

**Deloitte.**



FFIEC statement on risk management  
for cloud computing services

CENTER *for*  
**REGULATORY  
STRATEGY**  
**AMERICAS**

### Background and context

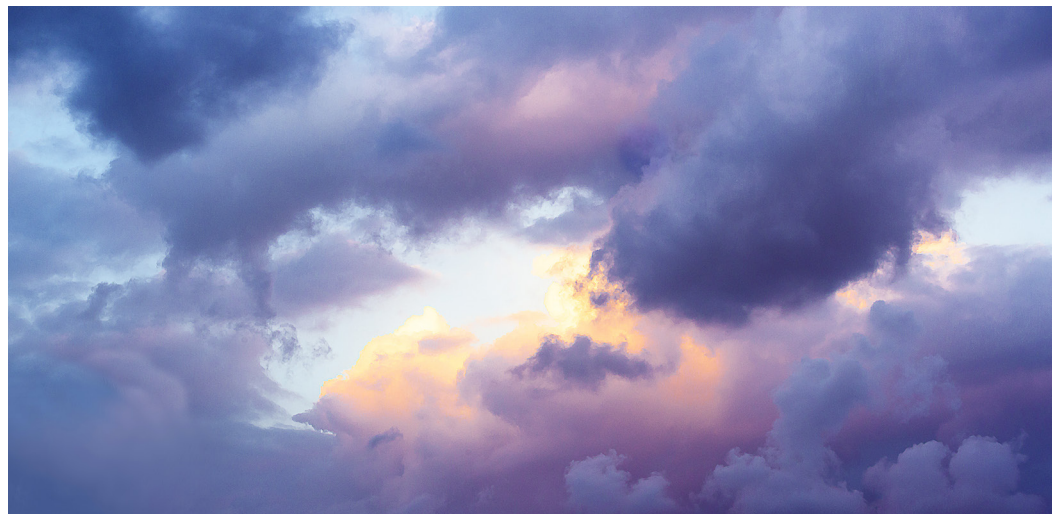
On April 30, 2020, Federal Financial Institutions Examination Council (FFIEC), on behalf of the bank regulators<sup>1</sup> issued a joint-statement<sup>2</sup> to address the use of cloud computing services and security risk management principles in the financial services industry. The statement represents a continuation of increased regulatory attention and oversight of cloud computing within the industry. The recommendations within the statement represent close alignment with other global regulators and encourages financial services institutions (FSIs) to consider their risk management practices as it relates to usage of the cloud in the domains of:



- Information security;
- Business continuity planning;
- Third party risk management;
- Privacy and data protection; and
- Record retention practices

While the widespread adoption of cloud computing by FSIs have led to many benefits, the increased reliance on cloud service providers (CSPs) and the critical roles CSPs often play to support their operations, have also increased certain risks and created new risks for these FSIs to manage. The statement recognizes that regulatory expectations have been heightened for increased risk management and enhanced cloud computing controls that are not only the responsibility of the FSI but are shared responsibilities between the FSIs and the CSPs; however, the ultimate responsibility lies with the FSI, particularly when safeguarding customer information. Recognizing the statement does not specifically prescribe any new requirements, it is intended to reinforce considerations that are recognized by the banking regulators by highlighting the following:

- Application of sufficient oversight and governance of the CSP(s)
- Clearly defined roles and responsibilities, control ownership matrices between the FSI and the CSP (as well as governance of the FSI over the CSP), and level of oversight and monitoring procedures to ensure effectiveness
- Balancing of benefits of cloud computing while weighting the costs and requirements to operate within risk tolerance levels and mitigating factors (as necessary)



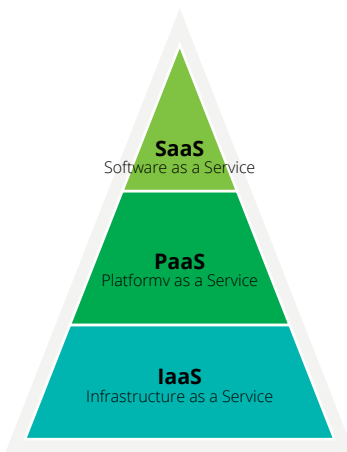
### Statement's consistency with FFIEC Handbooks

The statement touches upon much of the guidance provided previously in FFIEC Handbook<sup>3</sup>, but specifically provides welcome practical focus areas for FSIs on how to approach cloud-based implementation. The statement provides a high level summary of the different cloud environments —Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) — and reinforces many of the key takeaways from the underlying playbooks, namely the definition of roles and responsibilities between FSIs and CSPs.

### Responsibilities reinforce accountability:

The statement reiterates the need to clearly define, in contractual form, the expected responsibilities matrix that accompanies each adoption model between provider and consumer of cloud services. This is consistent with previous guidance, though the statement is pointed that while responsibilities should be defined and will be institutionally unique, ultimate accountability remains with the FSI.

The FSIs can help to manage and identify the responsibilities specific to the CSPs within their contracts. However, in addition the responsibilities and controls outlined in the vendor's contract, the FSIs should have an established approach to proactively monitor and oversee the CSP's performance in executing on their responsibilities and their ability to successfully manage risk. The graphic below provides examples of the division of responsibilities for IaaS, PaaS, and SaaS.



### SaaS

**FSIs** are responsible for user specific application configuration settings, user access and identity management, and risk management

**CSPs** are responsible for updating and maintaining infrastructure and applications



### PaaS

**FSIs** are responsible for managing risk, configuration of cloud platform, implementing and managing controls over development, deployment and administration of applications

**CSPs** are responsible for underlying infrastructure and platforms (including network, servers, operating systems or storage)



### IaaS

**FSIs** are responsible for managing risk, configuration of cloud platform, implementing and managing controls over operations, applications, operating systems and data storage

**CSPs** are responsible for managing and maintaining physical data center i.e. hardware, network infrastructure, environmental controls, hypervisor etc.

### Specific consideration for modern technologies






In addition to providing some general considerations in cloud adoption and review, the statement provides considerations for the usage of modern architectural constructs and technologies within the cloud, and at times provides some very specific direction. While it does not prohibit usage of these technologies, it does raise heightened attention to the following:

- **Micro-services:** advises FSIs to consider the risk posed by implementing multiple micro-services and the impact this can have to increase the FSI's attack surface area; and
- **Containerization:** advises FSIs on the risks of using the technology in comparison to virtual machines, namely in the areas of data management, security and complex monitoring.

This provides perspective regarding balance as it relates to these architectures and technologies, as often they are purported as assisting operational control, particularly for containerization where the ability to replicate and standardize configurations is touted as a strength. The emphasis of this statement recognizes the operational interdependence that FSIs have with CSPs for these purposes, between the basic provision of cloud storage and through infrastructure.

**Provision of a risk management practice framework**

The statement encourages FSI adopters of cloud services to apply a risk-based framework and provides five considerations as examples it believes are key in this adoption. These considerations are layered and hierarchical, and cover the following:

Illustrative Areas	Summary of FSI Considerations
 <p><b>Governance</b></p>	<ul style="list-style-type: none"> <li>Establish a cross-functional group with representation from technology, risk management, and compliance to provide the required subject matter expertise to develop the appropriate structure and approach tailored to the organizations use of cloud computing</li> </ul>
 <p><b>Cloud Security Management</b></p>	<ul style="list-style-type: none"> <li>Complete due diligence with CSPs to provide evidence of controls and compliance prior to engaging in a relationship</li> <li>Develop responsibility matrices formalizing expectations and responsibilities that are not clearly outlined in the contract</li> <li>Utilize assurance reports or require the 'right to audit' as a part of the contracts and Service Level Agreements (SLAs)</li> </ul>
 <p><b>Change Management</b></p>	<ul style="list-style-type: none"> <li>Consider the use of cloud specific testing resources with additional knowledge around cloud computing, risks, and the associated security requirements</li> <li>Specific reference is also provided to the utilization of micro services architecture, and the implementation of it in a manner which least exposes firms to surface area attacks</li> </ul>
 <p><b>Resilience &amp; Recovery</b></p>	<ul style="list-style-type: none"> <li>Include various "stress test" scenarios in business continuity plans (BCPs) which may impact the CSPs ability to continue operations or its speed in recovering, including but not limited to a viral pandemic forcing all operations to be performed remotely</li> </ul>
 <p><b>Audit &amp; Controls Assessment</b></p>	<ul style="list-style-type: none"> <li>Conduct recurring background checks on CSP employees who support critical FSI cloud-based processes</li> <li>Highlight specific CSP-related regulations and requirements with which the FSI must comply and request additional evidence of compliance from the CSP for these areas</li> <li>Adapt a controls framework to incorporate the specific requirements of cloud services, including cyber resilience, data management and any additional monitoring technology that is needed to support</li> </ul>

This framework provides an initial benchmark for FSIs to conduct a self-assessment, evaluate their cloud usage, compare against these risk management practices. This benchmarking can be further enhanced through comparisons against industry frameworks like NIST, ISO etc.

**What it doesn't cover**

While the statement provides best practices in certain areas and specific direction on technical components of cloud adoption, FSIs should not consider it as a rule, guidance, or checklist. FSIs should consider additional risk management measures such as ongoing assessments of concentration risk, data privacy and protection, data residency, increased adoption of new cloud services for regulated workloads etc. This needs to be further complemented consistently with other FFIEC guidance, particularly those focused on operational and enterprise risk.



“Global adoption rates have been on the rise in recent years, with the overall market expected to grow 17% in 2020, to \$228 billion.”

### Timing of the Guidance

#### Expansion of cloud adoption in financial services

The benefits of cloud adoption have been well documented, and FSIs have been quick to consider the benefits that the cloud brings in terms of computing, storage and scaling power to their business and technology environments. Global adoption rates have been on the rise in recent years, with the overall market expected to grow 17% in 2020, to \$228 billion<sup>4</sup>. These increased adoption rates have compelled global regulators to move quickly to address the systemic risk posed by the cloud in financial services. Simultaneously, FSIs continue to be subject to regulatory scrutiny and supervisory findings in this area, with a recent Federal Reserve Board Supervision and Regulation report detailing that over 60% of outstanding actions being present in the areas of governance and controls, including IT risk management and cybersecurity<sup>5</sup>.

#### In the context of the COVID-19 pandemic

The recent global pandemic, COVID-19, has further turned the regulatory spotlight on FSIs utilizing the cloud. Indeed, the global event has tested FSI’s business and technology process, including operational and technological resiliency capabilities to adapt and in many cases recover from operational disruption. It has also further highlighted some of the cyber and operational risks both FSIs and CSPs need to mitigate and manage related to information security, operational resiliency, and business continuity planning. COVID-19 has accelerated businesses to think about how to operate in the “new normal” with virtually almost all work being performed remotely and often reliant on cloud-based services and infrastructure. Furthermore, the impacts from COVID-19 can be felt by the FSIs operations due to increased market volatility and associated activities such as higher transaction volumes and settlements. Cloud scalability and elasticity has likely proven pivotal for those FSIs where cloud adoption is mature and has helped relieve part of the operational stresses.

In response to the pandemic, there has been an influx of pandemic related relief programs, such as the Small Business Association’s Paycheck Protection Program (PPP), which due to a very large number of applicants with short processing times required, have only added to the increased stress on the FSIs’ underlying technology infrastructure. Indeed, the impact of the event has already compelled firms to reevaluate many of their processes and technology postures; industry commentary has noted that this global event will likely drive those already considering a cloud strategy to move faster or compel those who were undecided to think deeper as they consider a wider digital transformation.<sup>6</sup>

The statement by the FFIEC has been likely planned for a while as bank regulators were turning their priorities to non-financial risks including cybersecurity and operational resiliency. The timing for this statement is key as it arrives at a time when resiliency, continuity and more widely operational risk are top of mind in the context of the pandemic. It provides a timely and practical risk management guidance to FSIs who either are already utilizing cloud-based services or those who are in the early stages of cloud adoption.

#### How does this statement compare to regulators globally?<sup>7</sup>

In short – globally there is an increased resonance between the regulators on the topic of cloud. The statement provides similar risk management principles highlighted by other regulators globally. In particular, the Australian Prudential Regulatory Agency (ARPA)<sup>8</sup>, European Banking Authority (EBA)<sup>9</sup>, and the Bank of England’s Prudential Regulatory Authority (PRA)<sup>10</sup> have all provided detailed guidance on the use of outsourced services, particularly focusing on the risks posed by cloud computing. Most of these regulators have highlighted similar key areas including governance, business continuity, shared responsibilities between the FSIs and CSPs, information security, data privacy, risk assessments, ongoing oversight, and audit and controls.

**FSIs can consider taking the following steps to address risks associated with cloud services:**

1. Perform an assessment of your firm's governance model of all cloud services leveraged
2. Integrate cloud to continuity-based playbooks, including business continuity, disaster recovery, and recovery and resolution (RRP) playbooks
3. Consider external review of operational risks and controls of cloud services to your FSI
4. Consider security management in the adoption of emerging technologies, including microservices and containerization, to balance the value of adoption with a need to minimize security vulnerabilities
5. Develop a meaningful partnership between the CSPs and your third-party providers to develop operational responsibility matrices, identifying security and operational risks, and assigning transparent ownership and oversight of mitigating control activities. Also consider access and review of third-party assurance reports, or the right to audit, as part of continued service review processes
6. Consider opportunities for consistent periodic testing of critical controls in your processes that are operated by CSPs

The statement from FFIEC recommends that the FSI's plan to use cloud should be in alignment with its overall IT strategy, architecture and risk appetite. Similar to the guidance around the world, the US regulators are moving towards ensuring that FSIs adopt leading practices like inventory the use of systems and information assets residing in a cloud environment, understand how and where their key processes and associated information is reliant on cloud based third parties, and how to best implement and monitor the cloud specific risk controls.

The previous guidance from Australia, Europe and UK provides more detail in many of the areas listed above and contains additional guidance on how FSIs can categorize their third party risks, assess the effectiveness of the CSPs ability to manage risk, and develop exit strategies or transition plans in the event the relationship with the CSP is not adequately managed.

On May 8, 2020, the European Central Bank released a blog titled "The first lesson from the pandemic: state-of-the-art technology is vital."<sup>11</sup> The blog actively encourages the use of technology to supplement firms operational resiliency in the light of COVID-19. The blog also states that regulators "are working hard to adapt our methodological toolbox and adjust our supervisory recommendations across all prudential risk categories to this new, fully digital reality." This demonstrates that global regulators aren't just looking at the costs of innovation, but rather how it can facilitate control and compliance.

Global regulators have emphasized these requirements are to be further evaluated, communicated and credibly challenged against various plausible scenarios prior to implementation. Given the overlapping expectations from regulators around the world, global FSIs should develop a consistent and comprehensive approach that synthesizes the compliance requirements from each jurisdiction in which they operate or plan to operate, while also looking to apply regional uniqueness to their approaches and underlying controls where there are specific requirements.

**So, what's next?**

The statement provides a key insight regarding bank regulators' views on this topic, and is a timely reminder of areas of concern given the increasing cloud adoption rates within FSI, and emphasizes the need to strengthen operational resiliency in light of the impact of COVID-19. In addition, FSIs must be vigilant in implementation of their responsibilities vis-à-vis CSPs as vendors. FSI own the governance, risk management, and control responsibilities for interaction with CSPs and must provide sufficient control and oversight over areas with heightened risk exposure.

With the regulatory spotlight turning toward cloud resiliency and security, both CSPs and FSIs need to rethink and reimagine their governance frameworks in order to provide the required oversight and transparency regulators expect.

**Authors:****Vik Bhat**

Principal | Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP

**Sunil Kapur**

Managing Director | Deloitte Risk & Financial  
Advisory  
Deloitte & Touche LLP

**Sean Hodgkinson**

Senior Manager | Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP

**With thanks to****Christopher Finn**

Manager | Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP

**Eric Monzon**

Manager | Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP

**Kyle Cooke**

Senior Consultant | Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP

**Bradley Paternostro**

Senior Consultant | Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP

---

**Endnotes**

- 1 The Federal Financial Institutions Examination Council (FFIEC) comprises the principals of: The Board of Governors of the Federal Reserve System (FRB), Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and State Liaison Committee (SLC).
- 2 FFIEC, "[Joint Statement: Security in a Cloud Computing Environment](#)," accessed May 13, 2020.
- 3 FFIEC, "[FFIEC Information Technology Handbook](#)," accessed May 13, 2020; FFIEC, "[Outsourced Cloud Computing](#)," accessed May 13, 2020.
- 4 Gartner, "[Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020](#)," accessed May 13, 2020.
- 5 Board of Governors of the Federal Reserve System, "[November 2019 Supervision and Regulation Report](#)" accessed May 13, 2020.
- 6 Wall Street Journal, "[Companies Hit Pause on Digital Transformation Despite Spending More on Cloud](#)" accessed May 13, 2020.
- 7 Deloitte, "[Cloud: the regulatory approach](#)," accessed May 13, 2020; Deloitte, "[Regulatory barriers: perceived or real?](#)" accessed May 13, 2020; and, Deloitte, "[Transitioning to the Cloud: considerations for firms](#)," accessed May 13, 2020.
- 8 Australian Prudential Regulatory Authority (APRA), "[Information Paper: Outsourcing Involving Cloud Computing Services](#)," accessed May 13, 2020.
- 9 European Banking Authority (EBA), "[Final Report on EBA Guidelines on outsourcing arrangements](#)," accessed May 13, 2020.
- 10 Prudential Regulatory Authority (PRA), "[Outsourcing and third party risk management](#)," accessed May 13, 2020.
- 11 European Central Bank, "[The first lesson from the pandemic: state-of-the-art technology is vital](#)," accessed May 13, 2020.

This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this article.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.