: World Bank staff.

this includes MoUs and letters of intent aimed at information sharing, which apply also to fintech developments. Multilaterally, most if not all international financial standards-setting bodies have devoted time to fintech in the ordinary course of business. When appropriate, working groups have been set up to address specific challenges. For example, the Basel Committee on Banking Supervision has a working group on cyber security and a taskforce on fintech. By January 2018, IOSCO had established the ICO Consultation Network, where members could discuss their experiences and bring concerns about ICOs, including cross-border problems.[29] Then in May 2018, IOSCO set up its FinTech Network, covering matters beyond ICOs but with the same objective of discussing experiences and bringing concerns.[30, 31]

Interoperability and a single point of contact: Building on an earlier proposal of the UK Financial Conduct Authority to create a global sandbox, a group of financial regulators created the Global Financial Innovation Network (GFIN) in 2018—a network of regulators to share experiences and best practices and to communicate to firms, a forum for joint policy work, and an environment in which to test cross-border technologies.[32] It has 50 member organizations drawn from more than 20 jurisdictions, which is what makes GFIN stand apart from other fora in which experience is shared. The underlying principle of the sandbox is that, if a fintech firm is found to be satisfactory in a joint sandbox, then it passes muster with all the GFIN members who are signed up. GFIN is therefore a vehicle for coordinating sandbox initiatives, creating a cross-border testing framework so that firms can access different sandboxes simultaneously through a single point of contact. Cross-border testing has begun, with 17 jurisdictions participating, and the results are expected to inform future development of GFIN as much as the technology development of participating firms.[33]

Agreement on international standards: The standards-setting bodies may do more on fintech going forward. HKMA is chairing the Supervisory Review and Cooperation Committee in the FSB, which is examining this.[34] Under their guidance, that committee is looking into developing standards, potentially including for AI and sharing intelligence on fintech developments. The follow-on to the Bali Fintech agenda identifies crypto-assets, mobile money services, and P2P lending as areas for potential international standards (IMF 2019). Still, some authorities remain skeptical; fintech may not be ripe for standard setting, and existing standards, such as for clearance and settlement, payments systems, and data privacy, already cover many aspects of fintech.

There are two additional areas of concern for which something like common regulatory standards may be required. The first relates to the resolution of fintech firms. The second is oversight of cloud service providers. These firms do not service only the financial sector, so their supervision poses a serious institutional challenge to the current structures for financial regulation and global financial regulatory cooperation, but a very few firms worldwide dominate this industry, and financial companies are becoming increasingly dependent on them. Serious consideration should be given to some sort of international regulatory oversight.

Development of common platforms: Two key examples of potential common platforms have emerged. In October 2017, HKMA and MAS signed a fintech cooperation agreement to bolster ties between Hong Kong and Singapore and foster fintech development in the region.[35] They planned to collaborate on a number of initiatives, including joint innovation projects, referrals of innovative businesses, information sharing, and exchange of expertise. The two authorities also committed to linking a Hong Kong DLT trade finance platform with a similar platform in Singapore so that banks in one jurisdiction can transact with banks in the other and avoid fake and duplicate transactions.[36] To ensure that the linked platforms can operate together, HKMA and MAS would harmonize trade finance regulations.

CONCLUSION

This report has reviewed progress in prudential regulatory practices nationally and internationally. Although much has been done since the global financial crisis 12 years ago, four areas are worth noting where additional efforts may be needed to strengthening regulation in the future.

- At the top of the list is oversight of cloud computing service providers, which are currently outside the regulatory perimeter. The challenge is a global one that requires regulators in different sectors and jurisdictions to cooperate to oversee these giant providers effectively. Then, if services are corrupted or interrupted or a provider fails, public policy needs to ensure that the financial system is insulated from the worst consequences.
- Emerging requirements for capital and liquidity related to e-money providers and lending platforms seem inadequate to address the types of risks these firms face. Supervisory practices regarding the segregated accounts for these firms also fall short. This is particularly of concern because, together with capital, float accounts are the first line of defense for customers.
- To manage the ever-increasing data flows from regulated entities and more difficult analytical challenges and to take advantage of big data, supervisors have embraced suptech. This represents an opportunity, but it also poses risks related to the capacity of supervisors, operations, and data similar to those that regulated institutions face.
- Details of the extension of safety nets to nonbank e-money providers, especially in jurisdictions where they are systemic, are unclear. As a practical matter, what ensures that customer services will be uninterrupted if a nonbank provider fails? In several jurisdictions, making e-money safety nets robust may depend on changes in bankruptcy law.

ENDNOTES

1. See https://www.fca.org.uk/firms/global-financial-innovation-network
2. World Bank 2019 a, By implication, this definition incorporates a broad notion of "a business model." The narrow and maybe more proper interpretation of a "business model" is the way that an organization adds value—the services and products it produces. The broader interpretation includes significant aspects of how the business is organized. So, for example, outsourcing of information technology does not affect the business model narrowly defined, but when outsourcing is extensive, it affects the organization of a business significantly and thus affects its business model as broadly defined.
3. See https://www.bankofengland.co.uk/prudential-regulation
4. See https://www.ecb.europa.eu/pub/pdf/fsr/art/ecb.fsrart201405_03.en.pdf?0ee45487b0d8552eb4ec32396d2702c7
5. World Bank 2018. http://documents.worldbank.org/curated/en/686891519282121021/Financial-sector-s-cybersecurity-regulations-and-supervision
6. See https://searchcio.techtarget.com/definition/distributed-ledger
7. One indication of the speed of fintech developments is the rate of regulatory revision. For example, the EU Directive on payments, issued in 2018, was superseded by a new version issued in 2019. See https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366
8. Interviews with the Office of the Comptroller of the Currency and the San Francisco Federal Reserve Board.
9. Some jurisdictions set policy with respect to a slightly different concept. For example, in China, their policy is set for what they call "internet finance."
10. See https://www.fsb.org/work-of-the-fsb/policy-development/additional-policy-areas/monitoring-of-fintech/. The Bali Fintech Agenda definition, mentioned in the introduction, came later. The two definitions are extremely similar.
11. APRA for example, applies its bank standards for fit and proper to fintech firms.
12. Based on an interview with Carlos Orta, consultant.
13. See https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-74.html
14. See https://vulcanpost.com/667288/mas-digital-banks-singapore/
15. See https://www.bis.org/publ/bcbs238.htm
16. The U.S. National Institute of Standards and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (https://csrc.nist.gov/publications/detail/sp/800-145/final)
17. See http://thecloudmarket.com/stats
18. See https://www.linkedin.com/pulse/core-banking-systems-market-now-martin-whybrow/
19. See https://www.makeuseof.com/tag/linux-market-share/

20. See https://www.linkedin.com/pulse/core-banking-systems-market-now-martin-whybrow/

21. See https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

22. See http://www.mas.gov.sg/news-and-publications/media-releases/2016/MAS-Issues-New-Guidelines-on-Outsourcing-Risk-Management.aspx

23. See https://acpr.banque-france.fr/en/risks-associated-cloud-computing

24. See https://www.bis.org/publ/bcbs195.htm

25. See https://gallery.technet.microsoft.com/shared-responsibilities-81d0ff91/file/153019/2/Shared%20Responsibilities%20for%20Cloud%20Computing%20(2017-04-03).pdf

26. Although there have been unique cases (auto industry bailout in the United States) in which corporate insolvency law was used in specific ways to protect "systemically important" businesses, this was widely seen as a perversion of corporate insolvency law and is far from the norm.

27. Often referred to as receiver, trustee, or various other names depending on jurisdiction and context.

28. It is possible, particularly under common law, that e-money deposits could be considered funds held "in trust" and therefore separate from the estate. It is precisely this uncertainty that would lead one to conclude that this area deserves more attention from regulators.

29. See https://www.iosco.org/news/pdf/IOSCONEWS485.pdf

30. See https://www.iosco.org/news/pdf/IOSCONEWS497.pdf

31. In the same month, the Committee on Payments and Market Infrastructures published a strategy to encourage and help focus industry efforts to reduce the risk of wholesale payments fraud. See https://www.bis.org/cpmi/publ/d188.htm

32. See https://www.fca.org.uk/publication/consultation/gfin-consultation-document.pdf

33. See https://www.fca.org.uk/firms/global-financial-innovation-network

34. See http://www.fsb.org/work-of-the-fsb/policy-development/additional-policy-areas/monitoring-of-fintech/.

35. See https://www.hkma.gov.hk/eng/key-information/press-releases/2017/20171025-4.shtml

36. In recent discussions with the HKMA, a similar trade finance initiative linking eight European authorities was mentioned, but recent searches have not found anything regarding authorities cooperating in Europe. Still, there is evidence of banks operating in Europe to create a cross-border trade finance consortium called we.trade (https://we-trade.com/), and we.trade and its Asian counterpart, eTradeConnect, have recently signed a MoU to develop interoperability between their two networks. (https://cms.we-trade.com/app/uploads/we.trade-and-HKTFPCL-Joint-press-release-FINAL.pdf.)

BIBLIOGRAPHY

Basel Committee on Banking Supervision. 2018. "Implications of Fintech Developments for Banks and Bank Supervisors. Sound Practises." Basel, Switzerland: Basel Committee on Banking Supervision.

Carney, Mark. 2017. "Building the Infrastructure to Realise FinTech's Promise." www.bankofengland.co.uk/speeches.

———. 2017. "The Promise of FinTech – Something New Under the Sun? Speech given by Governor of the Bank of England Chair of the Financial Stability Board Deutsche Bundesbank G20 Conference on Digitising Finance, Financial Inclusion And." Bank of England. https://www.bankofengland.co.uk/speech/2017/the-promise-of-fintech-something-new-under-the-sun.

"CSA BUSINESS PLAN | 2016-2019." 2019. https://lautorite.qc.ca/fileadmin/lautorite/publications/organisation/rapports-acvm/CSA-BusinessPlan-2016-2019.pdf.

DeNederlandscheBank. 2016. "More Room for Innovation in the Financial Sector." https://www.dnb.nl/en/binaries/Discussion document AFM-DNB More room for innovation in the financial sector_tcm47-345198.pdf.

———. 2017. "Regulatory Sandboxes." Toronto Centre. http://res.torontocentre.org/guidedocs/Regulatory Sandboxes.pdf.

Eley, Slavka. 2018. "RegTech and SupTech: Innovation, Risks and Opportunities." European Banking Authority.

ESMA, EBA and EIOPA 2017 "Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions"

European Banking Authority. 2017. "Discussion Paper on the EBA's Approach to Financial Technology (FinTech)." http://www.eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+%28EBA-DP-2017-02%29.pdf.

———. 2018. "The EBA's Fintech Roadmap." http://www.eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf.

———. 2019. "Guidelines on Outsourcing Arrangements." https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

European Commission. 2018. "FinTech Action Plan: For a More Competitive and Innovative European Financial Sector." Brussels, Belgium: European Commission.

European Commission. 2017. "Consultation Document - Public Consultation on FinTech: A More Competitive and Innovative European Financial Sector." https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en.pdf#disintermediating%0Ahttps://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf.

European Commission - FISMA. "Detailed Summary of Individual Responses to the 'Public Consultation on FinTech: A More Competitive and Innovative European Financial Sector,'" n.d. https://ec.europa.eu/info/sites/info/files/2017-fintech-summary-of-responses-annex_en.pdf.

Financial Conduct Authority. 2017. "Distributed Ledger Technology Feedback Statement on Discussion Paper 17 / 03." https://www.fca.org.uk/publication/feedback/fs17-04.pdf.

———. 2017. "Regulatory Sandbox Lessons Learned Report." https://www.fca.org.uk/publications/research/regulatory-sandbox-lessons-learned-report.

Financial Stability Board. 2017. "Artificial Intelligence and Machine Learning in Financial Services Market Developments and Financial Stability Implications." http://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/.

———. 2017. "Supervisory and Regulatory Issues Raised by FinTech That Merit Authorities' Attention." Financial Stability Board. http://www.fsb.org/wp-content/uploads/R270617.pdf.

———. 2017. "FinTech Credit Market Structure, Business Models and Financial Stability Implications." http://www.fsb.org/wp-content/uploads/CGFS-FSB-Report-on-FinTech-Credit.pdf.

Groepe, Francois. 2018. "The Fintech Phenomenon: Five Emerging Habits That May Influence Effective Fintech Regulation." South African Reserve Bank. April: 1–11.

Hong Kong Monetary Authority. 2016. "Fintech Supervisory Sandbox (FSS)." Guidelines and Circulars. http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160906e1.pdf.

International Association of Insurance Supervisors. 2017. "FinTech Developments in the Insurance Industry." https://www.iaisweb.org/file/65625/report-on-fintech-developments-in-the-insurance-industry.

International Organization of Securities Commissions. "Research Report on Financial Technologies (Fintech). 2017." Madrid, Spain: International Organization of Securities Commissions.

CGAP 2019. "Deposit Insurance Treatment of E-Money: An Analysis of Policy Choices"

Jesse Mcwaters, R., and R. Galaski. 2017. "Beyond Fintech: A Pragmatic Assessment of Disruptive Potential in Financial Services." Deloittes/ World Economic Forum. http://www3.weforum.org/docs/Beyond_Fintech_-_A_Pragmatic_Assessment_of_Disruptive_Potential_in_Financial_Services.pdf.

Mario Marcello. 2017. "FinTech and the Future of Central Banking: A Latin American Perspective." Speech Given at the Cambridge Centre for Alternative Finance of the University of Cambridge, Cambridge, United Kingdom, June 29.

Monetary Authority of Singapore. 2016. "Guidelines on Outsourcing." http://www.mas.gov.sg/news-and-publications/media-releases/2016/MAS-Issues-New-Guidelines-on-Outsourcing-Risk-Management.aspx

Mersch, Yves. 2018. "The Regulatory Level Playing Field." Speech Given at the Second Annual Conference on "Fintech and Digital Innovation: Regulation at the European level and beyond", Brussels, February 27

National Economic Council. 2017. "A Framework for FinTech." Washington, DC: National Economic Council.

Office of the Comptroller of the Currency. 2016. "Exploring Special Purpose National Bank Charters for Fintech Companies." Washington, DC: Office of the Comptroller of the Currency.

Prudential Regulatory Authority. n.d. "Business Plan 2018/19." Bank of England. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/pra-business-plan-2018-19.pdf.

Ravi Menon. 2016. "Singapore's FinTech Journey – Where We Are, What Is Next.", Speech Given at the FinTech Conference. Singapore, November 16

US Government Accountability Office. 2018. "Financial Technology." https://www.gao.gov/assets/700/690803.pdf.

Yoo, C., and J. Blanchette. 2015 "Regulating the Cloud, Policy for Computing Infrastructure."

REFERENCES

ACPR (Autorité de Contrôle Prudentiel et de Résolution). 2013. "Guidance: Risks Associated with Cloud Computing." https://acpr.banque-france.fr/en/risks-associated-cloud-computing.

APRA (Australian Prudential Regulation Authority). 2017. "Licensing: A Phased Approach to Authorizing New Entrants to the Banking Industry." Sydney, Australia: APRA.

APRA. "ADI Licensing: Restricted ADI Framework." https://www.apra.gov.au/file/7446

Ballard Spahr LLP. 2018. "State regulators file second lawsuit opposing OCC fintech charter." https://www.consumerfinancemonitor.com/2018/10/29/state-regulators-file-second-lawsuit-opposing-occ-fintech-charter/

Banque de France 2016. "Financial Stability Review - Digital Banking and Market Disruption: A Sense of Déjà Vu?"

Basel Committee on Banking Supervision. 2017. "Consultative Document: Sound Practices for the Management and Supervision of Operational Risk." Basel, Switzerland: Basel Committee on Banking Supervision.

BIS (Bank for International Studies). 2012. "Principles for the Sound Management of Operational Risk." https://www.bis.org/publ/bcbs195.htm

Brainard, Lael. 2017. "Where Do Banks Fit in the Fintech Stack?" Washington, DC: Board of Governors of the Federal Reserve System.

Cambridge Center for Alternative Finance. 2019. "Landscape of Peer to Peer/Marketplace Lending Presentation." Cambridge, UK: Cambridge Center for Alternative Finance.

Capgemini Research Institute. 2019 "World Payments Report".

CGAP. 2015. "Deposit Insurance for Digital Financial Products 3 Approaches."

Chinese Ministry of Finance. 2018. "Guidelines on Promoting Healthy Development of Internet Finance," Beijing, China: Chinese Ministry of Finance

Claessens, Stijn, Jon Frost, Grant Turner, and Feng Zhu. 2018. "Fintech Credit Markets Around the World: Size, Drivers and Policy Issues." Basel, Switzerland: Bank for International Studies.

Committee on Payment Clearing and Settlement. 2017. "Distributed Ledger Technology in Payment, Clearing and Settlement." Basel, Switzerland: Bank for International Settlements.

Dias, Denise. 2017. "FinTech, RegTech and SupTech: What They Mean for Financial Supervision." Toronto Centre. https://res.torontocentre.org/guidedocs/FinTech%20RegTech%20and%20SupTech%20-%20What%20They%20Mean%20for%20Financial%20Supervision%20FINAL.pdf

EBA (European Banking Authority). 2019. "Report on Regulatory Perimeter, Regulatory Status and Authorization Approaches in Relation to FinTech Activities." London, UK: EBA.

———. 2018. "Guide to Assessments of Fintech Credit Institution Licence Applications." Frankfurt, Germany: ECB.

Gates Foundation. forthcoming. Inclusive Digital Financial Services: A Reference Guide for Regulators." Seattle, WA: Gates Foundation

Hauser, Andrew. 2017. "The Bank of England's FinTech Accelerator: What Have We Done and What Have We Learned?", Speech Given at a meeting for Fintech contacts of the Bank of England's Agency for the South East and East Anglia at the offices if Mills & Reeve. Cambridge, October 2017.

HKMA (Hong Kong Monetary Authority). 2016. "Fintech Supervisory Sandbox (FSS)." Guidelines and Circulars. http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160906e1.pdf.

IMF (International Monetary Fund). 2019. "Fintech: The Experience So Far." Washington, DC: IMF.

Institute of International Finance. 2016. "RegTech in Financial Services: Technology Solutions for Compliance and Reporting." Institute of International Finance. https://www.iif.com/publication/research-note/regtech-financial-services-solutions-compliance-and-reporting.

Microsoft. 2017. "Shared Responsibilities for Cloud Computing." Redmond, WA: Microsoft.

OCC (Office of the Comptroller of the Currency). 2019. Testimony of Beth Knickerbocker, Chief Innovation Officer, Office of the Comptroller of the Currency, Before the Task Force on Financial Technology, Committee on Financial Services, United States House of Representatives. https://www.occ.gov/news-issuances/congressional-testimony/2019/ct-2019-70-written.pdf.

Ravi Menon. 2016. "Singapore's FinTech Journey – Where We Are, What Is Next.", Speech Given at the FinTech Conference. Singapore, November 16.

Tsai, Gerald. 2017. "Fintech and the U.S. Regulatory Response." San Francisco, CA: Federal Reserve Bank of San Francisco.

UNSGSA (Office of the UN Secretary-General's Special Advocate for Inclusive Finance for Development) FinTech Working Group and CCAF (Cambridge Centre for Alternative Finance). 2019. "Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech." New York: UNSGSA.

USGAO (US Government Accountability Office). 2018. "Financial Technology." https://www.gao.gov/assets/700/690803.pdf.

WBG (World Bank Group). 2018 a. "Financial Sector's Cybersecurity: Regulations and Supervision." Washington, DC: WBG.

———. 2018 b." Global Financial Development Report - Bankers without Borders." https://doi.org/10.1596/978-1-4648-1148-7.

———. 2019 a The Bali Fintech Agenda Chapeau Paper. Washington, DC: WBG.

———. 2019 b . "Evaluation of China's P2P Lending Regulatory Framework: International Comparison." Washington, DC: WBG.

WBG and University of Cambridge. 2019. "Regulating Alternative Finance: Results from a Global Regulatory Survey." Washington, DC: WBG.


WORLD BANK GROUP