CLOU D COMPUTING: ISSUES FOR SUPERVISORS

N O V E M B E R 2 0 2 0
# CLOUD COMPUTING: ISSUES FOR SUPERVISORS

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>2</td>
</tr>
<tr>
<td>Benefits of cloud computing</td>
<td>4</td>
</tr>
<tr>
<td>Supervisory concerns</td>
<td>6</td>
</tr>
<tr>
<td>Risks at the level of individual institutions</td>
<td>6</td>
</tr>
<tr>
<td>Risks at the system level</td>
<td>8</td>
</tr>
<tr>
<td>Challenges faced by supervisors</td>
<td>9</td>
</tr>
<tr>
<td>Risks of not using cloud computing</td>
<td>10</td>
</tr>
<tr>
<td>Regulatory and supervisory responses</td>
<td>10</td>
</tr>
<tr>
<td>Responses by international standard setting bodies (SSBs)</td>
<td>10</td>
</tr>
<tr>
<td>Regional-level responses</td>
<td>11</td>
</tr>
<tr>
<td>Country-level regulatory responses</td>
<td>12</td>
</tr>
<tr>
<td>Country-level supervisory responses</td>
<td>13</td>
</tr>
<tr>
<td>Regulate cloud providers?</td>
<td>14</td>
</tr>
<tr>
<td>Next steps for supervisors</td>
<td>16</td>
</tr>
<tr>
<td>Taking immediate steps</td>
<td>16</td>
</tr>
<tr>
<td>Establishing a sound basis for the supervision of cloud computing outsourcing</td>
<td>17</td>
</tr>
<tr>
<td>Conclusion</td>
<td>21</td>
</tr>
<tr>
<td>References</td>
<td>22</td>
</tr>
</tbody>
</table>
Introduction

In recent years, financial institutions in both advanced economies and emerging markets and developing economies (EMDEs) have increasingly been adopting cloud computing through outsourcing arrangements with cloud computing service providers (CSPs).

Cloud computing creates a range of opportunities and benefits for financial services, but it also carries risks for individual institutions and for the financial sector. Outsourcing, including of data processing and storage, is a familiar arrangement for many financial institutions and their supervisors. However, cloud computing raises unique concerns. One difference is that institutions may lose physical access to the stored data and its processing, which are controlled by CSPs.² Using the cloud increases the number of potential points of failure, while the location and conditions of data are not necessarily known or determined by the financial institution. CSPs use geographically dispersed infrastructure with regional or global distribution, and they service both financial and non-financial sectors, challenging traditional audit and risk assessment methods.

This Toronto Centre Note contrasts the observed and potential benefits of cloud computing outsourcing with the supervisory concerns that its growth raises, particularly from the perspective of EMDE supervisors. It discusses the regulatory and supervisory responses and highlights next steps for supervisors.

Cloud computing

Financial institutions are developing approaches to cloud computing as part of their broader technology and business strategies where the cloud is both (a) central to meeting client expectations for seamless, immediate, and personalized services, which in turn requires cloud-enabled infrastructure, and (b) the natural next step as firms go through their regular technology upgrade cycle.³

Although still an emerging practice when compared to prevailing IT architecture, there is little question that cloud computing will become commonplace and may eventually substitute for current practices. Many institutions, including internationally active banks, have already started to implement a cloud-first approach, where deploying on-premises, proprietary IT resources becomes an exception. New challenger institutions tend to take a cloud-only approach, where investing in proprietary IT infrastructure is not even considered.

With the outbreak of COVID-19, the cloud has enabled firms across the globe to shift swiftly to work-from-home arrangements, ensure cross-border services, deal with sudden increases in volatility and transaction volumes, and continue to provide customer services. The pandemic

¹ This Toronto Centre Note was prepared by Denise Dias.
² World Bank (2019).
has shown the value of the cloud for continuity and resilience. The pandemic has accelerated digitization in which the cloud is a fundamental building block.⁴

### Cloud computing services and providers

Cloud computing is the use of an online network of hosting processors to increase the scale and flexibility of computing capacity. It is enabled by virtualization technologies that allow CSPs to segregate and isolate multiple clients on a common set of physical or virtual hardware. It enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example networks, servers, storage, applications, and services) that support a range of platforms (for example mobile devices and workstations). Multiple customers share the same physical resources, but their data and other resources (for example applications) are kept separate. Financial institutions may adopt a combination of deployment models and services.

Source: Basel Committee (2018)

Cloud deployment models are:

**Private cloud** – infrastructure for the exclusive use by a single institution, either on-premises or off-premises when hosted by a CSP (Virtual Private Cloud). It may be owned and managed by the institution or by the CSP.

**Public cloud** – cloud infrastructure available for public use. Multiple clients share the same infrastructure concurrently, with different levels of segregation depending on the service.

**Hybrid cloud** – cloud composed of two or more cloud infrastructures that operate as a single entity by using standardized technology. Data and applications can move between private and public platforms.

**Community cloud** – cloud infrastructure for the exclusive use of a specific group of institutions.

---

⁴ Institute of International Finance (2020).
Supervisors should understand how cloud computing services and CSPs function in their jurisdictions and globally to determine appropriate responses. Prohibiting cloud computing outsourcing or not reacting at all are inadequate responses. At the international level, more coordination is needed to help avoid regulatory and supervisory inconsistency, particularly with regard to global CSPs servicing multiple jurisdictions. Balanced and informed regulatory and supervisory adaptation is needed. While complex questions remain, responses at the national and international levels should be based on the appreciation of the fundamental role cloud computing will continue to play in financial services.

Benefits of cloud computing

The benefits of cloud computing include expediting processes, enabling fast and safe scalability, increasing efficiency, lowering costs, reducing some risks, enhancing operational resilience, and improving profitability. It also has relevance for financial inclusion and gender equality because the cloud drives institutional diversity and competition by dramatically lowering entry barriers. Even the smallest institution can have access to state-of-the-art IT resources that would otherwise be possible only for deep-pocketed institutions. The cloud is behind innovative, customer-centric product and service delivery design by making big data analytics available to firms without the required computer processing power, and by enabling data sharing schemes such as open finance. Cloud computing is therefore fundamental to data-powered financial innovation and inclusion.

By pooling third-party resources and, to a certain degree, commoditizing IT outsourcing through fairly standardized contracts, cloud computing leads to efficiency gains and cost reductions. In addition to efficiency gains, individual institutions can also increase flexibility in terms of scale, scope, and data accessibility and availability. The various configurations of on-demand cloud services enable institutions to ramp up their data analytics capacity to support innovation – such as by using cloud-based big data analytics. Advanced analytics used for product design can be coupled with mobility and agility in service delivery, avoiding investing in in-house analytical capacity prior to proving the viability of a new product or service.
By lending processing power to firms of any size and business model, cloud computing also supports institutional diversity and increases contestability, leading to greater competition. New entrants, regardless of size, can use CSPs’ computing powers, paying according to usage level. In competitive terms, this is unprecedented. Size and mainframe power are no longer an entry barrier nor a competitive advantage.

Cloud computing can also improve risk management and contingency arrangements, by improving the management of data and cyber security risks. Large CSPs can reduce risk by pooling resources and heavily investing in data and cyber security defenses. Their capacity is often unmatched by individual financial institutions. Global CSPs have the ability to learn from threats at the global level and update their defenses accordingly.

The risk-reducing potential of the cloud is derived from its distributed nature since data centers are located in multiple countries and the data of a client may be distributed across different locations. This enables institutions to sustain operations through major disruptions. During the COVID-19 pandemic, not only could operations and staff quickly go remote, but also institutions were able to avoid losses by shifting customers to digital transactions. Cloud computing can increase security and resilience and can improve business continuity arrangements.5

<table>
<thead>
<tr>
<th>Public cloud</th>
<th>Community cloud</th>
<th>Private cloud</th>
<th>Hybrid cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost-saving: organisations pay only for the services they use</td>
<td>Cost-effectiveness: organisations share costs of a private cloud model for specific community needs.</td>
<td>Increased flexibility: computing resources are customised according to the organisation’s IT requirements</td>
<td>Cost-effectiveness: organisations pay for extra computing resources only when necessary</td>
</tr>
<tr>
<td>Virtually unlimited scalability: computing resources are available according to demand</td>
<td>High scalability: computing resources are available according to demand</td>
<td>High scalability: computing resources are available according to demand</td>
<td>Flexibility: additional resources of the public cloud may be available on demand</td>
</tr>
<tr>
<td>High reliability: business continuity supported by vast network of servers</td>
<td>Tailored security: security levels according to community needs.</td>
<td>High and tailored security: high control and security levels since resources are not shared</td>
<td>Control and security: organisations can maintain a private cloud for sensitive assets</td>
</tr>
<tr>
<td>Agility and availability: reduced time-to-market and fast implementation</td>
<td></td>
<td>Risk-averse: provides data preservation during an outage</td>
<td>Risk-averse: provides data preservation during an outage</td>
</tr>
</tbody>
</table>

Source: FSI staff.

---

Supervisory concerns

Risks at the level of individual institutions

Cyber risks
Outsourcing to CSPs can increase the risk of cyber incidents and data leakages, and can pose security and governance challenges for financial institutions’ internal controls and data management, especially during the integration with legacy systems (which require specialized expertise that some financial institutions may lack). These risks could, in turn, lead to compliance, legal, and reputation risks. Depending on the scope of the services and the type of data involved, CSPs and sub-contracted firms may be storing, processing, and managing sensitive data across geographically dispersed computing infrastructures.

The level of risk is largely determined by the ability of the CSP to protect the confidentiality, integrity, and availability of data and of the systems and processes that are used to process, transfer, or store these data. The increasing level of abstraction and opaqueness as services move from IaaS toward SaaS can inhibit effective risk management. Subcontracting by CSPs (a common practice) could increase the risks, and the security risk management capability and practices across CSPs vary substantially. Traceability of operations is key in this context, but not always guaranteed. The table below summarizes the main security risks in cloud computing.

<table>
<thead>
<tr>
<th>Examples of cloud computing security risks</th>
<th>Table 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy and organisational</td>
<td></td>
</tr>
<tr>
<td>Lock-in</td>
<td>Clients that rely strongly on the services of one cloud provider may experience severe difficulties if migrating to another provider or back to an in-house IT environment.</td>
</tr>
<tr>
<td>Loss of governance</td>
<td>Control is ceded by the client to the cloud provider regarding cloud infrastructure and other issues that may affect security.</td>
</tr>
<tr>
<td>Supply chain failure</td>
<td>If a cloud provider outsources parts of its production chain to third parties, or uses services of another cloud provider, potential for cascading failures may be created.</td>
</tr>
<tr>
<td>Technical</td>
<td></td>
</tr>
<tr>
<td>Isolation failure</td>
<td>Failures, errors or attacks in shared environments may lead to situations where one tenant has access to another tenant’s resources or data.</td>
</tr>
<tr>
<td>Malicious insider</td>
<td>Various kinds of damage may be caused to a consumer’s assets if an insider at the cloud provider abuses a high-privilege role.</td>
</tr>
<tr>
<td>Management interface compromise</td>
<td>To manage and interact with cloud services, clients use application programming interfaces (APIs) that are internet-accessible, which may increase their exposure to attacks.</td>
</tr>
<tr>
<td>Insecure or ineffective deletion of data</td>
<td>Given the clients’ reduced visibility of the physical location of data, as well as reduced ability to verify complete data deletion, a client’s information may not be completely deleted from all cloud providers’ resources.</td>
</tr>
<tr>
<td>Legal</td>
<td></td>
</tr>
<tr>
<td>Data protection</td>
<td>Clients may experience difficulties in checking compliance of cloud providers to data protection legislation since data may be processed and stored in different locations and even between different clouds.</td>
</tr>
</tbody>
</table>

Source: ENISA.


---

6 European Banking Authority (2019).
7 Australian Prudential Regulatory Authority (2018).
Institutions’ ability to assess and manage risks
There is an asymmetry in bargaining power between even the largest financial institutions and large CSPs. Compared with other outsourcing, CSP contracts are more standardized to allow the provision of services at large scale and across borders. There may be little scope to change terms and conditions. The ability of financial institutions to customize cloud contracts, set conditions for service delivery (for example data location and business continuity tests), and conduct due diligence and audits may be more limited than in other outsourcing.

Less sophisticated financial institutions may lack the technical capacity to conduct due diligence and audit CSPs, and to fulfill their roles in the cloud’s shared responsibility model. They may not be in a position to effectively identify, assess, mitigate, and monitor the risks related to cloud computing outsourcing. Moreover, the multi-tenant and distributed nature of CSP facilities creates practical issues for traditional audit methods such as vulnerability assessments, penetration tests, access to audit logs, and activity monitoring. To complicate matters further, subcontracting is pervasive, and financial institutions may not have a say in how and where it happens. An institution may not know, when signing a cloud computing services agreement, how many physical facilities will be used, when, and where. And they may have no option other than to terminate the contract if they disagree with subcontracting or other changes in the service provision.

Dependency risk
Financial institutions can become dependent on CSPs. The more financial institutions rely on outsourced parties, the less control they have over risk management and on the outcomes of the decisions taken by third parties. CSPs may not offer full transparency on how risks are managed and how outsourced and sub-outsourced tasks are conducted. In addition to cloud computing, CSPs may be providing other services to an institution such as big data analytics and machine learning, which could be central to their business strategy. By combining outsourcing of multiple valuable or potentially critical services, CSPs may become difficult to substitute, becoming a source of concentration risk. (Re)absorbing the outsourced activities may not be an option, as financial institutions may lack comparable capacity, infrastructure, and expertise.

Vendor lock-in risk
There is a clear risk of vendor lock-in due to technical challenges to port data and applications and due to the specialized nature of the services. These concerns depend on various factors, such as the asymmetry of power between the financial institution and the CSP, the quality of the CSP’s risk management, the type of cloud services provided, the nature of the data, and the legal and regulatory framework. Cloud computing has not yet reached a point where any application can be run on any cloud and seamlessly migrate from the private to public cloud and from one CSP to another. Portability of data and applications is not technically easy and can be a source of operational and cyber risks. As a result, financial institutions may have limited options in the event of a disruption at a CSP. This could have consequences for business strategy, business continuity, and recovery planning.

---

8 IOSCO (2020) and Financial Stability Board (2020b) both mention this issue.
10 This issue of multiple dependencies on CSPs was noted by Beau (2018).
11 Large institutions may be able to mitigate concentration risk diversification through a multi-vendor approach. For example, HSBC uses three of the global CSPs for key cloud computing outsourcing – AWS, Microsoft, and Google.
The Financial Stability Board (FSB 2019a) notes that it is an open question whether the cloud materially changes risks such as lock-in and concentration risks, compared to existing data centers and services. Nevertheless, financial institutions may be unable to devise effective exit strategies from cloud computing outsourcing. Some emerging techniques (for example containerization\(^\text{12}\)) could address the portability problem and increase operational resilience. The FSB (2020b) highlights supervisors’ growing focus on the development and testing of business continuity plans and exit strategies for third parties, as well as adequate management of vendor lock-in and related risks.

**Risks at the system level**
In addition to the risks to individual institutions, complex supervisory questions arise at national and global levels. The concentration of cloud computing outsourcing on a few CSPs and the cross-border provision of cloud services creates complexities related to data sovereignty, data protection, supervisory perimeter, scope, and coordination, and the regulatory treatment of CSPs. Without a collaborative effort between home and host countries and a degree of international coordination, responses to cloud computing outsourcing could result in inconsistencies and loopholes that could diminish the positive contributions of cloud computing and even increase its risks.

**Data sovereignty**
Data sovereignty and legal risks emerge in cross-border cloud computing. Most of the largest global CSPs are US-based companies. Arguably, US national security laws provide the US government the right to access data handled by US companies, regardless of where the data are stored, including the data of foreign citizens. While this is debatable, such access may not require prior notification or agreement with the host supervisor. The law could also allow the US government to limit access to the data, and/or block data release to a supervisor, on national security grounds. Such situations could have major consequences for the business continuity of financial institutions, audits, and investigations. Smaller countries and EMDEs may be in a precarious position to negotiate agreements with the US on this matter.

**Concentration risk**
At the national and global level, the concentration of cloud computing outsourcing on a few CSPs introduces stability concerns. When existent and relevant, domestic CSP markets replicate the picture. The handful of dominant global CSPs are often seen as better than smaller competitors in managing cyber security; have well-established redundancy protocols, failover, and other technical risk mitigations; have standardized contracts and services; offer a range of services beyond the cloud; and are among the few companies that have the processing power needed for advanced analytics using machine learning, AI, and big data analytics. Their dominant position is likely to get stronger with a growing client base in multiple countries.

There are no hard data showing the concentration of the global financial sector in the large CSPs. A failure, major cyber incident, or even political interference in a CSP could have systemic implications, potentially across several countries. The FSB (2017) notes the risks of CSPs linking multiple systemically important institutions or markets. The European Supervisory

\(^{12}\) Containerization allows the abstraction of applications from the computing environment. A container is a standard unit of software that packages up code and all its dependencies, making it a standalone, executable package that includes everything needed for it to run across different environments. Containers virtualize the operating system instead of hardware, leading to such portability. Source: Docker.com.
Authorities (ESAs) underline that view by noting that CSPs become a source of ICT and cybersecurity risk and, due to concentration and their interconnectedness in the financial sector, CSPs can become a single point of failure and threaten financial stability.

Challenges faced by supervisors

Audit and access rights
Supervisors – particularly in EMDEs – could face challenges to access data and conduct audits at global CSPs. Limitations stem not only from the foreign location of CSP facilities and potential legal inconsistencies with the supervisor’s own legal framework, but also from the distributed approach to data management. The data of a regulated institution may be stored concomitantly in more than one country location and several physical facilities and can move around them. Data flows are dynamic rather than static and pre-determined. Data centers could be in countries with which a supervisor does not have a coordination agreement, or potentially a country with which the supervisor’s government does not have good diplomatic ties. The multi-tenant nature of CSP facilities also raises concerns over security and confidentiality during audits.

Imposing requirements on outsourcing arrangements
Supervisors may also face difficulties in imposing minimum contractual clauses on large global CSPs. As in other outsourcing in financial services, regulation often gives the power to the supervisor to impose minimum contractual clauses in outsourcing agreements. For example, this may include a financial institution’s and the supervisor’s right to access and audit third-party service providers, and a clause to guarantee the continuation of service provision in case a financial institution is put into resolution. However, the supervisor’s bargaining power – especially in EMDEs – may be reduced when dealing with global CSPs. CSPs may resist adopting compulsory contractual clauses.13

Capacity and expertise
The challenges in cloud computing are exacerbated in EMDEs due to less developed regulatory and supervisory frameworks. Even though financial innovation in EMDEs is rampant, EMDE supervisors are likely to have more limited experience with effectively assessing outsourcing arrangements and may operate with an incomplete, underdeveloped, or inexistent regulatory framework for cyber and data security risks, outsourcing, and operational risk and resilience. They may also lack enough staff with the skills, expertise, and experience in IT and cyber security risks to make judgments about a financial institution’s management of cloud risks and outsourcing arrangements. This could even hinder their ability to evaluate reports by specialized auditors about a particular CSP. The FSB (2020b) shows that concerns with resources and skills to supervise outsourcing and other third-party relationships may also affect supervisors in advanced economies.

13 Australian Prudential Regulation Authority (2015) notes that this has been a problem in Australia.
Risks of not using cloud computing

Despite the risks, not moving to the cloud could be riskier. As a supervisor has noted, “cloud usage is not without risk – but nor is the status quo.”\(^\text{14}\) Keeping legacy systems based on aging technology within a financial institution increases its operational risks\(^\text{15}\) and reduces its resilience and the effectiveness of its contingency and business continuity arrangements. Moreover, it is a strategic risk.

Cloud computing is also a driving force of a shifting competitive landscape. Mobility, rapidity, and flexibility – including scalability – are key to responding to shifting consumer preferences. Moreover, cloud computing may be essential to participate in data sharing schemes (FSB 2019a).\(^\text{16}\) The question facing many incumbent financial institutions is not whether to adopt the cloud, but how and when.

Regulatory and supervisory responses

Regulatory frameworks are being updated to deal with new types of outsourcing, including cloud computing. Prevailing regulatory approaches to outsourcing in financial services rely primarily on the duty and ability of the regulated institution to identify, measure, manage, and mitigate the risks of outsourcing, and empower supervisors to impose contractual and other conditions on outsourcing arrangements and sometimes on third parties. Financial institutions need to identify and give special attention to the outsourcing of critical or important activities and functions. While these foundations remain valid, cloud computing introduces challenges that are only starting to be recognized by international standard setting bodies and national regulators.

Responses by international standard setting bodies (SSBs)

The only international SSB that has directly addressed cloud computing in its standards is the International Organization of Securities Commissions (IOSCO). In May 2020, it issued for consultation an update to its outsourcing principles. The guidance focuses on material or critical outsourcing and addresses specifically some cloud computing issues. The language used gives flexibility for financial institutions to outsource to CSPs and to deal with some of the difficulties posed by such outsourcing. However, IOSCO proposes restrictions such as requiring approval by the regulated institution prior to any sub-contracting by CSPs, which could pose practical hurdles. IOSCO also discusses considerations such as the need, when determining materiality or criticality, to consider the industry-level aggregated exposure to a service provider, including CSPs.

In August 2020, the Basel Committee on Banking Supervision (BCBS) issued for consultation an update of its 2003 Principles for Sound Management of Operational Risk\(^\text{17}\) and a draft set of Principles for Operational Resilience.\(^\text{18}\) These two consultation papers are relevant for cloud computing.

\(^{14}\) Byers (2018).

\(^{15}\) Institute of International Finance (2019) and Financial Stability Board (2017).

\(^{16}\) Data sharing schemes include open banking, which is the sharing of customer data kept by banks; open finance, which expands this concept to other financial sectors; and open data, which adds non-financial data (for example social media, telecom, and e-commerce data).

\(^{17}\) Basel Committee (2020a).

\(^{18}\) Basel Committee (2020b).
computing but do not address all of its specificities. Despite the critical role cloud computing outsourcing can play in operational resilience and operational risk, there is no mention in these documents of cloud computing as a source of risk or as a risk mitigation tool. Cloud computing was also briefly addressed in BCBS (2018), which noted that banks should have effective governance structures and risk management processes.

The FSB has been active in exploring developments in cloud computing from a financial stability perspective. It has shown particular interest in concentration on large CSPs and the interconnectedness of systemically important financial institutions through CSPs. The FSB (2017) called for international coordination to deal with risks such as those posed by CSPs, while FSB (2019b) explores the stability implications of third-party dependencies in cloud services, touching upon some of the issues discussed in this Note. Finally, FSB (2020a) notes that as financial institutions’ reliance on third party service providers such as CSPs increases, the effectiveness of their practices for cyber incidence and recovery will need to evolve accordingly.

**Regional-level responses**

The European Supervisory Authorities (ESAs) have considered cloud computing outsourcing in updates to their frameworks. The European Banking Authority (EBA) issued recommendations for cloud computing outsourcing in 2017, which were later incorporated into updated guidelines on outsourcing arrangements. The European Insurance and Occupational Pensions Authority (EIOPA) issued guidelines on outsourcing to CSPs in January 2020. The European Securities and Markets Authority (ESMA) issued, for consultation, draft guidelines on outsourcing to CSPs in June 2020, which is very much aligned with EIOPA’s guidelines. The three sets of guidelines take similar balanced approaches, although ESMA’s and EIOPA’s go into greater detail. For instance, ESMA’s draft requires firms to have an up-to-date cloud computing outsourcing strategy, specific (and tested) exit and transition plans, and secure deletion of data at the CSP after a transition. Another example is the permission, in the guidelines of both EIOPA and ESMA, to use alternative methods to audit CSPs. These important regulatory developments may have influence beyond the EU.

The overall approach of the ESAs is to impose stricter requirements on critical or important CSP outsourcing. They cover similar content and ask for proportional and risk-based implementation of the guidelines. Generally, no restrictions to outsourcing to CSPs are imposed, including on data location and prior approvals (although there are exceptions). The ESAs acknowledge the challenges for financial institutions and supervisors to deal with large CSPs, such as to exercise access and audit rights, to control the risks of sub-contracting, to require CSPs to take on insurance, and to require specific contractual clauses.

---

19 In the US, the Federal Financial Institution Examination Council (FFIEC) has noted in its IT Examination Handbook (FFIEC 2015) that some institutions have adopted cloud-based disaster recovery arrangements. FSB (2019b) acknowledges the resilience benefits of cloud computing outsourcing.

20 European Banking Authority (2019).

21 European Insurance and Occupational Pensions Authority (2020).

22 European Securities and Markets Authority (2020).
Country-level regulatory responses

The Financial Stability Institute (FSI 2018) classifies the different regulatory treatments of cloud computing into:

1. General outsourcing regulations
2. Governance and risk management rules specific to cloud computing outsourcing
3. Information security regulations specific to cloud computing outsourcing
4. Specific recommendations or supervisory expectations on cloud computing

A growing number of supervisors are issuing specific guidance or supervisory expectations for cloud computing, either as a standalone document or as part of a broader regulation, but which explicitly deals with cloud computing. Some jurisdictions such as the UK Prudential Regulation Authority (2019a and 2019b) have recently updated their outsourcing regulations and also issued a framework for operational resilience. Among the countries that have issued specific cloud guidance, there is a fair level of commonality in the scope and approach taken.

Responses to the cloud in EMDEs have ranged from updating cyber security regulation (for example in Brazil), to prohibiting the use of the cloud for certain data (for example in Pakistan), to no response (most countries in Sub-Saharan Africa). Only a few EMDE authorities have issued specific regulations. Some EMDEs lack foundational regulations such as on outsourcing and cyber and data security risk. In their absence, and coupled with likely insufficient understanding of cloud computing, supervisors may become overzealous and take potentially counter-productive measures such as:

- data localization requirements;
- local incorporation of CSPs and local staff;
- in-country replication of data stored in the cloud;
- prohibition from using the cloud for certain types of data or functions/activities;
- prescriptive technical system, infrastructure, or encryption specifications; and
- prior supervisory approval for all cloud computing outsourcing and sub-outsourcing, regardless of materiality.

Data localization and cross-country legal inconsistencies for data protection could impede or make it difficult for globally active financial institutions to use CSPs in different jurisdictions to leverage the best capability of each, or to use a single CSP that maintains data centers in different jurisdictions as a tool to increase operational resilience by easily porting data and applications.

Country-level responses are likely to evolve as understanding about the risks and the benefits of cloud computing outsourcing in financial services – including its role in risk mitigation and resilience – improves. For example, in 2018 the Bank of Israel lifted its earlier requirement for prior approval for cloud computing outsourcing and opened the possibility of using the cloud for

---

23 Examples of this include the Australian Prudential Regulation Authority (APRA), the Central Bank of Brazil, Canada’s Office of the Superintendent of Financial Institutions (OSFI), the Financial Superintendence of Colombia, France’s Prudential Supervision and Resolution Authority (ACPR), Germany’s Federal Financial Supervisory Authority (BaFin), the Bank of Israel, the Monetary Authority of Singapore (MAS), South Africa’s Prudential Authority (PA), the Financial Conduct Authority in the UK, and the Federal Financial Institutions Examination Council (FFIEC) in the US.

core activities or systems. The box below illustrates how APRA’s regulation of cloud computing outsourcing has evolved. Meanwhile, possibly in response to regulatory concerns, some CSPs are offering services that could be more easily accepted by regulators not willing to abandon traditional practices. An example is AWS’s Outposts.

**The evolution of Australia’s approach to cloud computing outsourcing**

The Australian Prudential Regulation Authority (APRA) is an example of how the regulatory and supervisory approach to cloud computing can evolve over time. In 2010, APRA communicated to regulated institutions its concerns regarding cloud computing outsourcing (APRA 2010). APRA noted that institutions were failing to recognize the significance of cloud computing and to apply the same rigor as for other outsourcing. Institutions needed to consult APRA prior to entering into offshore outsourcing of material activity.

In 2015, APRA issued its first cloud-specific guidance (APRA 2015), covering strategy, governance, IT risk, and assurance mechanisms. APRA made clear that it had reservations about cloud computing outsourcing due to immature risk management and mitigation practices, including cursory risk assessments by regulated institutions, insufficient CSP due diligence, and limits to access and audit rights. In its risk classification, public cloud was considered as having heightened inherent risk. Situations classified as having an extreme impact on financial institutions included hosting information essential to determining obligations to clients in the cloud, so APRA discouraged the use of public cloud for this purpose. APRA encouraged Australian-hosted options and CSPs that catered to clients with comparable security requirements, risk profiles, and risk appetites.

In 2018, APRA shifted its stance, issuing a more extensive and detailed cloud computing regulation (APRA 2018). It recognized improvements in risk management practices and transparency of CSPs, including when involving sensitive information. There are no blanket prohibitions or limitations to cloud computing outsourcing, although Australian-hosted clouds and clouds restricted to financial institutions are still seen as less risky. The guidance states that risks are a function of the nature of the cloud usage, and classifies cloud-inherent risks into low, heightened, and extreme. Risk management expectations vary according to this classification.

The use of public cloud “involving systems of record which maintain information essential to determining obligations to customers and counterparties” continues to be classified as an extreme inherent risk, which requires financial institutions to demonstrate that they have sufficiently strong risk management and mitigation techniques and capabilities prior to engaging in such arrangements. In addition, other regulations apply to cloud computing outsourcing (general outsourcing, business continuity management, management of security risk in information, and IT and management of data risk).

**Country-level supervisory responses**

There is more limited information in the public domain about supervisory responses to cloud computing outsourcing. The FSI (2018) highlights practices adopted by insurance supervisors, who usually place cloud computing outsourcing under operational risk assessments and adopt traditional techniques such as:
On-site inspections that review outsourcing documentation, processes related to cyber security management, monitoring reports and controls, and business continuity plans.

Off-site reviews that focus on assessing the insurer’s governance and risk management practices, review of notification/approval files, public information such as third-party certification and assurance reports, regulatory reports, and specific requests (thematic reviews and questionnaires).

The Basel Committee (2018) identifies two regimes for third-party supervision, which are relevant for cloud computing outsourcing. In the first, the supervisor has the statutory authority to directly supervise third-party service providers or activities provided by third-party service providers to banks (as for example in Argentina, Luxembourg, Saudi Arabia, Turkey, and the US). In the US, the federal banking agencies have used such legal authority to conduct examinations of third-party service providers and develop a formal program for significant technology service providers. In Luxembourg, the Commission de Surveillance du Secteur Financier (CSSF) maintains a register of third-party service providers, for which a formal supervisory program has been developed. In the second, which is most common internationally, the supervisor gains access to third parties through the contracts these parties have signed with supervised banks.

Some supervisors are starting to look more closely at system-level issues in cloud computing. For example, the UK’s Prudential Regulation Authority (PRA) is in its third round of surveys on cloud use in the banking sector and its first for the insurance sector. The survey shows that banks use much more cloud computing outsourcing than insurers, covering a wide range of processes. The PRA has not taken specific measures such as requiring diversification/redundancy of CSPs on banks, or selection of service types to address other concerns (for example data location or physical segregation of servers for exclusive use of banks). However, the PRA will continue to work on concentration risk and the lack of substitutability of CSPs. Lael Brainard of the US Federal Reserve has noted the concentration risk and that the Federal Reserve may force institutions to use multiple cloud providers. One of the aims would be a bank’s ability to fail over automatically to a second system if the main one collapses.

Regulate cloud providers?

Currently, supervisors rely on the ability and duty of regulated financial institutions to assess and manage third-party service providers in outsourcing arrangements. But cloud computing outsourcing can reduce the visibility of and access to CSPs, which could reduce the effectiveness of the current regulatory and supervisory approach to outsourcing. Resolution authorities are affected as well, as they could face practical or legal obstacles to access data, terminate or extend CSP contracts, or guarantee service continuity during resolution.

The issues introduced by cloud computing outsourcing challenge the supervisory perimeter. Some supervisors have powers to supervise CSPs directly, based on outsourcing and other regulations. They may be able to take direct measures on CSPs identified as critical in their

26 See Roland (2019).
27 Financial Stability Board (2019b) and Financial Stability Board (2020b).
There are two problems with this approach. First, many EMDE supervisors may not be able to extrapolate their perimeters based on current regulation and if they do, they may be ill-equipped – technically and politically – to do so, especially when dealing with global CSPs. Second, this approach does not solve the cross-border issues. In such a context, limiting cloud computing outsourcing such as by imposing data localization may be tempting.

The use of an activity-based approach to regulation and supervision is also relevant here. In most jurisdictions, regulatory perimeters and supervisory activities are defined by types of institutions, not types of activities. CSPs are not only CSPs; they offer a range of other related and unrelated services to financial and non-financial institutions, corporates, and consumers. Their reach is much broader than financial services. Imposing requirements on CSPs, such as separation of different businesses and other rules typically imposed on financial institutions, would be at least counterproductive. However, their critical role in the financial sector asks for pragmatic solutions to allow monitoring, oversight and, potentially, supervision. This could require a balance between activity- and institution-based regulation.

There is a continuing discussion of whether CSPs should be directly regulated and supervised. This mostly concerns US-based global CSPs, but the discussion is also being held within the European Union and some other jurisdictions. In April 2019, the ESAs issued a Joint Advice (ESAs 2019) requesting the European Commission to devise a legislative solution to create “an appropriate oversight framework to monitor the activities of critical third-party service providers.”

The designation of CSPs in Europe or elsewhere as critical infrastructure could allow for direct regulation by some authority. However, the broad reach of CSPs, in terms of geographies and economic sectors, makes this a complex endeavor. Open questions include:

- How would criticality be defined:
  - at the local, national, regional, or international level?
  - based on CSPs being a financial market infrastructure or a national strategic infrastructure, or both?
  - by which (financial or non-financial) authority (or authorities)?
  - based on what criteria? Would criteria change across sectors?

- If criticality is defined for the financial sector only, should CSPs ringfence services to the financial sector?
  - What technical and business challenges would this create?

- Would all CSPs be regulated and treated equally or would a tiered approach be used?
  - If a differentiated treatment is adopted, would it lead to greater market concentration, vendor lock-in, and higher prices for designated CSPs?

- Which authority (or authorities) would oversee CSPs?
  - Should there be a cross-national CSP regulator?

- If CSPs are regulated in their home countries, what does it mean for host countries?
  - Would this solve the issues faced currently by EMDE supervisors?

---

29 The advice asked for an oversight framework for CSPs that established criteria for defining the criticality of CSPs, the extent of the activities subject to the oversight framework, and the designate of an oversight authority (or authorities).

30 This list is based on and expanded from Institute of International Finance (2019).
The IIF (2019) and FSB (2019b) present alternatives to regulating CSPs as critical infrastructure. A potentially less problematic and comprehensive approach could include:

1. Modernizing third-party management and large exposure frameworks to allow supervisors to identify and directly oversee critical CSPs and dependencies, with permission to impose a range of requirements on outsourcing agreements and CSPs, including in the case of system-level concentration.

2. Requiring financial institutions to adopt multi-cloud (combined deployment models), multi-vendor, and/or hybrid approaches (part of scalable computing services remains in-house while working in utility mode with multiple CSPs).

3. Supporting and encouraging industry initiatives towards greater data portability across CSPs and between these and in-house architecture, such as containerization. In fact, such developments may be a necessary condition for points (1) and (2).\(^{31}\)

Large EMDEs may be able to impose requirements on CSPs and take other actions, but smaller and low-income countries could face challenges. Countries like China and India, with a vast potential market for CSPs, have proven that they can impose limitations on CSPs without jeopardizing the growth of cloud computing usage in the financial sector as well as the development of a local CSP industry. Most EMDEs, however, have much less room to maneuver. Imposing data location (in a specific foreign country) or localization (in-country), minimum contractual clauses, local incorporation, local staff, in-country data replication, access and audit rights, and other requirements may lead CSPs to exit or not enter the country.\(^{32}\)

Where there are large domestic CSPs in EMDEs, they are unlikely to have technology, level of service, and risk management capacity comparable to global CSPs. Concentration of outsourcing to them could potentially be riskier than cross-border outsourcing.

**Next steps for supervisors**

**Taking immediate steps**

Supervisors need not wait for an up-to-date regulatory framework to start acting. They can take practical steps to incorporate attention to cloud computing outsourcing in the course of their current activities. This could help them both to assess the risks being taken by supervised firms using cloud computing, and to inform the development of a regulatory approach and market practices that balance the potential benefits and risks of this type of outsourcing. Supervisors could, for instance:

1. Discuss with the senior management at financial institutions using cloud computing:
   - Their strategy on cloud computing outsourcing and expected outcomes, and how it relates to their IT and risk management strategies.

---

\(^{31}\) The European Commission’s work to set the foundation for a single digital data market is an interesting example. It has, among other initiatives, developed self-regulatory codes of conduct on data portability for easier cloud switching (https://ec.europa.eu/digital-single-market/en/cloud).

\(^{32}\) The International Organization of Securities Commissions (2020) acknowledges this risk, while the Basel Committee (2018) notes that the direct regulation of third-party service providers could hinder the development of innovative models.
Currently outsourced activities and functions, and the risks involved.
How cloud computing outsourcing is addressed in the institution’s operational risk management framework, and any adaptations introduced to its third-party/vendor management framework.
The criteria used to identify important/critical cloud computing outsourcing arrangements and how these are treated differently.
How cloud computing outsourcing affects business continuity planning and contingency arrangements, as well as testing.
Their views and measures around vendor lock-in and concentration risks, and their level of dependency on CSPs.
How cloud computing outsourcing affects data and cyber security risks and how the institution manages and mitigates these risks.
Their strategy with regard to location of data storage and processing.
The adequacy of the institution’s skills and expertise to assess, manage, and mitigate the risks of cloud computing outsourcing.
The criteria and methods used to evaluate and audit CSPs.
The challenges faced when negotiating contracts with CSPs.
Whether institutions have adopted or are considering adopting multi-cloud, multi-vendor, and hybrid approaches, and the challenges faced.

2. Conduct an initial survey on cloud computing outsourcing practices in the market to map the main CSPs, main sub-contractors (to the extent possible), the services being provided under cloud models, and potentially identify the concentration and interconnection of systemic institutions through CSPs.

3. Draw upon existing expertise – including by collaborating with IT specialists – to enhance the understanding of supervisory staff about cloud computing services and models, risks, and benefits, for example by organizing internal workshops.

Establishing a sound basis for the supervision of cloud computing outsourcing

1. Issue or update foundational regulations to underpin safe cloud adoption

Some EMDEs lack basic regulations that underpin the safe adoption of cloud computing or have outdated regulations. These include regulations on general outsourcing, operational risk management (including operational resilience), governance, internal controls, and data and cyber security. EMDE supervisors facing growth in the adoption of cloud computing need to accelerate reforms to put in place the basic up-to-date foundations for cloud computing outsourcing supervision, including the collection of data and information on outsourcing arrangements.

Likewise, supervisors should assess whether there are legacy barriers to the adoption of cloud computing in the current framework, such as requirements for specific types of data to be stored or processed in proprietary data centers, and/or in data centers within country borders. Rules that prohibit the outsourcing of essential services or functions could also hinder cloud computing outsourcing. There could be instances where, even in the absence of a regulatory barrier, supervisors direct financial institutions towards well-known data and IT architectures and away from the cloud. The focus should shift to the risks involved. Cloud computing outsourcing, due to
its distributed nature, redundancy features, and scalability, could potentially reduce some key risks in the provision of essential services and could enhance operational resilience.

2. **Issue guidance and/or requirements specific to cloud computing outsourcing**

The risks and complexity introduced by cloud computing require specific guidance for the application of principles such as those on outsourcing and cyber and data security. While non-specific regulations provide an important foundation, they may lack the level of specificity for optimal regulatory and supervisory treatments of cloud computing outsourcing. The aim should be to address the risks, to allow financial institutions to tap the benefits of the cloud – including to enhance operational resilience – and to provide some level of regulatory certainty to financial institutions and CSPs. Issues to be covered in such rules and guidance could include (non-exhaustive):

- application of the regulatory definition of critical or important/material outsourcing to cloud computing;
- governance of cloud computing outsourcing arrangements;
- risk assessment, including political and legal risks depending on the location of data;
- supervisory notification and/or approval;
- CSP due diligence, lock-in risk, concentration risk;
- minimum contractual clauses;
- treatment of sub-contracting;
- risk management and mitigation;
- continuous assessment and monitoring of CSPs;
- resilience, business continuity, and recovery; and
- exit strategy.

Cloud computing technology as such should not be the focus of regulation. The approach should be technology neutral, allowing the best solutions to emerge and be tested. Requirements should also be proportionate and commensurate with the criticality of outsourcing and the size and complexity of the financial institution. Given the state of development of cloud computing outsourcing in financial services, the regulation could also provide examples of good and poor practices in risk management.\(^33\)

3. **Enhance cross-sector consistency and cooperation**

The regulatory guidance and requirements on cloud computing outsourcing need to be consistent across financial sectors and across functional authorities. In jurisdictions where there are multiple sector-based (for example banking and insurance) or function-based (for example prudential and conduct) financial authorities, there is a need for them to work together in issuing consistent requirements for cloud computing outsourcing and CSPs. The systemic issues created by CSP concentration also require coordinated action, such as to identify the risk of the potential failure of a large CSP, to identify tipping points, and to devise contingency and crisis management plans. Additionally, cloud computing is at the intersection of regulatory domains, in particular data protection, but also consumer protection, competition, and ICT regulation.\(^34\) As called for by the FSB (2017), supervisors should coordinate with relevant non-financial authorities to ensure that legal or regulatory inconsistencies, ambiguities, and gaps are

---

\(^33\) See, for example, APRA (2018).

\(^34\) The ICT or similar authority in some jurisdictions has issued cloud computing regulations.
minimized. The ESAs’ work on supervisory convergence in the area of ICT risks, including cloud computing outsourcing, is an example of such an attempt.

4. Understand and prepare for systemic risks

In addition to regulations focused on the risks faced by individual financial institutions, supervisors should start preparing to deal with the financial stability risks potentially posed by CSPs. Information needs to be collected on existing critical or important cloud computing outsourcing, concentration on individual CSPs, and interconnectedness within the financial system. Supervisors should strive to assess the risks of a potential failure of a significant CSP, or other type of problem (for example government action in the home country of a CSP), and to devise strategies to mitigate the risks. The FSB (2017) specifically calls for supervisors to determine whether current oversight frameworks for important third-party service providers are appropriate (as discussed above). This could require coordination between financial authorities in different jurisdictions and with other domestic authorities, such as ICT authorities.

5. Increase supervisory capacity and expertise

Updating supervisory capacity and expertise will be fundamental for EMDE supervisors to address successfully the challenges and opportunities posed by cloud computing, to participate in the discussions at SSBs, to engage with other countries and with CSPs, and to implement an effective supervisory approach to cloud computing outsourcing (at micro and macro levels) that can evolve over time. Supervisors need to increase their knowledge about cloud computing arrangements, CSPs, third-party management, data portability, legal issues affecting cloud computing, contractual models, cyber security, operational resilience, and business continuity, and how cloud computing may have an impact on these areas. Supervisors also need enhanced technological expertise to understand and supervise effectively. They should assess their staffing and training programs and consider the availability of specialized skills.

6. Work towards bilateral and multilateral coordination

Cross-border regulatory inconsistencies will appear if national responses proliferate in an uncoordinated manner. This could have an adverse impact on supervisory effectiveness and on the development of technical solutions for the cloud that could increase financial sector resilience. There is a compelling case for a consistent international approach to cloud computing. At least bilateral coordination between the home and host countries should be sought to decide upon matters such as jurisdiction over CSPs and solutions for supervisors and resolution authorities to exercise audit and access rights and to protect the data of a country’s citizens held by a foreign CSP.

But bilateral agreements are not enough. A multi-jurisdiction approach would be necessary and particularly important for EMDEs. The FSB (2017) has already called for greater global coordination to deal with risks such as those arising from cloud computing outsourcing. International coordination remains poor in many areas, including financial supervision and taxation (as demonstrated by lingering tax disputes involving US-based BigTechs), while transnational legal, regulatory, and supervisory inconsistencies can hinder the potential benefits of cloud computing. For example, inconsistencies in data protection laws and data localization rules can limit a CSP’s ability to move data across data centers, even though this could be one of the greatest contributions by global CSPs to financial sector resilience.

SSBs could lead analyses of key concerns in cloud computing outsourcing and develop guidance for regulation and supervision in this area. Such guidance could build on IOSCO’s updated principles for outsourcing, on the work done in the EU, and on existing country-level regulations and supervisory approaches. The guidance could be a joint guidance by the key SSBs since the issues are similar across sectors and considering the cross-sector reach of CSPs. The FSB could provide guidance for the identification, monitoring, and mitigation of financial stability issues, including the analysis of potential cross-border contingency and coordination arrangements in the event of a failure of a global CSP, building on its work to date. The FSB could also play a role in collecting and disseminating data about CSP concentration, based on information shared by country authorities.

Discussions that could be triggered, headed, and/or facilitated by SSBs include:

- minimum standards of governance and risk management with regard to critical or important cloud computing outsourcing;
- the application of the definition of criticality to cloud computing outsourcing;
- harmonized minimum contractual clauses for global CSPs;
- solutions for access and audit rights at global CSPs;
- alternative methods to assess CSPs, including third-party certification and pooled audits;\(^{37}\)
- the impact of different approaches to cloud computing outsourcing on operational resilience and business continuity;
- the practicality and impact of imposing data location and localization on CSPs;
- technical and business solutions for data portability;
- the scope of home/host jurisdiction over CSPs and supervisory coordination;
- data sovereignty issues and protection of a country’s citizens’ data held by CSPs;
- methods to assess the risk of concentration of CSPs and mitigation options;
- the collection, monitoring, and dissemination of data on outsourcing to global CSPs;
- risk mitigation and diversification by individual institutions, including multi-vendor, multi-cloud strategies and hybrid strategies; and
- the downsides and benefits of approaches to directly regulate and/or supervise CSPs.

It is fundamental that EMDEs have a voice in the international standard setting process so that the guidance takes into account their particular challenges, such as the more limited bargaining power with global CSPs and with the home country authorities of CSPs operating in their markets.

\(^{36}\) The Bank of England (2020b) has noted that it will be working with SSBs to develop and adopt international standards for safe cloud usage in the financial sector.

\(^{37}\) Examples of third-party certification include the Cloud Security Alliance’s (CSA) Security Trust Assurance and Risk (STAR) Program and the American Institute of Certified Public Accountants’ System and Organization Controls (SOC) certifications. The CSA has developed cloud security audit criteria and certification programs for cloud computing auditors. In the EU, an analysis of cloud certification schemes was published in 2019 (European Commission 2019).

\(^{38}\) According to FSB (2020b), pooled audits are those conducted by groups of financial institutions sharing the same third party.
7. Support or push for market solutions that could reduce vendor lock-in

Market solutions such as containerization are needed not only to reduce lock-in risk and its related risks, but also to maximize the benefits of cloud computing outsourcing in financial services, allowing financial institutions to take full advantage of the best characteristics offered by each CSP in each jurisdiction, with maximum flexibility. Such flexibility could be an important element in enhancing operation resilience. In addition to participating in the discussions held at SSBs, supervisors should actively facilitate and promote domestic industry working groups or other methods (for example tech sprints) to accelerate the identification and adoption of technical and business solutions to the limitations of cloud services, in particular data (non-) portability.

Conclusion

The financial sector is still at the early stages of adoption of cloud computing as an alternative architecture to in-house systems and models. The potential benefits of this transformative model of handling data and IT assets are unquestionable. One potential benefit includes enhancing operational resilience, as demonstrated in the wake of the COVID-19 pandemic.

At the same time, cloud computing takes supervisors out of their comfort zone not only because of the inherent data and cyber security risks, but also because it challenges, to some degree, basic tenets of the current supervisory approach to outsourcing. In addition, large global CSPs and the concentration of the cloud market introduce complexity and systemic concerns.

In designing their responses, supervisors need to consider not only how traditional financial institutions manage the risks of their outsourcing arrangements, but also how new business models adopted by challengers can flourish based on cloud computing, to increase contestability, competition, and innovation. Regulatory and supervisory responses need to have enough flexibility to adapt as the cloud market develops further and as risk management practices evolve.

EMDE supervisors in particular should step up their ability to understand and assess the benefits and risks arising from cloud computing as part of their supervisory process. Those lacking foundational regulations such as on operational risk, and data and cyber security need to accelerate regulatory reforms to impose basic requirements to underpin safe cloud adoption. While outsourcing to CSPs can largely rely on such regulations, cloud-specific guidance and/or requirements may also be necessary. Supervisors should also assess whether the current framework poses undue obstacles for cloud computing and whether it gives them enough tools to deal with large CSPs that could become critical in the financial sector.

Given the global nature of the main CSPs, there is a compelling case for international coordination and collaboration to discuss solutions to the cross-border complexity introduced by global CSPs. While there will be value in bilateral coordination and supervisory arrangements between home and host countries, internationally-agreed solutions – that also take into account the context of EMDE supervisors and their particular challenges – would produce better results by reducing room for cross-border inconsistencies and gaps and regulatory arbitrage, and preventing counter-productive measures that could limit the potential benefits of cloud computing. International standard setting bodies should take a prominent role in triggering the necessary discussions and in the development of minimum standards.
References


European Insurance and Occupational Pensions Authority. *Guidelines on outsourcing to cloud service providers.* February 2020. [https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en](https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en)


Institute of International Finance. *CSP and Criticality: Potential Treatments and Solutions.* September 2019. [https://www.iif.com/Portals/0/Files/content/Innovation/09042019_csps.pdf](https://www.iif.com/Portals/0/Files/content/Innovation/09042019_csps.pdf)


