FSB FINANCIAL STABILITY BOARD

Third-party dependencies in cloud services

Considerations on financial stability implications

9 December 2019

The Financial Stability Board (FSB) is established to coordinate at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations under the FSB's Articles of Association.

Contacting the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Contents

Executive summary

For decades, financial institutions (FIs) have used a range of third-party services. Many jurisdictions have in place supervisory policies around such services, which often address managing the risks associated with the use of third-party services by assigning responsibility to the FIs. Yet recently, with the adoption of cloud computing and data services across a range of FI functions, there may be new issues for authorities and financial stability that stem from the scale of services provided via the cloud and the small number of globally dominant players. This report assesses what the FSB has learned in this area to date, and sketches considerations on financial stability and avenues for international discussions going forward. It follows up on earlier analysis in this area.[1] At present, the FSB has determined that there are no immediate financial stability risks stemming from the use of cloud services by FIs.

The analysis draws on conversations with the public and private sector (banks, insurers, asset managers, cloud providers), and academics, public sources, and proprietary data. Survey data of 294 FIs of varying sizes from around the world[2] show that respondents tend to rely on a narrow set of major cloud service providers. While respondents noted using at least two providers on average, likely due to the use of different providers for different applications and for risk management purposes, the four providers identified most frequently in the survey at the global level were also the frequent providers that survey respondents separately identified in North America, Latin America, Europe, and Asia-Pacific. Some other providers were identified as regionally significant. It is worth noting, however, that these data provide no indication of the scale or criticality of FIs' reliance on cloud services and that the FSB has not analysed risk mitigation practices by FIs or cloud service providers to limit risks to firms or the financial system. Conversations with FIs suggest relatively low but increasing use of cloud services for "core" or critical systems of FIs. However, some papers highlight that at least a partial migration to the cloud may become a milestone in the digital transformation journey of incumbent FIs.

Cloud services may present a number of benefits over previous technology, such as on-premises data centres. By creating geographically dispersed infrastructures, and investing heavily in security, cloud service providers may offer significant improvements in resilience for individual institutions. They may allow institutions to scale more quickly, to deliver improved automation, and to operate more flexibly by reducing initial investment costs and freeing institutions from the replacement cycles of their own infrastructure. Cloud service providers should also benefit from economies of scale, which may result in lower costs to clients.

At the same time, there could be risks for FIs that use third-party service providers, including cloud services. Operational incidents at third-party service providers may result in temporary outages affecting FIs, and misconfigurations of new tools could result in data breaches. There may be a reduction in the ability of FIs and authorities to assess whether the service is being delivered in line with legal and regulatory obligations and the firm's risk tolerance due to contractual limitations on FIs' and authorities' rights of access, audit and information. These

---

[1] FSB (2019a), "*FinTech and market structure in finance: market developments and potential financial stability implications*", February; FSB (2017a), "*Financial stability implications from FinTech: regulatory and supervisory issues that merit authorities' attention*", June.

[2] Data originating from Forrester's Global Business Technographics® Infrastructure Survey, 2017

legal limitations may also restrict the ability of authorities to effectively access critical data held by third parties if necessary. For instance, bank resolution authorities may have difficulties when exercising step-in rights in resolution if critical bank data systems are held in third-party systems. The shared tasks, if not well articulated and understood, could lead FIs to collectively underinvest in risk mitigation and oversight. In addition, potential concentration in third-party provision could result in systemic effects in the case of a large-scale operational failure or insolvency if FIs do not appropriately manage third-party risks at the firm level. In this regard, global cloud services could pose avenues for financial stability risks similar to other significant third-party service providers.

Finally, there are a number of cross-border issues in the oversight of providers and management of systemic risks. Since the use of cloud services does not reduce the responsibility of FIs, authorities and FIs should ensure that they understand the characteristics of cloud services offered by third parties prior to any significant migration, and maintain good governance in using them. Meanwhile, the cross-border implications of data localisation rules may need to be considered too, including the importance of access to regulatory and supervisory data.

A number of existing international standards apply to outsourcing and third-party dependencies in general, and are applicable to cloud services. The standard-setting bodies (SSBs) are doing further work in this area. Going forward, further discussion among supervisory and regulatory authorities on current approaches to these issues would be constructive. In particular, there may be merit in assessing: (i) the adequacy of regulatory standards and supervisory practices for outsourcing arrangements; (ii) the ability to coordinate and cooperate, and possibly share information among authorities when considering cloud services used by financial institutions; and (iii) the current standardisation efforts to ensure interoperability and data portability in cloud environments.

1. Introduction

Financial institutions (FIs) use a wide range of third-party services. Outsourcing is not a new phenomenon for FIs, nor for the authorities that supervise them. Indeed, many jurisdictions have in place policies around outsourcing, which often underscore that outsourcing activities, functions and services does not exempt FIs from their responsibility for managing risks and meeting their regulatory obligations. International bodies have also provided guidance regarding the risks associated with third-party service providers, including on cyber risk[3] and resilience.[4] Other industry and international standards are already being applied to cloud services as well.[5] Recently, the importance of third-party service providers of cloud computing and data services to FIs has been growing rapidly.

Previous work by the Financial Stability Board (FSB) has highlighted that this growth may bring new challenges for authorities. Managing operational risks from third-party providers was one of the three issues identified in the 2017 FSB FinTech Issues Group report.[6] The FSB produced further analysis during 2018-2019 as a part of its market structure report.[7] Taken together, this work highlighted that while increased reliance on third-party providers' services may bring key benefits and reduce operational risk at the individual firm level (idiosyncratic risk), it could increase risks at the level of the financial system, particularly if third-party risks are not adequately managed at the firm level. There may be negative externalities by which each FI does not take into account the additional risk from its actions or adequately develop business continuity, contingency plans and exit strategies. The sector and authorities may collectively underinvest in risk mitigation and oversight, for example by not adequately developing the human capital to address those challenges. Particularly where concentration is high and risks are not managed appropriately at the firm level, a large-scale operational failure or insolvency of certain critical third-party infrastructure could result in system-wide disruption and systemic effects. Further, the potential scarcity of the needed technical expertise to assess the adequacy of these third-party providers' controls may raise new questions for supervisors aiming to ensure systemic stability and robust risk management techniques by FIs.

At their joint meeting in September 2018, the FSB's Standing Committee on Assessment of Vulnerabilities (SCAV) and Standing Committee on Supervisory and Regulatory Cooperation (SRC) members noted that further work is warranted to better understand the issues, including the size of such activities, concentration in the market, and benefits and risks to financial stability. Some members asked specifically for follow-up work on cross-border and regulatory perimeter issues.

---

3 G-7 (2018), "*G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*".

4 CPMI-IOSCO (2012), "*Principles for Financial Market Infrastructures*", April. See also section 5.

5 For instance, the International Organization for Standardization (ISO) has numerous standards employed by cloud service providers, including for information security management (ISO 27001), security controls for the provision and use of cloud services (ISO 27017), and measures to protect privacy for public cloud environments (ISO 27018). The NIST Cybersecurity Framework also addresses those issues.

6 FSB (2017a).

7 FSB (2019a).

In February 2019, SCAV posed further questions on the resilience of cloud infrastructure, and vendor concentration and lock-in risks.[8]

This report gives an overview of the financial stability benefits and risks of reliance on cloud services. It draws on analysis conducted over the past months, including calls and meetings with private sector speakers (from banks, insurers, asset managers and cloud providers), public sector and academic speakers, and data from public and private sources. In particular, it surveys cloud services, the current market for cloud services for FIs (based on new data), and benefits and risks, including lock-in and concentration risks and cross-border issues and the risk mitigation practices employed by FIs and cloud providers. Based on ongoing work for the FSB Standing Committee on Supervisory and Regulatory Cooperation (SRC), it also has factual information on standards and practices applicable to third-party risk.[9]

The trends in FIs' use of cloud services could lead authorities to consider new approaches to micro and macroprudential supervision of firms, infrastructures and activities. In some jurisdictions, they may also raise questions for FSB members around their approaches to third-party risk and give rise to the potential for greater cooperation between financial authorities and non-traditional partners such as those responsible for IT and security. These issues can be usefully addressed in the SRC, and in the standard-setting bodies (SSBs).

2. Types of third-party dependencies

Third-party service providers relevant to FIs can be classified according to different criteria. While the focus of recent discussions is on digital services and cloud services specifically, disruptions to other third-party services such as physical hardware, telecommunications, electricity, etc. could also trigger serious business continuity incidents. Indeed, traditional data centres could be more vulnerable to physical disruptions than newer services.

The table in the annex summarises important third-party digital services and the financial stability implications related to the adoption of these services by FIs. This includes data communications, data centre management, real time data provision, and cloud services. An important feature identified in the table is the complexity of the network of third-party dependencies. While such webs of vendor relationships have existed in the past, new interdependencies may be emerging. For instance, FIs often outsource functions like customer relationship management, human resources and financial accounting, and third-party service providers in these areas may themselves depend on cloud services. This can make identification of concentration risks, at the level of individual FIs and systemically, even more opaque.

This complexity even suggests the existence of interdependencies among third-party suppliers ("fourth parties"). FIs may thus be reliant on an aggregation or network of very disparate services, especially when FIs, through "open application programming interfaces (APIs)", are

[8] For the purposes of this report, lock-in is defined as a situation whereby a firm is unable to easily change its cloud provider either due to the terms of a contract, a lack of feasible alternative providers or technical features. See Grace A. Lewis (2012), "*The Role of Standards in Cloud Computing Interoperability*", Carnegie Mellon Software Engineering Institute, October.

[9] For an overview of national regulatory and supervisory frameworks in this area, see Hal Scott, John Gulliver and Hillel Nadler (2019), "*Cloud Computing in the Financial Sector: A Global Perspective*", July.

collaborating with start-ups that tend to rely on cloud services instead of maintaining on-premises infrastructure.

The balance of risks surrounding these third-party dependencies is complex. The failure of a key third-party provider could in theory trigger financial instability, particularly if risks are not appropriately managed at the firm level. Yet if the services of the failing provider could be transferred in a rapid and orderly fashion during stress, the financial stability impact could be significantly mitigated. In such a case, building in redundancies or interoperability for critical systems could help mitigate or transfer risks (e.g. incidents at data centres of the failing entity; obsolete systems).

Given the complexity of the network of third-party service providers, proper assessment and supervision of third-party dependencies requires highly skilled personnel at both FIs (who have primary responsibility for managing third-party risks) and at supervisory authorities. It may be challenging for both to hire and retain such talent. For small and medium-sized FIs in particular, this may also not be cost effective. The scarcity of experts in relevant risk management, customer management and legal roles could also be an issue.

3. Features of cloud services markets and models

Spending on overall enterprise software and services is growing quickly. Across all industries, Gartner estimated that global IT spending on data centres, enterprise software and services would grow at 7% per year from 2017 through 2019, reaching $1,668 billion.[10] Spending on public cloud services is growing even faster, with an expected growth rate of 17.5% in 2019. Gartner expects worldwide public cloud service revenue to grow from $182 billion in 2018 to $331 billion in 2022.[11]

In the financial services sector, spending on hardware, software, IT services and internal IT should have amounted to around $440 billion in 2018, according to IDC, and was projected to grow to nearly $500 billion in 2021.[12] In a report, Citi notes that IT expenses are already higher in the banking industry than any other (ca. 9% of revenues) and almost two to three times those of other major industries.[13] An increasing share of this spending is going to cloud services.

IDC forecasted $16.7 billion in spending on public cloud services by banks in 2018, with a five-year cumulative average growth rate of 23%.[14] This included a number of different types of cloud service models, as illustrated in table 1, ranging from infrastructure components being provided in the cloud (IaaS), to software platforms hosting client owned applications (PaaS), complete applications run in the cloud and offered as a service (SaaS) or even a suite of applications and processes managed and delivered in the cloud (BPaaS). Software as a service

---

[10] This is around twice the overall growth rate of IT spending. See Gartner (2018a), "*Gartner Says Global IT Spending to Grow 3.2 Percent in 2019*", October; FSB (2018), "*FinTech and market structure in financial services: Market developments and potential financial stability implications*", PLEN/2018/127-REV.

[11] Gartner (2019), "*Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019*", April.

[12] IDC (2018a), "*Worldwide Financial Services External and Internal IT Spending to Reach $500 Billion in 2021, According to IDC Financial Insights*", June.

[13] Citi (2018), "*The bank of the future. The ABCs of digital disruption in finance*", March.

[14] IDC (2018b), "*Worldwide Public Cloud Services Spending Forecast to Reach $160 Billion This Year, According to IDC*". "Core" or "crown jewel" systems can be understood as those systems critical for an FI's operations.

(SaaS) is the largest cloud service model in terms of revenues across all industries, but Gartner predicts that infrastructure as a service (IaaS) will have the fastest growth rate through 2021.

Alongside those four main types of deployments affecting the extent to which software and infrastructure components are used in the cloud, companies can choose how cloud services are delivered to them, with three deployment models outlined in table 2.

Table 1: Cloud service models

Service type	Infrastructure as a service (IaaS)	Platform as a service (PaaS)	Software as a service (SaaS)	Business process as a service (BPaaS)
Description	Supplies customers with IT infrastructure, provided and managed over the internet on a pay as you use basis, e.g. servers and storage	Supplies customers with an on-demand environment for developing, testing, delivering and managing software applications over the internet	Allows customers to connect to and use cloud-based apps over the internet on a subscription basis	Automated business process delivered from a cloud service. BPaaS usually has a well-defined interface which makes it easy to be used by different enterprises.
Examples	Rackspace, NYSE Euronext CMCP, Amazon AWS EC2	Microsoft Azure, Google App Engine, IBM Cloud PaaS	Microsoft Office 365, Google Docs	ADP Employease, AMEX Concur
2019 revenue forecast (Gartner)	$39 billion	$19 billion	$95 billion	$49 billion

Source: Abhinav Garg (2017), "*Cloud Computing for the Financial Services Industry*", Sapient Global Markets; Gartner (2018b), "*Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019*", September; Gartner (2019).

Table 2: Types of Deployment

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

The deployment of cloud technologies in the financial service industry is still at its initial phase, with around 70% of financial services companies reporting in a recent survey that they were only at the initial or trial and testing stage.[15] Where deployments are happening, available information suggests relatively low use of cloud services for "core" or critical systems of FIs, and in particular the so-called "crown jewel" systems and data that are essential to their business.[16] An exception is certain general business systems such as e-mail or risk-modelling that are considered critical but where the advantages of cloud deployment are seen as outweighing the risks. Some private sector contacts suggest that cloud deployment is fastest in research and development functions where computing demands are variable and high.[17] Cloud deployment is also faster in functions that are not tightly tied to legacy software systems. Various industry contacts note that cloud deployment is expanding rapidly, and they expect that a larger share of activities will be conducted in the public cloud in the future.

A small number of providers dominate the market for public cloud services. Across all industries, the top five public cloud companies earn over three-quarters of the total public cloud infrastructure revenues.[18]

In 2017, Forrester Research surveyed 294 financial services and insurance firms planning to begin or expand their use of public cloud providers. The sample firms came from a large number of jurisdictions, different areas of financial services and insurance, and a range of sizes.[19] Collectively, these firms used or planned to use 32 different public cloud providers, of which 20 were mentioned by at least 10% of respondents. This represents a degree of diversity in service providers – although the data do not give insights on which cloud services FIs used for specific functions. On average, the respondents noted using at least two providers, which may be due to the use of different vendors for different applications or for risk management purposes.[20] Overall, a large fraction of the respondents are using or plan to use the largest providers for at least some services. While the share of respondents in the sample using a service cannot be interpreted as a market share, the survey suggests that certain providers may be more important in the financial services sector than they are for the aggregate market, across all industries.

---

15 Information Age (2019), "*Financial services companies must embrace the cloud*", February.

16 For one example, see G Gangadharan and Shri Lalit Mohan (2017), "*Cloud Computing Adoption in Indian Banks – A Survey*", Institute for Development and Research in Banking Technology.

17 This and other information derives from conversations held by FSB members in meetings with the private sector . In line with the use of the Chatham House rule, statements are not attributed to individual institutions or speakers.

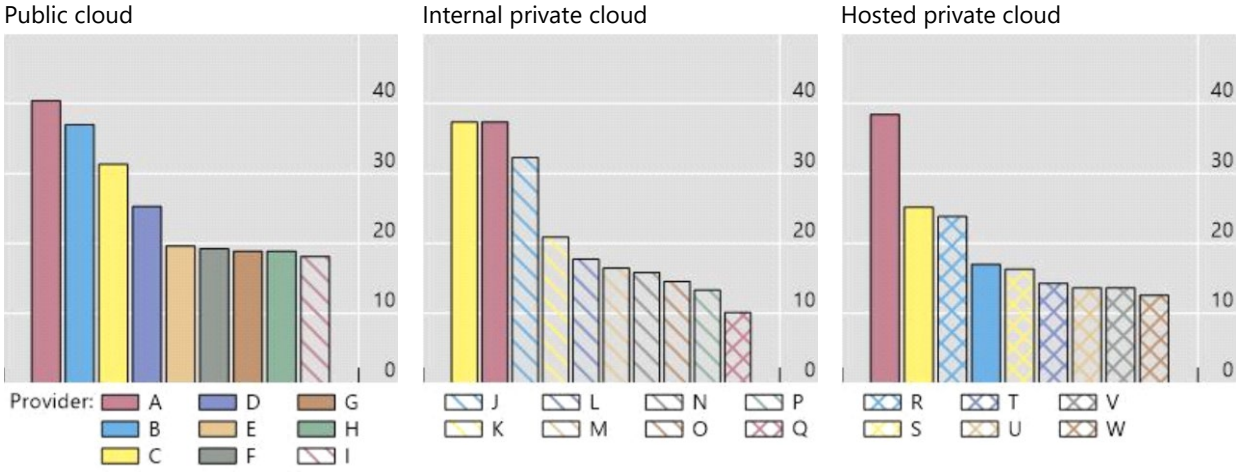
18 Synergy (2019), "*Fourth Quarter Growth in Cloud Services Tops off a Banner Year for Cloud Providers*", February; Synergy (2018), "*Cloud Revenues Continue to Grow by 50% as Top Four Providers Tighten Grip on Market*", July; and Canalys (2018), "*Cloud infrastructure market grows 47% in Q1 2018, despite underuse*", April.

19 About 44% of firms came from North America, 32% from Europe, 18% from Asia-Pacific, and 5% from Latin America. 23% had more than 20,000 employees, 31% had 5,000-20,000 employees, and 10% had fewer than 250 employees.

20 This is consistent with evidence from other sources. For instance, see Daniel Flaherty (2018), "*A Brief History of Cloud Computing and Security*", McAfee, March.

Share of FIs using or planning to use specific cloud providers[1]

In % of respondents, all regions Graph 1



[1] From a sample of 265 financial services firms (public cloud), 158 firms (internal private cloud) and 294 firms (hosted private cloud), respectively. Firms may use multiple providers, such that responses add up to more than 100%.

Source: Forrester's Global Business Technographics® Infrastructure Survey, 2017.

The dominant public cloud services have a global presence. The four providers that FIs used most identified in the Forrester survey at the global level were also frequent providers used in the North American region (116 respondents), Latin America (14 respondents), Europe (86) and Asia-Pacific (43). Some other providers were regionally significant, being identified by at least 20% of respondents in at least one region. In some jurisdictions, financial services companies rely to a greater extent on domestic providers.[21] Some of these jurisdictions have laws or regulations restricting the processing of data abroad (see section 4.2.1 below).

According to the survey, the same large providers tend to be dominant for both internal (or on-premises) private cloud and for hosted private cloud services. Again, the large providers were also dominant across regions.

The survey suggests FIs have options when it comes to cloud services, but do rely to a large extent on the same small subset of providers of cloud services. There may be a number of reasons for this phenomenon. For instance, in a conversation with FSB members, one FI contact noted that larger providers are likely to have much better security and lower insolvency risk than smaller providers. Moreover, many cloud providers apply a graduated pricing based on usage, which incentivises firms to use the cloud providers having the widest range of possible applications available to clients (e.g. in data analytics, artificial intelligence tools)

4. Potential benefits and risks

The use of cloud services from third-party providers may offer a range of benefits to FIs and the financial system, and give rise to some potential risks. This section considers these in turn.

[21] See IDBRT (2017), "*FAQs on Cloud Adoption for Indian Banks*".

4.1 Potential benefits of cloud services

Table 3 provides an overview of benefits offered when using cloud services.

Table 3: Overview of benefits of cloud services

Cost reduction	• Reduce the initial capital expenditure investment required for traditional IT infrastructure (place to store and secure data).[22] • Leverage metering capabilities to allow for increases or decreases in capacity on demand, minimising overhead on IT expenditure.[23]
Flexibility	• Access a shared pool of configurable computing resources. • Launch new innovation/business function with minimal investments in supporting systems.[24] • Shift in business focus quickly with minimal sunk costs in developing in-house data architecture.
Scalability	• Scale back office functions rapidly in response to change in business developments.[25] • Support organisational structure changes as well as the ability to absorb new data from outside sources.
Standardisation	• Uniform with multiple outside vendor systems as cloud technology has specific standards.[26] • Streamline mergers and acquisitions through compatible systems.
Security and Resilience	• Provide efficient solutions to mitigate traditional technology risks, such as capacity, redundancy, and resiliency concerns.[27] • Allow greater control in the management of variable IT demands, while offering new commercially viable methods to implement enhanced security controls.[28]

The sections hereafter focus on two categories of benefits when using cloud services: (i) cost and competition, and (ii) security and resilience.

4.1.1 Cost and competition

Cloud services may lower the barriers to entry and reduce costs in financial services. As such, entities seeking to remain competitive in the shifting financial services landscape may find compelling reasons to start moving toward a cloud-based IT architecture. By utilising cloud services, FIs may achieve cost savings by forgoing purchasing and the maintenance of certain costly IT infrastructure. Moreover, users do not have to establish costly on-premises data centres that cover peak-level computing burdens. Instead, they can use cloud services in a flexible manner so as to accommodate seasonal fluctuations in the needs for computing. The economies of scale provided by many cloud services providers may allow firms to deliver improved automation. By tapping into the flexibility typically on offer from cloud computing, firms may also support volatile workloads on-demand, and shift newly available resources

---

22 KPMG (2014), "*Cloud Economics: Making the Business Case for Cloud*".

23 IIF (2018), "*Cloud Computing in the Financial Sector Part 1: An Essential Enabler*", August.

24 Kiran Kawatra and Vikas Kumar (2014), "*Benefits of Cloud for Banking Sector*", Conference Paper at International Conference on Interdisciplinary Research and Technological Developments Vol. 5 Issue 4, pp. 16.

25 Ibid.

26 Accenture Consulting (2017), "*Moving to the Cloud, A Strategy for Banks in North America*", pp. 3-6.

27 Gartner (2017), "*Cloud Strategy Leadership*".

28 Cary Springfield, "*The Impact of Cloud Computing on the Banking Sector*",International Banker, September.

towards productive new capabilities and services for consumers. They can embark on new activities such as experiments on FinTech-type services in a swift manner.

There may be benefits for industry-wide competition. The costs and extended procurement timeframes to replace legacy IT infrastructure can delay a firm's ability to improve the quality of its services or bring new applications for consumers to market, potentially limiting the dynamism associated with digitalisation and financial technology. Small and medium-sized enterprises (SMEs) may lack the requisite capital to invest in infrastructure required to scale up new services quickly. For FinTech firms and other start-ups, cloud computing may be the only feasible option to bring new services or products to market quickly, which can potentially lower barriers to market entry and increase financial inclusion.

The flexibility and scalability as well as improved cyber security and data protection capabilities typically offered by cloud computing, in terms of the deployment and service models, provides avenues for firms and authorities to develop the necessary competence and familiarity with cloud computing.[29] By doing so, firms may opportunistically develop "cloud native" applications or migrate legacy enterprise systems to the cloud as needed. Cloud computing may also support firms' access to new artificial intelligence and machine learning services. These tools can offer predicative analytics or big data solutions to help firms manage risk more effectively, potentially benefitting financial stability.

In a study across industries, Deloitte reports an average net return of up to $2.5 for every $1 invested in cloud services, notably through an average reduction of 19% in IT capital expenditure and an average staff time savings of two to three hours per employee per week.[30] In addition, Deloitte notes that 70% of the surveyed companies have used cloud to develop new products, services or business models, to enter new markets, or to enable other product or service innovations.

4.1.2 Security and resilience

Providing resilient information technology services for a financial institution requires a technical and governance architecture that can manage risks and respond to adverse events. This includes:

- a robust IT risk oversight and governance function;
- technological features that promote resilience, including redundancy, geographic diversity and elimination of single-points-of-failure; and
- advanced incident response capabilities that protect business continuity and allow quick recovery.

From a technological perspective, large public cloud providers can often offer an IT environment that is at least as robust as the one individual FIs could create on their own premises. Economies of scale can allow cloud providers to less expensively achieve a high degree of redundancy, geographic diversity and advanced security and engineering. For example, a smaller FI that may not be able to afford to build their own redundant data centres across several geographic locations can get these benefits less expensively using public cloud

---

[29] For an overview of the deployment and service models, see Eric Simmon (2018), "*Evaluation of Cloud Computing Services Based on NIST SP 800-145*", SP 500-322, February.

[30] Deloitte (2018), "*Economic and social impacts of Google Cloud*", September.

providers. It can also take advantage of IT personnel with up-to-date skills and knowledge, improving its flexibility in preparing for and responding to new types of threats. Public cloud providers can, for example, develop proprietary hardware and software solutions that reduce software vulnerabilities discovered in off-the-shelf IT components.[31] These features are far beyond what most FIs can achieve using in-house IT.[32]

Simply moving to the public cloud does not, on its own, increase resilience, however. Risks can increase unless appropriate oversight, governance and processes are in place to promote security and resilience. In one survey, more than eight out of ten IT and security professionals reported that misconfiguration of their cloud infrastructure resulted in security and compliance incidents.[33] Limited experience and expertise with the cloud means that FIs may need to invest in additional expertise to create secure and resilient IT infrastructure in the cloud. For example, the ease of setting up services in the public cloud may encourage various business lines to deploy there without taking into account all the risks. Cross-institution coherent cloud governance processes are essential to control this risk. Public cloud providers also have limited experience managing risks for critical financial institution workloads. To address this concern, there are currently initiatives by the public cloud industry to develop codes of conduct[34] to ensure a minimum common level of commitment of cloud suppliers regarding the assurances of data protection and data portability across suppliers required to implement trustable resilience strategies using public clouds.[35]

Tasks for protecting resilience are shared and segregated in cloud infrastructure. FIs may view traditional private data centres as providing a greater degree of control and responsibility over critical IT infrastructure, despite the reality that there is always a degree of shared responsibility between FIs and third-party service providers. Public cloud arrangements explicitly require shared control and responsibility as a core feature. Clearly outlined contractual and operational responsibilities are critical to protect resilience. By identifying these responsibilities, parties can determine how information will be exchanged – both during normal times and during incidents – and how coordination will be achieved. This is not a wholly new challenge for FIs, which have experience managing risks and coordinating outsourcing arrangements of many types. But new types of complexity may be present when outsourcing critical IT processes to the public cloud. For example, FIs may have a limited ability to inspect the software and hardware that provide isolation between their applications and the applications of other cloud users. In addition, it may be difficult to test how effectively cloud providers will respond to incidents. FIs need to assess and manage these risks if the public cloud is to provide high resilience. They must also address regulators' concerns pertaining to cyber issues with respect to the use of public cloud services.[36] In addition, authorities need to develop the capacity to oversee complex arrangements with shared responsibilities for risk management.

---

31 E.g. Max Smolaks (2017), "*Google reveals details about Titan, its server security chip*", Data Centre Dynamics Ltd, August.

32 For more on the comparative advantages of BigTech firms, see FSB (2019b), "*BigTech in finance*", December.

33 Max Smolaks (2017).

34 See EU Cloud COC, "*The EU Cloud COC*" and CISPE, "The CISPE Code of conduct".

35 This is supported by the European Union's initiative: EU (2019), "*Free flow of non-personal data*", 28 May.

36 IIF (2019), "*Cloud Computing in the Financial Sector, Part 3: Could Service Provides (CPSs)*", February.

4.2 Potential risks of cloud services

While access to cloud technology may bring cost savings, improved cyber security and increased operational resilience benefits, the associated potential risks and liabilities remain with the FI.[37] Outsourcing arrangements can challenge the ability of FIs to manage risks effectively (see section 5). Moreover, some cloud providers report that they invest in explaining the shared responsibility model, but that this may not always be well understood by clients, including FIs. For instance, for a broader set of companies beyond just FIs, one recent survey found that respondents had on average at least 14 misconfigured IaaS instances running at any given time, resulting in an average of 2,269 misconfiguration incidents per month.[38] As technology advances, knowledge asymmetries between FIs, which may underinvest in the technical side of outsourcing oversight and mitigating measures, and cloud providers, may increase, further challenging the ability of FIs to maintain effective oversight, and of authorities to conduct effective supervision on regulated activities.

In some jurisdictions, cloud adoption could require FIs and relevant authorities to obtain new forms of access, audit and information rights. Any material reduction in transparency or oversight of third parties could undermine the ability of firms and authorities to effectively manage the firm's legal and regulatory obligations, risk tolerance, or contractual agreement. Undue limitations on access rights can also reduce the ability of authorities to exercise step-in rights in resolution, if critical bank data systems are held in third-party systems.

While cloud technology may offer security and operational resilience benefits, and FIs have a range of options available to minimise availability risks, temporary outages and data breaches involving FIs have occurred.[39] A significant failure at a cloud service provider is unlikely due to their high technological and physical resilience, but not impossible. Large cloud providers have reported outages affecting multiple customers and multiple locations. Technological failures rarely last long, but cloud providers could also face challenges in providing their services due to legal or financial stress. However, a number of cloud vendors have a demonstrated ability to recover in a timely manner and with little or no customer impact. Vendor insolvency may lead to a permanent loss of availability, although there may be legal obligations or other mechanisms to ensure continuity of service. Operational failure at third parties could in certain specific scenarios compromise the integrity or confidentiality of data, potentially affecting the ability to recover swiftly or resulting in large fines under data protection rules.

In concentrated markets for cloud services, these risks could be further amplified, potentially leading to system-wide disruptions or even stability risks if financial institutions were to increase their reliance on cloud technology for core operations. Both FIs themselves and authorities may not know the extent of common usage of these providers. In addition, the degree to which FIs are prepared for outages at cloud providers, caused by technical, legal or financial problems, may be unclear. In particular, firms need to assess their ability to access data and

---

37 See BCBS (2017), "*Sound practices: Implications of fintech developments for banks and bank supervisors*", August.

38 While this included sensitive information that was misconfigured to be publicly readable, it was not necessarily directly related to the running of key financial functions and thus might not affect financial stability. See McAfee (2019), "*Cloud adoption and risk report*", January.

39 See FSB (2018), pp. 22-24; Lloyds of London and Air Worldwide (2018), "*Cloud Down: Impacts on the US Economy*", Emerging Risk Report 2018, Technology.

timetables to transfer IT infrastructure from a failing provider to another cloud provider or to in-house infrastructure.

Offsetting these concerns, most cloud service providers offer solutions to address issues surrounding availability, data privacy, concentration risk, cyber security, operational resilience, and lock-in risk, which are key concerns shared by many authorities examining cloud usage in financial services.[40] Cloud service providers can allow customers to encrypt data and may recommend that they do so. However, there could still be data breaches and leakages despite such security measures put in place at cloud services level. Providers do not need to control the encryption keys providing access to data, as customers can opt to retain responsibility.

In case of failure of a financial institution highly dependent of public cloud suppliers, the existence of these suppliers could potentially both benefit and undermine the work of a resolution authority. On one side, the transformation of legacy IT systems done by the financial institution before being able of moving them to public cloud infrastructure could imply that implementation of "living will" provisions could be easier to execute during the resolution process.[41] On the other side, poorly designed public cloud solutions or weak management of supplier's Service Level Agreements lacking technical and legal provisions for extreme situations could make resolution process extremely difficult (e.g. due to legal restrictions to move sensitive data across jurisdictions).[42]

4.2.1 Implications of market concentration on competition (lock-in risks)

It may be difficult to assess the degree of concentration risk from financial institutions' use of cloud providers in some jurisdictions. Increased market concentration can mean increased pricing power and a decrease in effective competition in a market.[43] Consideration of the economic effects of these issues is primarily an issue for competition regulators. But a potentially relevant issue for financial stability is if market concentration leads to lock-in, whereby a firm is unable to easily change its cloud provider either due to the terms of a contract, a lack of feasible alternatives or technical features.

Whether lock-in affects financial stability depends first on the activity or economic function that is carried out on the cloud, as well as the scale of that activity. Lock-in could then matter in two possible scenarios:

1. If it prevents the orderly transfer of the FI's activity to another cloud provider or to the direct management of the FI in the event of the termination of the outsourcing agreement.

2. If practical and contractual arrangements undermine the FI's ability to maintain continuity of their services in the event of severe disruption at the cloud provider.

---

[40] See Slavka Eley (2017), "*FinTech and cloud in banking*", EBF cloud banking conference keynote speech, 7 December.

[41] For instance, this could be facilitated if the transformation of legacy system were fully aligned with the well-known RDARR principles, see BCBS (2013), "*Principles for effective risk data aggregation and risk reporting*", January.

[42] See Juan Carlos Crisanto, Conor Donaldson, Denise Garcia Ocampo and Jermy Prenio, "*Regulating and supervising the clouds: emerging prudential approaches for insurance companies*", Financial Stability Institute, December, FSI Insights on policy implementation No. 13, Item 49, pp.18.

[43] A.P. Lerner (1934), "*The Concept of Monopoly and the Measurement of Monopoly Power*", *The Review of Economic Studies,* Volume 1, No. 3, pp. 157–175.

One possible option to mitigate these risks is to adopt a multi-vendor approach in which services are replicated across more than one provider.[44] This may have efficiency implications, as firms may take on additional cost to run the same services. A multi-vendor approach may also magnify the risk of misconfiguration if the vendors use proprietary security standards and protocols. These considerations suggest that FIs will have to navigate numerous potential trade-off, e.g. between efficiency and resilience.

Collective efforts of cloud service providers and standards organisations may also help ensure that hosted applications and data become more easily transferable between providers. Again, depending on the services used a financial firm may be forced to trade some efficiency or innovation benefits specific to one provider in order to ensure ease of transfer.

4.2.2 Risks stemming from the cross-border dimension

Cloud computing is often compartmentalised by both geographic zones and via proprietary software. Indeed, cloud service providers try to diversify their data centres in terms of geographical location and to ensure sufficient redundancy within each centre, in order to ensure that the impact of an incident would not cause system-wide spillovers.[45] FIs remain responsible for complying with all relevant legal requirements, including risk management process, contingency planning, credit assessments and cross-sector coordination for any third-party relationship. For instance, containerisation, multi-vendor strategies, back-ups, and redundancies are relevant strategies to manage single-point-of-failure risks.

Legal challenges may arise in the cross-border provision of cloud services. For instance, there may be uncertainties over the legal obligations under foreign law of third-party service providers operating on a cross-border basis either regarding access to and use of data or to continue to provide services where the financial viability of the bank concerned is under threat. Ensuring operational continuity in resolution remains important.[46]

Some jurisdictions have imposed, or announced their intent to impose, measures that would require financial services suppliers and cloud service providers to store and process their data locally, including through measures that would require "mirroring" of data on local servers or measures that prevent cross-border data transfers. These measures may aim to protect national security, the confidentiality of client data, or supervisory access to data. They may also aim to reduce the complexity of oversight as, in the case of insolvency, access to critical data stored in another jurisdiction may only be obtained through legal assistance, which could complicate a swift and orderly liquidation or restructuring.

While authorities thus have legitimate concerns in specific cases, data localisation measures can also raise costs, create other inefficiencies (e.g. bias as data lakes may differ from one location to the other), generate weak points in the security of systems, and make it more difficult for market participants to leverage global risk management and compliance programmes.[47] Finally, some authorities have noted the need to consider how to reconcile such rules with cross-border access to regulatory and supervisory data.

---

44 See Gartner (2019), "*Why Organizations Choose a Multicloud Strategy*", May.

45 See AWS (2019b), "*Building Mission-Critical Financial Services Applications on AWS*", April.

46 For more on this, see FSB (2016), "*Guidance on Arrangements to Support Operational Continuity in Resolution*", August.

47 See Ravi Menon (2018), "*Innovation, inclusion, inspiration*", speech at Singapore FinTech Festival, 12 November.

It is critical from a financial stability perspective that financial regulators have cross-border access to information to fulfil their regulatory and supervisory mandates. Efforts to address risks associated with data localisation requirements in financial services should recognise the need for such access wherever information is stored or processed.

5. Stocktake of standards and practices applicable to third-party risk

The overall implications of the use of cloud services for financial stability will also depend on the regulatory standards and supervisory practices applicable to outsourcing and third-party risk by different public sector authorities. This section offers a brief summary overview of the SSB[48] initiatives based on their responses to a short survey questionnaire.

5.1 Guidelines covering outsourcing and third-party relationships in general

A range of international standards and high-level principles for regulated entities currently apply to outsourcing and third-party relationships. The concept of outsourcing was defined in the February 2005 paper on *Outsourcing in Financial Services* by the Joint Forum (BCBS, IAIS and IOSCO), as "a regulated entity's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the regulated entity, now or in the future".[49] This concept (or its variation), and the concept of third-party relationships or dependencies, are used in a range of other relevant work. The FSB and CPMI-IOSCO do not provide a formalised definition for outsourcing or third-party relationships, but refer to risks arising from outsourcing and third-party dependencies. For instance, the CPMI-IOSCO *Principles for Financial Market Infrastructures* (PFMI) include standards for financial market infrastructures (FMIs)[50] that outsource some operations to another FMI or a third-party service provider (including critical service providers) in the context of governance arrangements, operational risk, interdependencies, and the authorities' expectation on those critical service providers.[51] The PFMI also mention that FMIs are also typically dependent on the adequate functioning of utilities like power and telecommunications companies. IOSCO meanwhile defines "outsourcing" in its February 2005 IOSCO *Principles on Outsourcing of Financial Services for Market Intermediaries* as "an event in which a regulated outsourcing firm contracts with a service provider for the performance of any aspect of the outsourcing firm's regulated or unregulated functions that could otherwise be undertaken by the entity itself".[52] A similar notion is used in its other reports.

---

48 They are the Basel Committee on Banking Supervision (BCBS), the International Organisation of Securities Commissions (IOSCO), International Association of Insurance Supervisors (IAIS), Committee of Payments and Market Infrastructures (CPMI) and the FSB.

49 Joint Forum (2005), "*Outsourcing in Financial Services*", February

50 A financial market infrastructure is defined as a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions.

51 CPMI-IOSCO (2012).

52 IOSCO (2005), "*Principles on outsourcing of financial services for market intermediaries*", February.

The BCBS, CPMI, FSB, IAIS and IOSCO all provide guidelines that cover outsourcing in some way. The 2005 Joint Forum paper provides high-level principles for outsourcing activities that apply across the banking, insurance and securities sectors. The principles focus on establishing coherent policy and risk management programmes for outsourcing activities and recognise that a firm's senior management remains responsible for activities that are outsourced. Issues for consideration in drawing up contracts and contingency planning are also discussed. Some broad principles are also set out to help supervisors take outsourcing into account in their regular risk reviews of firms.[53]

For insurers, IAIS addresses outsourcing of material activities in its *Insurance Core Principles* (ICPs). ICP 8 (Risk Management and Internal Controls) requires insurers to maintain oversight and accountability for activities or functions that are outsourced. ICP 2 (Supervisor) requires that wherever supervisory functions are outsourced to third parties, the supervisor sets expectations, assesses their competence and experience, monitors their performance, and ensures their independence.[54]

IOSCO addresses outsourcing in a number of guidelines and various reports. For example, the February 2005 IOSCO *Principles on Outsourcing of Financial Services for Market Intermediaries* requires the firm to have full legal liability and accountability for all functions that it outsources. Its principles promote due diligence in the selection and monitoring of service providers, strong contracts, maintaining information security and business continuity, client confidentiality, and maintaining stability in case of concentration of outsourcing functions and termination.[55]

The IOSCO report on *Delegation of Functions* looks at delegation of a function to a third party, in the context of the asset management industry. It sets out general principles for such delegation of a function that could be enacted to ensure the protection of investors, that markets are fair, efficient and transparent, and reduce systemic risk. For example, the delegation of a function to a third party should be done in a manner so as not to deprive the investor and/or regulator of the means of identifying the company legally responsible for the delegated functions.[56] Precautions should be taken to mitigate against the possibility of conflicts of interest, and a collective investment scheme (CIS) operator should not systematically delegate core operations. The report also highlighted the importance of enhanced cooperation between regulators. For asset management, in the January 2017 FSB recommendations to address structural vulnerabilities from asset management activities, the FSB also recommends that authorities should have requirements or guidance for asset managers to have comprehensive and robust risk management frameworks and practices, especially with regards to business continuity plans and transition plans. Specifically, the recommendation asks asset managers to consider operational risks or challenges when providing services to other market participants or when relying on third-party services themselves.[57]

---

53 Joint Forum (2005).

54 IAIS (2018), "*Insurance Core Principles*", November.

55 IOSCO (2005).

56 IOSCO (2000), "*Delegation of functions*", December, Principle 1.1.

57 FSB (2017b), "*Policy Recommendations to Address Structural Vulnerabilities from Asset Management Activities*", January, Recommendation 13.

The IOSCO *Principles on Outsourcing by Markets* set out the factors that markets (exchanges) should consider when deciding whether, and to whom, to outsource processes, services or functions. The principles also aim to assist market authorities in their oversight of these arrangements.[58] IOSCO has also issued other guidelines covering outsourcing by regulated entities. For example, its December 2015 report on the *Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity* sets out a number of sound practices to address risks arising from outsourcing, in particular in relation to critical systems. [59]

As for FMIs, the CPMI-IOSCO PFMI provide, among other requirements, that an FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations.[60] An FMI that relies upon or outsources some of its operations to another FMI or a third-party service provider (e.g. data processing and information systems management) should ensure that those operations meet the same requirements they would need to meet if they were provided internally. The FMI should have robust arrangements for the selection and substitution of such providers, timely access to all necessary information, and the proper controls and monitoring tools. The PFMI notes that some service providers may be critical (e.g. those that generate environmental interdependencies such as financial messaging providers) and states that "a contractual relationship should be in place between the FMI and the critical service provider allowing the FMI and relevant authorities to have full access to necessary information".[61] The contract should ensure that the FMI's approval is mandatory before the critical service provider can itself outsource material elements of the service provided to the FMI, and that in the event of such an arrangement, full access to the necessary information is preserved. These guidelines help to promote regular and strong communication between FMIs and critical service providers. An FMI that outsources operations to critical service providers should also disclose the nature and scope of this dependency to its participants, and the FMI should inform its relevant authorities about any such dependencies on critical service providers and utilities, and take measures to allow these authorities to be informed about the performance of these critical service providers and utilities.[62] CPMI and IOSCO have also published a set of oversight expectations for critical service providers.[63]

Finally, the FSB offers Guidelines to help authorities and firms to evaluate whether firms that are subject to resolution planning requirements have appropriate outsourcing arrangements in the case that a firm enters resolution.[64] For this, the FSB defines a critical shared service as "an

---

58 IOSCO (2009), "*Principles on Outsourcing by Markets*", July.

59 IOSCO (2015), "*Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity*", December.

60 CPMI-IOSCO (2012), Principle 17, Key consideration 7.

61 CPMI-IOSCO (2012), 3.17.20.

62 CPMI-IOSCO (2012), 3.17.21.

63 See CPMI-IOSCO (2012), Annex F. For example, a critical service provider is expected to identify and manage relevant operational and financial risks to its critical services and ensure that its risk-management processes are effective. For details, see CPMI-IOSCO (2014), "*Assessment methodology for the oversight expectations applicable to critical service providers*", December.

64 FSB (2016).

activity, function or service is performed by either an internal unit, a separate legal entity within the group *or an external provider"*[65] to help evaluate which services are critical.

5.2 Guidelines that cover cloud services

At present, only the BCBS has published sound practices on outsourcing or third-party relationships that are dedicated to cloud services. In its report *Sound Practices on the implications of fintech developments for banks and bank supervisors*, the BCBS noted that banks that use technologies like cloud computing should ensure that they have effective governance structures and risk management processes, and supervisors should ensure that banks adopt risk management processes and control environments.[66] The CPMI-IOSCO's PFMI do not specifically provide standards for cloud services. However, since the PFMI are principle-based, the above guidelines on outsourcing and third-party relationships also apply to FMIs' cloud outsourcing where relevant.[67] IOSCO has not issued reports that are dedicated to cloud services but has issued reports that de facto address risks arising from cloud services. For example, its December 2015 report on the *Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity* specifically identifies data centres as a critical system that may be outsourced and provides some sound practices. The FSB does not have specific guidelines related to cloud outsourcing, but has published analysis of the financial stability implications of third-party dependencies.[68] IAIS does not provide specific guidance.

5.3 Current and future work on outsourcing, third-party relationships and cloud services

A number of specific or indirectly related initiatives are currently underway for outsourcing, third-party relationships and cloud services at SSBs. In June 2019, the BCBS agreed to conduct further work on financial technologies, including work related to banks' dependencies on unregulated third parties and the implications for existing supervisory regimes for outsourcing. CPMI does not have any plans to issue further guidelines on outsourcing and cloud outsourcing. CPMI and IOSCO continue to encourage FMIs to strengthen their cyber resilience, which includes monitoring third-party relationships.

IAIS is currently working on the supervision of control functions with respect to insurers, which might include issues related to outsourcing of control functions. It is also considering work on a best practices paper related to insurers' reliance on and exposure to specialist technology providers, in which cloud providers might be included.

The IOSCO Board has approved a mandate for work on the risks associated with the use of third-party service providers and updating the IOSCO principles on outsourcing in light of recent developments. In this regard, a working group has been established in the context of

---

65 FSB (2013), "*Guidance on Identification of Critical Functions and Critical Shared Services*", July.

66 BCBS (2018) "*Sound Practices: implications of fintech developments for banks and bank supervisors*", January.

67 Similarly, the June 2016 CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures provides supplemental guidance to the PFMI on cyber risk, in particular addresses risk in relation to data, interconnections with service providers and outsourcing. See CPMI-IOSCO (2016), "*Guidance on cyber resilience for financial market infrastructures*", June.

68 FSB (2017a); FSB (2019a).

secondary markets, market intermediaries, credit rating agencies and derivatives. It is: developing a report that will address recent trends in the use of outsourcing and third-party service providers; updating IOSCO's principles on outsourcing, where appropriate; and considering the application of those principles in cases where regulated entities outsource critical services or material activity to unregulated third-party service providers. This work has also looked specifically at the cloud and associated IT developments as well as vulnerabilities.

Finally, the FSB is currently working on developing effective practices relating to a financial institution's response to, and recovery from, a cyber incident, that include firm's relations with third party service providers.[69]

6. Implications

Going forward, a discussion among supervisory and regulatory authorities on current approaches to these issues would be constructive. In particular, the following three areas could benefit from further work:

(i) on existing regulatory standards and supervisory practices for outsourcing arrangements, and whether there is a need to further assess the systemic dimension of risks in FIs using public cloud services and, if appropriate, for SSBs to update current frameworks. This task is currently being addressed by SRC;

(ii) on exploring possibilities for better coordination and cooperation and information-sharing among authorities when considering cloud services used by FIs;

(iii) on standardisation efforts to ensure interoperability and data portability in cloud environments (e.g. by examining further initiatives by key organisations such as ITU-T, NIST, ISO/IEC) and the role authorities could have in relation to this ongoing work.

[69] See FSB (2019a).

Glossary

This glossary defines terminology used in this report. Where available, definitions are aligned with previous reports of the FSB, the Basel Committee on Banking Supervision (BCBS), BIS Committee on the Global Financial System (CGFS), Committee on Payments and Market Infrastructures (CPMI), Financial Action Task Force (FATF), BIS Markets Committee (MC) and International Organization of Securities Commissions (IOSCO), as summarised in the glossary of the Economic Consultative Committee (ECC) ad hoc group on digital innovation. Some definitions are drawn from the US National Institute of Standards and Technology (NIST).

- **Business process as a service (BPaaS):** automated business process delivered from a cloud service. BPaaS usually has a well-defined interface which makes it easy to be used by different enterprises.
- **Cloud computing:** an innovation in computing that allows for the use of an online network ('cloud') of hosting processors so as to increase the scale and flexibility of computing capacity.
- **Disaster recovery as a service (DRaaS)**: a cloud computing and backup service model that uses cloud resources to protect applications and data from disruption caused by disaster. It gives an organisation a total system backup that allows for business continuity in the event of system failure.
- **Hybrid cloud:** services combining public and private cloud resources, with technology allowing data and applications to be shared between them.
- **Infrastructure as a service (IaaS):** model of cloud service where customers are supplied with IT infrastructure, provided and managed over the internet on a pay as you use basis, e.g. servers and storage.
- **Outsourcing:** a regulated entity's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the regulated entity, now or in the future.
- **Platform as a service (PaaS):** model of cloud service where customers are supplied with an on-demand environment for developing, testing, delivering and managing software applications over the internet.
- **Private cloud:** services in which computing resources are used solely by one single organisation, either physically in the company's on-site data centre(s) ("on-premises") or externally with the third-party provider ("hosted private cloud"). In both scenarios, services are not accessible or even publicly visible over the internet.
- **Public cloud:** services, including general computing and/or software resources, offered by a third-party provider over the public internet. Whilst these services are generally available to any entity willing to subscribe to them, access control functions ensure the proper usage of the services by the legitimate entity under a contractual agreement with the third-party provider.

- **Resilience:** the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
- **Scalability:** the measure of a service's capacity to increase or decrease in performance in response to changes in volumes, or general computing or network needs.
- **Service level agreement (SLA):** a contractual agreement between a company and a service provider defining the shared responsibilities, the level of service, priorities, and guarantees regarding timing, availability, performance, and other key aspects of the service delivered.
- **Software as a service (SaaS):** model of cloud service allowing customers to connect to and use cloud-based applications over the Internet on a subscription basis.
- **Vendor lock-in**: a situation whereby a firm is unable to easily change its cloud provider either due to the terms of a contract, a lack of feasible alternative providers or technical features.

List of contributors to the report

Workstream lead	**Vichett Oung** Deputy Director, Financial Stability Directorate Banque de France
Australia	**Darren Flood** Deputy Head, Financial Stability Department Reserve Bank of Australia
Canada	**Joshua Slive** Senior Policy Advisor Bank of Canada
China	**Mu Changchun** Deputy Director-General, Payment System Department People's Bank of China
Japan	**Norio Hida** Associate Director General, Payment and Settlements Systems Bank of Japan
Korea	**Juyoung Kim** Economist, Financial Stability Research Division Bank of Korea
	Jin-Soo Lee Director, International Finance Division, Financial Policy Bureau Financial Services Commission
Netherlands	**Maarten Willemen** Senior Policy Advisor, Financial Stability Division De Nederlandsche Bank
Russia	**Iuliia Burkova** Consultant, Financial Stability Department Central Bank of the Russian Federation
Spain	**César Pérez-Chirinos** Technology and Innovation Adviser General Secretariat of the Treasury and Financial Policy Ministry of Economy and Finance
	Marta Barón FinTech Technical Adviser General Secretariat of the Treasury and Financial Policy Ministry of Economy and Finance
	Sergio Gorjón Head of Unit, Financial Innovation Bank of Spain

UK	**Chris Ford** Policy Analyst Bank of England
	Orlando Fernández Ruiz Senior Technical Specialist Bank of England
	Steven McWhirter Technical Specialist Financial Conduct Authority
US	**David Mills** Associate Director Board of Governors of the Federal Reserve System
	Melissa Leistra Lead Financial Institution Policy Analyst Board of Governors of the Federal Reserve System
	Dan Greenland Deputy Director, Office of International Financial Markets U.S. Department of the Treasury
	Beth Caviness Officer, Markets Group Federal Reserve Bank of New York
	Robert Peterson Senior Advisor, International Affairs Office for Financial Research
ESMA	**Patrick Armstrong** Senior Risk Analysis Officer, Innovation and Products Team European Securities and Markets Authority
FSB secretariat	**Jon Frost** (until August 2019) Member of the Secretariat
	Joseph Noss Member of the Secretariat
	Alexandre Stervinou Member of the Secretariat

With thanks to Yasushi Shiina, Karen Gallagher-Teske and José Maria Vidal Pastor.

Annex: Digital services and financial stability

Dependencies, adoption status and potential benefits and risks of reliance on third parties

(Legend: ---, --, -, =, +, ++, +++ represent a qualitative assessment, from large decrease to large increase, of benefits or risks to FIs as result of outsourcing the corresponding digital service)

Third Party Digital Service					Benefits for FIs			Risks for FIs			Benefits for the financial system as a whole			Risks for the financial system as a whole	
Type	Subtype	#	Direct dependencies from #	Adoption status[70]	CAPEX Savings	OPEX Savings	IT Experts Savings	Cross Border	Loss of Knowledge	Supplier lock-in	Increased resilience	Efficiency Gains	Quick Access to Disruptive Technology	Concentration	Loss of Risk Understanding
Data communications	Backbone grade	1	6	Large FIs	N/A	+	N/A	=	N/A	=	+	++	+	+	N/A
	Internet traffic, voice over IP & VPN	2	1, 6	All FIs	N/A	N/A	N/A	=	N/A	=	N/A	N/A	N/A	N/A	N/A
Data centre hardware management	Mainframes	3	2	Most FIs	+	++	++	+	++	++	=	++	++	++	+++
	Mid-range servers	4	2	Some FIs	+	++	++	+	++	++	=	++	+++	++	+++
	Storage	5	2	Some FIs	+	++	++	+	++	++	=	++	+++	++	+++
Networking hardware management	Firewall & ciphering	6	2	All FIs	+	++	++	++	++	++	+	+++	+++	++	+++
Cloud computing	Infrastructure as a Service (IaaS)	7	2	Most FIs[71]	++	++	++	+	+++	++	+	++	+++	++	+++

[70] This column has been introduced as a qualitative proxy for the % of financial institutions already adopting it.

[71] It must be noted that a large number of FIs are still in testing/trial status of IaaS adoption, sometimes due to regulatory or supervisory uncertainty

Third Party Digital Service					Benefits for FIs			Risks for FIs			Benefits for the financial system as a whole			Risks for the financial system as a whole	
Type	Subtype	#	Direct dependencies from #	Adoption status[70]	CAPEX Savings	OPEX Savings	IT Experts Savings	Cross Border	Loss of Knowledge	Supplier lock-in	Increased resilience	Efficiency Gains	Quick Access to Disruptive Technology	Concentration	Loss of Risk Understanding
Software as a Service	Platform as a service (PaaS)	8	2	Early adopters	++	++	++	+	+++	++	+	+++	++	++	+++
	Disaster recovery as a service (DRaaS)	9	2, 7, 8	Early adopters	++	++	++	+	+++	++	+	+++	++	++	+
	IT management as a service	10	2, 7	Early adopters	++	++	++	+	+++	++	+	++	=	++	+
	Core banking software	11	2, 8	Some FIs, many neo-banks	++	++	++	+	+++	++	-	++	++	++	+++
	CRM	12	2, 8	Many FI	++	++	++	+	+++	++	-	++	+++	++	+
	Credit scoring	13	2, 8	Early adopters	++	++	++	+	+++	++	-	++	+++	++	+++
	Credit recovery	14	2, 8	Early adopters	++	++	++	+	+++	++	-	+	++	++	+
	Other	15	2, 8	Early adopters	++	++	++	+	+++	++	-	++	++	++	+++
Other commodity, cloud hosted services	Mobile app stores	16	2, 8	Mandatory in practice	N/A	N/A	N/A	+	N/A	++	-	N/A	N/A	++	+++
	Denial of service attacks protection	17	2, 8	Many FIs	+++	++	++	N/A	++	++	++	+++	+++	++	+++
	Non-transactional web hosting	18	2, 8	Many FIs	++	++	++	+	++	++	++	+++	=	+	++

Third Party Digital Service					Benefits for FIs			Risks for FIs			Benefits for the financial system as a whole			Risks for the financial system as a whole	
Type	Subtype	#	Direct dependencies from #	Adoption status[70]	CAPEX Savings	OPEX Savings	IT Experts Savings	Cross Border	Loss of Knowledge	Supplier lock-in	Increased resilience	Efficiency Gains	Quick Access to Disruptive Technology	Concentration	Loss of Risk Understanding
	Automated analytics (big data)	19	2, 8	Early adopters	+++	+	++	++	++	++	--	+++	+++	++	+++
	Generic artificial intelligence services	20	2, 8	Early adopters	+++	++	++	++	++	++	--	+++	+++	+++	+++
	Market sentiment analysis	21	2, 8	Early adopters	++	+++	++	+	++	++	--	+++	+++	+++	+++
	Social media monitoring	22	2, 8	Early adopters	++	+++	++	+	++	++	--	+++	+++	+++	+++
Real time data provision	Market Data Feeds	23	2, 8	Almost all FIs	N/A	N/A	N/A	+	N/A	++	--	+++	+++	++	+++