Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 37

Moving to the Cloud – The Intersection of Cloud Computing, Financial Services and Regulation in Europe, the United Kingdom and the United States

Diana Milanesi

2018

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology-related and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Diana is an attorney member of the State Bar of California, the New York State Bar, and the International Bar Association. Diana works as Legal Counsel at Monzo Bank, a leading UK digital challenger bank, where she focuses on corporate and capital raising transactions, tech commercial transactions, as well as partnership and open banking activities. Prior to joining Monzo Bank, Diana worked as Legal Adviser at Startup Europe India Network; Corporate Attorney at Squire Patton Boggs LLP (San Francisco (CA) office), where she advised domestic and international clients in connection with venture capital transactions, IPOs, Rule 144A/Regulation S offerings, fund formation, tech-focused transactions, cross-border reorganizations and M&As; and Legal Adviser at an international seed venture capital firm in San Francisco (CA), where she focused on seed and early stage venture capital investments in technology companies. Diana started her legal career as Associate in the Banking and Finance Department at Gianni, Origoni, Grippo, Cappelli & Partners (Milan office, Italy), where she gained extensive experience on banking and finance, private equity, and capital markets transactions.

Diana earned her Bachelor Degree in Judicial Science (LL.B.), *summa cum laude*, in 2007 and her Master Degree in Law (J.D.), *summa cum laude*, in 2009 both from Luigi Bocconi University, Italy. As part of her Master Degree in Law, in 2008 she attended an exchange program at Duke University School of Law, where she focused her studies on business law and financial regulation. In 2010, she received a certificate in debt market from the London School of Economics and Political Science, UK. Diana earned her LL.M. Degree from UC Berkeley School of Law in 2012, with a concentration in securities regulation and corporate finance. During the LL.M. program, she served as member on the Berkeley Business Law Journal. Diana received her J.S.D. Degree from UC Berkeley School of Law in 2017, with a concentration in venture capital, financial derivatives, regulation of capital markets and securities. During the J.S.D. program, she also attended MBA courses in financial derivatives, private equity, and venture capital at UC Berkeley Haas School of Business.

Diana has published various articles in the fields of securities law, financial regulation, and venture capital. She has also collaborated as lecturer and researcher at Mind the Bridge Foundation and Startup Europe Partnership, an integrated platform established by the European Commission to support the growth and sustainability of European startups and scaleups.

Her present research focuses on the rapidly evolving legislative and regulatory frameworks for financial technology in the U.S., EU and UK. She has been a TTLF Fellow since 2016.

General Note about the Content

Suggested Citation

This TTLF Working Paper should be cited as:
Diana Milanesi, Moving to the Cloud – The Intersection of Cloud Computing, Financial Services and Regulation in Europe, the United Kingdom and the United States, Stanford-Vienna TTLF Working Paper No. 37, http://ttlf.stanford.edu.

Abstract

Banks and other regulated financial institutions are becoming increasingly reliant on the cloud – using it to drive IT infrastructure ownership and maintenance costs down, improve business agility, rapidly scale computing capabilities, meet evolving business demands and customer needs and innovate at a higher pace.

As more and more data, functionalities and systems move to the cloud, financial regulators on both sides of the Atlantic have turned their attention and are now taking a much keener interest to the use of cloud solutions by banks and other regulated financial institutions. The fresh scrutiny comes as concerns mount among market participants over the continuing regulatory uncertainty and inconsistency of oversight being taken by regulators with regard to the cloud. To address these concerns, the European Banking Authority (EBA) in Europe and the Financial Conduct Authority (FCA) in the United Kingdom have recently issued new recommendations and guidelines for cloud outsourcing; while the U.S. Department of the Treasury has recently released a report identifying improvements to the cloud regulatory landscape in the United States.

As financial regulators develop clearer and more uniform guidance for the cloud, the need for effective dialogue among various stakeholders will also increase. Key to a successful cloud adoption in financial services will be a tight cooperation among regulators, financial institutions and cloud providers to ensure that the right frameworks, programs and processes for the cloud are developed and implemented, which will offer increased security while encouraging further innovation.

Table of Contents

Preface

The financial services industry is facing a significant shift as technology enables new forms of innovation and competition and drives changing customer expectations. Customers are courted by new entrants, including fintech companies and large tech giants, who increasingly leverage the power of technology to deliver personalised, flexible, seamless and on-demand banking and financial services. The new wave of competitors interacts with customers in real time, process customer data and analyse customer insights instantly, and assess customer needs based on constant direct and indirect input. Different from incumbent banks and long-established financial institutions, fintech companies and large tech giants have the advantage of not having to support and maintain outdated and expensive legacy technology infrastructures.

Faced with increased competition, incumbent banks and long-established financial institutions are turning to the cloud, employing it as a business asset to accelerate the transformation of their organisations, to reshape their models, processes and systems, and to evolve the offerings and the customer experience that they deliver. The cloud has, thus, progressively emerged as foundational element for their digital and business transformation, helping incumbent banks and long-established financial institutions compete in today's market while keeping pace with fintech innovation.

The benefits that banks and other financial institutions can realise by moving to the cloud are significant. Cloud computing can help banks and other financial institutions overcome the scaling limitations of legacy infrastructures and tap into advanced technologies developed by market leader service providers in a cost-effective manner. Further, cloud computing can help banks and other financial institutions reduce their infrastructure footprint, avoid expensive in-house IT infrastructure maintenance and upgrade costs, and introduce automation to deliver improved efficiency and cost savings. In addition, cloud computing can enable cost-effective

and real-time delivery of highly scalable resources, such as storage space and applications, and can contribute increased agility and flexibility to financial systems and processes. By leveraging the power of the cloud, banks and other financial institutions can also store and process vast amounts of data and rapidly add new computing capacity to meet ever changing needs. Cloud computing can enable IT resources to be centrally pooled, rapidly provisioned and quickly redeployed. Finally, banks and other financial institutions can take advantage of the cloud "pay as you go" cost structure, which allow them to pay only for what they need at a given time.

In addition to the foregoing, incumbent banks and long-established financial institutions are increasingly recognising that cloud computing can offer new and unprecedented opportunities to focus on innovation. Significantly, cloud computing can be used as a development platform that allow banks and other financial institutions to quickly create new testing environments and incrementally implement software changes (a critical challenge that the server model faces). Furthermore, banks can use the cloud as an analytics platform to leverage data into real-time customer insights in ways never before possible. Products and services can now be delivered in entirely different ways, opening up new forms of business and business models. By leveraging the power of cloud computing, banks and long-established financial institutions can also increase their agility and speed to seize new market opportunities, create new revenue streams, respond to a changing business environment, quickly adapt and rapidly scale to meet changing customer needs.

Though incumbent banks and long-established financial institutions see the benefits of cloud computing discussed above, they have been more reticent than other sectors to fully embrace cloud solutions and, particularly, to migrate data to public cloud services. While banks and long-established financial institutions are already using cloud computing for non-core and non-critical uses (e.g., e-mail, customer analytics, human resources and customer relationship

management), very few of them have transferred or are in the process of transferring front-office business processes or core services and operations (e.g., treasury, payments, retail banking, enterprise data etc.) to the cloud.

A number of factors contribute to explain this slow adoption, including security, privacy and operational concerns, as well as a vast and uncertain regulatory landscape.

Significant progress has already been made to reduce security, privacy and operational concerns. As cloud providers have become focused on servicing financial services firms, cloud offerings are now maturing with improved security and privacy features and service quality.

However, regulatory uncertainty still remains a key barrier to full cloud adoption. In particular, in Europe the current regulatory framework does not provide clear guidance with regard to the outsourcing process and the supervisory expectations that apply to outsourcing to cloud service providers by financial institutions. Where guidelines exist their implementation significantly varies across jurisdictions. This leads to market inefficiency and a lack of comparability of supervisory practices across Europe, which is crucial given the cross-border nature of cloud services. Inconsistency in the treatment of potential risks related to cloud services also leads to an uneven playing field across jurisdictions and institutions. Similar to Europe, significant regulatory challenges limit the adoption of, and migration to, cloud technology by financial services firms in the United States, driven in large part by the lack of an effective regulatory regime that has yet to be modernized to accommodate cloud and other innovative technologies. In this context, the large number of U.S. regulators involved with allowing the use of cloud in financial services and the uncertainty in the application of existing requirements and guidance create additional obstacles. Inconsistencies in U.S. regulators' experience and expertise with cloud computing have also been a contributing factor.

In response to the described scenario, financial regulators across Europe, the United Kingdom and the United States are now advancing the cloud dialogue. Over the past few months, they

have issued new proposals, recommendations and guidance on cloud computing with the aim to address the outdated framework on the process of outsourcing to cloud service providers by financial institutions and the lack of harmonised regulatory practices across jurisdictions. They recognise the potential for cloud to increase efficiency, flexibility and to allow rapid innovation and generally acknowledge that existing regulation needs to improve and operate in an agile way to keep up with fast-moving market developments.

The present paper investigates these recent EU, UK and U.S. policy and regulatory developments concerning the use of cloud computing by banks and other financial institutions in great detail. The paper is organised as follows:

- Chapter 1 presents an overview of cloud computing and its operating, service and deployment models; looks into the relationship between financial institutions and the cloud; and outlines related benefits, costs and risks;
- Chapter 2 provides an overview of recommendations and guidance on outsourcing to cloud service providers by financial institutions recently issued by EU regulators;
- Chapter 3 examines the guidance on cloud computing provided by UK regulators;
- Chapter 4 analysis the existing approach to cloud outsourcing by U.S. regulators and areas of proposed development; and
- Chapter 5 discussed three examples of new cloud-based challenger banks that are revolutionising the banking industry.

CHAPTER 1. CLOUD COMPUTING AND REGULATED FINANCIAL INSTITUTIONS

The National Institute of Standards and Technology ("NIST") has defined "cloud computing" as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1]

Essential characteristics of cloud computing are:[2]

- On-demand self-service - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without involving each service provider.
- Broad network access - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling - The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumers' demand. Examples of resources include storage, processing, memory, and network bandwidth.
- Rapid elasticity - Computing capabilities can be scaled rapidly up and down commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

[1] See, Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology (NIST), Special Publication 800-145 (September 2011), p. 2.
[2] Ibidem.

- Measured service - Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the utilized service.

1.1 Cloud Operating Models

Three are the main operating models for cloud computing:[3]

- Staff Augmentation - Firms can gain cloud expertise by hiring people with the right skill sets from service vendors. The additional staff can be housed in the firm's existing offshore captive center(s).
- Virtual Captives - Virtual captives have a dedicated pool of resources or centers to help with cloud operations and meet demand.
- Outsourcing Vendors - This approach uses offshore centers, facilities, and personnel from a third-party vendor to handle cloud operations.

1.2 Cloud Service Models

There are three main cloud computing service models:[4]

- Software as a Service (SaaS): SaaS allows use of a cloud service provider's applications on a cloud infrastructure. Users access the applications via a variety of client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual

[3] See, Capgemini Financial Services, *Cloud Computing in Banking. What banks need to know when considering a move to the cloud*, Financial Services Report (2011), p. 6.
[4] Id, pp. 2-3.

application capabilities, with the possible exception of limited user-specific application configuration settings. Examples of software that can be delivered this way include accounting, customer relationship management, enterprise resource planning, invoicing, human resource management, content management, and service desk management.

- Platform as a Service (PaaS): PaaS gives users more control as it allows them to deploy onto the cloud infrastructure their own or acquired applications, as long as they have been created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. This allows businesses to streamline the development, maintenance and support of custom applications, lowering IT costs and minimizing the need for hardware, software, and hosting environments.

- Infrastructure as a Service (IaaS): IaaS gives the clients the greatest overall control of function and scale by providing consumer processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

A study published by Cisco[5] reports that 71% of the total cloud workloads and compute instances in 2016 used the SaaS model, 21% used IaaS and 8% used PaaS. The study forecasts

[5] See, Cisco Global Cloud Index: Forecast and Methodology 2016–2021, White Paper (2018).

that by 2021, SaaS will account for 75% of the total cloud workloads and compute instances, IaaS for 16% and PaaS for 9%.

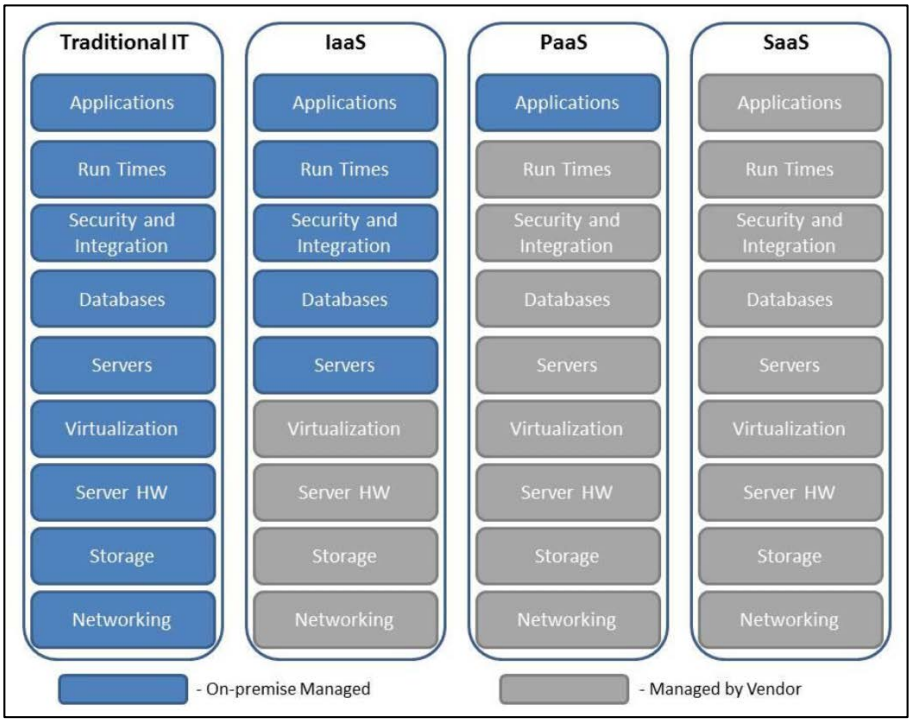
Due in part to security concerns and regulatory uncertainty as discussed in greater detail below, incumbent banks and other regulated financial institutions have been late in implementing cloud solutions relative to other sectors, but there has been clear uptake in more recent years. An industry study assessing the adoption of cloud services in the financial industry across 20 countries reports that over 60% of financial institutions surveyed developed and deployed a cloud strategy;[6] and a further study reports that 88% of European-based financial institutions surveyed were already using cloud-based services.[7]

In particular, a number of banks and other regulated financial institutions have already been using SaaS for non-core activities, such as billing, payroll, or human resources; and are actively exploring the possibility of moving more critical services to the cloud, such as treasury, payments, retail banking and enterprise data.[8] However, to date only relatively small incumbent banks and financial institutions have transferred the entirety of their core services onto the cloud.[9] When they have done so, they have mostly relied on the PaaS or IaaS models.[10]

[6] See, Cloud Security Alliance (CSA), *How Cloud is Being Used in the Financial Sector: Survey Report*, Report (March 2015).
[7] See, European Union Agency for Network and Information Security (ENISA), *Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations*, ENISA Report (7 December 2015).
[8] See, PWC, *Financial Services Technology 2020 and Beyond: Embracing disruption*, PWC Report (2016).
[9] See, Penny Crosman, *Small Banks Take a Test Flight in the Cloud*, American Banker (21 June 2015); Lee Campbell, *SaaS vs On-Premise and what that means for everyone involved*, Finextra (23 August 2018).
[10] See, BBVA, *Banking Analysis - Cloud banking or banking in the clouds?*, BBVA Research U.S. Economic Watch (29 April 2016), p. 3; European Banking Authority (EBA), *EBA Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech*, EBA Report (3 July 2018), p. 48; HTF Research, *Cloud Adoption*, HFT Research Paper – Sponsored by GFT (June 2018).

Chart 1

Cloud computing models and process and resource management



Source: Wenk, D. Porter's Five Forces Analysis of Cloud Computing.

1.3 Cloud Deployment Models

There are four main cloud computing deployment models, which differ by the level of exclusivity offered:[11]

- Private Cloud - The cloud infrastructure is operated for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- Community Cloud - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have similar needs and shared concerns (e.g., mission, security requirements, policy, and compliance

[11] See, Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing*, cit., p. 3.

considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

- Public Cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- Hybrid Cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Among the cloud computing development models discussed above, the adoption of public cloud is occurring throughout the economy at a rapid speed. A recent survey suggests that c. 92% of the respondents of businesses are adopting at least some form of public cloud services. [12] Further, market studies forecast robust growth in public cloud revenues. For example, a study by Gartner forecasts global public cloud revenue growing from $153.5 billion in 2017 to $186.4 billion in 2018, a 21.4% increase.[13] Other studies estimate that public cloud will become the dominant infrastructure model[14] and forecasts significant growth in data usage. For example, a study by Cisco estimates that by 2021, 95% of global data center traffic will come from cloud services and applications; annual global cloud traffic will reach 19.5 zettabytes (ZB) by the end of 2021, up from 6.0 ZB in 2016. Further, the study forecasts that by 2021, 73% of the

[12] See, RightScale Inc., *RightScale 2018 State of the Cloud Report, Data to Navigate Your Multi-Cloud Strategy*, Report (2018), p. 12.
[13] See, Gartner, Inc., *Press Release – Gartner Forecast Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018*, Gartner (12 April 2018).
[14] See, PWC, *Financial Services Technology 2020 and Beyond: Embracing disruption*, cit.

cloud workloads and compute instances will be in public cloud data centers (up from 58% in 2016) and 27% will be in private cloud data centers (down from 42% in 2016).[15]

Incumbent banks and other financial institutions have various options in their "path to the cloud." To date, large banks and other regulated financial institutions have generally expressed a preference for private clouds, as they allow great flexibility in data processing and security. However, private clouds come at the expense of reduced scalability and increased costs.

As a result, some well-established institutions are now exploring hybrid models in collaboration with big cloud providers (Amazon Web Services, Google and Microsoft being the market share leaders), [16] where some activities could be performed in the public cloud while more sensitive activities (including hosting of sensitive data) could be performed in a private cloud.[17] Public cloud is also gaining in importance. According to the International Data Corporation (IDC), public cloud investments are growing quickly and the banking sector is now among the industries that are forecast to spend the most on public cloud services, with spending expected to climb to over $16.7 billion in 2018.[18]

1.4 Outsourcing to the Cloud – Benefits

Moving core and non-core services onto the cloud is a strategic decision that comes with benefits, costs and risks. There are multiple ways to analyse and group the potential benefits

[15] See, Cisco Global Cloud Index, cit.

[16] See, e.g., Microsoft, *Bank of America chooses the Microsoft Cloud to support digital transformation*, Microsoft News Center (2 October 2017); Microsoft, *UBS taps Microsoft Cloud to power business-critical tech*, Microsoft News Center (26 April 2017); Microsoft, *Redwood Bank puts business customers first with Microsoft Azure*, Microsoft News Center (16 May 2018); Caroline Donnelly, *AWS public cloud - Barclays Bank reveals details of its plans to go all-in on the AWS public cloud through adopting the principles of DevOps*, ComputerWeekly.com (25 June 2018); Penny Crosman, *Banking Apps that Matter Will Head to the Cloud in 2016*, American Banker (24 December 2015); James Kaplan and Ishaan Seth, *Banking on the cloud – Interview at Don Duet, Global Head of the Technology Division at Goldman Sachs*, McKinsey Interview (April 2016); Sharon Gaudin, *Capital One rides the cloud to tech company transformation*, ComputerWorld (5 December 2016); Finextra, *BBVA travels deeper into the cloud*, Finextra (21 October 2016).

[17] See, Penny Crosman, *Why the Hybrid Cloud Matters to Banks*, American Banker (11 October 2013); BBVA, *Banking Analysis - Cloud banking or banking in the clouds?*, cit., p. 3; European Banking Authority (EBA), *EBA Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech*, cit., p. 48.

[18] See, International Data Corporation (IDC), *Worldwide Public Cloud Services Spending Forecast to Reach $160 Billion This Year, According to IDC*, IDC (18 January 2018).

of cloud computing for banks and other regulated financial institutions, but almost all of them stem from the ability to obtain computing power and tools at a lower cost and with improved quality, flexibility and functionality.

First, the traditional IT model requires institutions to make a significant front-loaded investment in software and hardware, as well as a large life-cycle investment in professional staff to maintain servers and upgrade software. Contrary, hosting and running applications in the cloud could help lower the costs due to the sharing of resources, specialization, benefits from higher scalability and flexibility, along with the opportunity to avoid capital costs and incur predictable expenses, which scale up and down according to the business needs. In addition, outsourcing to cloud services providers could lead to a higher overall quality of the cloud services, compared with the quality level of institutions that have their own cloud.[19]

Second, the cloud could help banks and other regulated firms become more agile when developing new products and services[20] and could enable them to more rapidly innovate by reducing barriers to entry to acquire high quality, more convenient and on-demand computing resources.[21]

Third, cloud solutions often come with more flexible and usage-based pricing models, allowing banks and regulated financial institutions to select services required on a "pay-as-you-go" basis and to scale computing resources up or down as needed. The institutions with occasional usage

[19] See, BBVA, *Banking Analysis - Cloud banking or banking in the clouds?*, cit., pp. 5-6; European Banking Authority (EBA), *EBA Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech*, cit., p. 53; Penny Crosman, *Banks Pushed Toward Cloud Computing by Cost Pressures*, American Banker (10 March 2014); Andrew Rossiter, *Cloud adoption - how to truly maximise the benefits*, Finextra (28 July 2018); Nazneen Sherif, *Cloud set to replace in-house tech for banks 'No other way' to meet demands of FRTB, XVA and other changes, claim proponents*, RiskNet (5 February 2018); PWC, *Financial Services Technology 2020 and Beyond: Embracing disruption*, cit.

[20] See, Barb Darrow, *Pssst, Amazon Cloud Is Not Really New to Banks*, Fortune Magazine (25 February 2016); Emmanuel Sardet, *Clouds Could Save Banks*, American Banker (10 October 2012).

[21] See, Jonathan Charley, *The Cloud is ready for Banks but are Banks ready for the Cloud?*, Finextra (22 August 2017); Mervyn Kelly, *Embracing cloud culture: Why the financial sector must migrate*, Finextra (23 August 2018); IBM, *Cloud computing for banking - Driving business model transformation*, IBM White Paper (2013); Nagendra Bommadevara, Andrea Del Miglio, and Steve Jansen, *Cloud adoption to accelerate IT modernization*, Digital Mckinsey Report (April 2018); Citi Research, *Opportunities from Cloud Computing*, Citi Insights (2012).

could pay for resources only when they are using them; whilst institutions with more stable usage patterns could potentially benefit from the possibly lower cost of outsourcing services than in-house development. Related to the above, the cloud computing approach could help speed up deployment while maintaining flexibility. This capability means that, as demand changes, no significant and costly adjustments in infrastructures will be required to accommodate the changes.[22]

Fourth, cloud computing can provide increased data security and administrative control compared to traditional platforms. This is especially valid for smaller institutions that have limited IT budgets. Cloud solutions are the result of comprehensive planning, innovative design, and efficient operations where security is of paramount importance. Moreover, cloud platforms are developed with connectivity in mind and by specialized cloud services providers with very little legacy constraints, which makes them potentially more secure. Further, cloud computing could provide a more reliable business continuity solution due to the distributed nature of storage and processing, as well as the ability to move data more quickly. [23] In addition, as the global regulatory compliance landscape evolves, cloud service providers are demonstrating increased maturity and now offer a variety of cloud solutions and technologies to help clients create a proactive and automated approach to compliance and meet their compliance obligations. [24]

Fifth, a financial company's data can be an important competitive differentiator and an invaluable asset for gaining and maintaining market competitive advantages. To position the

[22] See, e.g., Salesforce UK, *Why Move To The Cloud? 10 Benefits Of Cloud Computing*, Salesforce UK (17 November 2015); PWC, *Financial Services Digital – Get your head in the cloud*, PWC Report (August 2016).
[23] Cfr., Cloud Security Alliance (CSA), *Cloud Computing Vulnerability Incidents: A Statistical Overview*, Cloud Vulnerabilities Working Group (2013); Penny Crosman, *Why Banks Are Finally Embracing Cloud Computing*, American Banker (12 August 2013); Penny Crosman, *What If Cloud Providers Are More Secure than Banks?*, American Banker (29 January 2015); American Banker, *Banks Look Up to the Cloud as Computer Security Concerns Recede*, American Banker (28 July 2016).
[24] See, PWC, *The changing landscape - How to use RegTech and make regulatory compliance your strategic advantage*, PWC (2016).

financial company for growth and innovation, the data should be harnessed, analysed and processed in real-time and with a high degree of accuracy. Given their flexibility, security and scalability, cloud solutions can help banks and other regulated financial institutions with data mining, transforming enterprise data and providing richer data analytics insights.[25] The result is a more flexible and agile operating environment, where data becomes the driving force behind decisions related to product development and the customer experience.

1.5 Outsourcing to the Cloud – Challenges

When a bank or other regulated financial entity moves functions (particularly core functions) onto the cloud, there are a number of primary challenges that must be addressed including the following.

First, banks and financial institutions must select the right service, deployment, and operating models and put in place robust control mechanisms to protect the confidentiality and security of financial and personal data and mission-critical applications. Even though as discussed above the cloud could be more secure, as the use of cloud computing grows, the number of attacks and vulnerabilities could grow as well.[26]

Second, transitioning from a traditional to a cloud computing based environment could entail switching costs that can be very high. Further, moving the data from one cloud provider to another could generate significant migration costs.[27]

[25] See, Accenture, *Moving to the Cloud, A Strategy for Banks in North America*, Accenture Consulting Report (2017); Ernst & Young (EY), *The digital bank: tech innovations driving change at US banks*, Ernst & Young LLP (2016); BSA | The Software Alliance, *Moving to the Cloud*, A Primer on Cloud Computing, Research Insights (2017); PWC, *How bankers can become innovation leaders again*, PWC Report (February 2017); PWC, *Get on my cloud: Banks head to the public cloud for unexpected reasons*, PWC Publication (2017).
[26] Cfr., Cloud Security Alliance (CSA), *Cloud Computing Vulnerability Incidents: A Statistical Overview*, cit; Ponemon Institute, *Data Breach: The Cloud Multiplier Effect*, Research Effect (2014); Mckinsey, *Making a Secure Transition to the Public Cloud*, Digital Mckinsey Report (2018).
[27] See, Bob Violino, *The Real Costs of Cloud Computing*, Computerworld (5 December 2011); BBVA, *Banking Analysis - Cloud banking or banking in the clouds?*, cit., pp. 7-8.

Third, banks and other regulated financial institutions, whether incumbents or new entrants, that move core services to the cloud often face a significant lack of negotiating power vis-a-vis large cloud service providers when negotiating specific contract clauses in light of relevant regulatory requirements (e.g., services levels and rights to audit for both the institution and the supervisory authority). [28] Related to the above, an additional challenge is "vendor lock-in", whereby a bank or another regulated financial institution may find it difficult to exit and migrate to a new cloud service providers or re-initialise a service.[29]

Fourth, the issue of transparency on chain outsourcing is another area to be taken into consideration. The use of subcontractors from a high-risk area/country could negatively impact the wider operational risk and reputation risk of the institution. [30] In addition, oversight of cloud providers may become even harder if they employ subcontractors. Therefore, many banking regulators require that certain financial data for banking customers remain in their home country. As a result, concerns and complexity may arise in regard to the storage location of relevant data.

Fifth, significant uncertainty remains as per the extent to which banks and other regulated financial institutions could rely on cloud arrangements (particularly public cloud) and how regulatory authorities would apply existing outsourcing rules to any such arrangement. Existing regulatory frameworks remain too high level and leave room for multiple interpretations,

[28] See, European Union Agency For Network and Information Security (ENISA), *Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations*, cit.; U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*, Report (July 2018), p. 45 (noting that "[s]everal large technology-focused firms have been central to the development of cloud computing, and the growth of the public cloud market in particular. To achieve the scale necessary to maximize the potential of this technology requires substantial resources. For this reason, these firms continue to dominate the market though competition has increased").

[29] See, European Banking Authority (EBA), *EBA Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech*, cit., pp. 51-53; Paul Schaus, *Regulatory Ambiguity Is Slowing Bank Adoption of Cloud Services*, American Banker (30 August 2016); Mark Nicholls, *Heads in the cloud: banks inch closer to cloud take-up - Regulatory guidance helps clear the way for greater adoption of cloud computing*, RiskNet (30 August 2017) (discussing the complexity of negotiating contractual terms with cloud providers).

[30] See, European Banking Authority (EBA), *EBA Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech*, cit., pp. 51-53.

different reporting criteria, lack of harmonised regulatory practices and/or fragmentation at national level and across jurisdictions. This, in turn, forms a barrier for banks and other regulated institutions using the cloud, which remain responsible for their operations and compliance with applicable laws and regulations regardless of the use of outsourcing. It also increases regulatory risks and compliance costs for regulated financial institutions and contributes to their reluctance to move core services to the cloud as any regulatory changes going forward could result into unforeseen costs.[31] The following chapters 2 to 4 discuss these challenges in greater detail, investigating recent regulatory developments and policy initiatives concerning the use of cloud computing and outsourcing practices by regulated financial institutions in the Europe (EU), the United Kingdom (UK) and the United States (US).

[31] See, European Union Agency For Network and Information Security (ENISA), *Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations*, cit.

CHAPTER 2. FRAMEWORK FOR OUTSOURCING TO THE CLOUD - EUROPEAN UNION (EU)

2.1 Recommendations on Outsourcing to Cloud Service Providers

2.1.A CEBS Guidelines (December 2006)

General outsourcing guidelines have been in place since 2006 in the form of the Committee of European Banking Supervisors guidelines on outsourcing ("CEBS guidelines 2006"),[32] which most of the member states have comprehensively transposed.[33]

Since the introduction of the CEBS guidelines 2006, outsourcing practices have rapidly progressed and cloud services have grown in importance as driver of innovation. Interest in financial sector for use of cloud service solutions has grown significantly and both the volume of financial information/data to be managed by institutions and demand for outsourcing to cloud service providers have been increasing.[34] Relative to other more traditional forms of outsourcing, cloud outsourcing services have evolved to be much more standardised. This, in turn, has allowed the services to be provided to a larger number of different customers in a much more automated manner and on a larger scale. As a result, outsourcing services can now offer a number of advantages, such as economies of scale, flexibility, operational efficiencies and cost-effectiveness.[35] On the other hand, the use of cloud services has also raised a number of challenges such as data and system security, governance and compliance challenges, and concentration risk.

[32] See, Committee of European Banking Supervisors (CEBS), *Guidelines on Outsourcing* (14 December 2006).
[33] See, European Banking Authority (EBA), *Consultation Paper - Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/20101*, EBA Consultation Paper 2017/06 (17 May 2017), p. 21 (noting that a survey carried out by the EBA in September 2015 indicates that "of the 24 national frameworks, 53% totally transposed, 38% partially transposed, 8% did not transpose the CEBS guidelines 2006 … [i]n all jurisdictions the general framework on outsourcing applies to cloud computing. In terms of specific national frameworks on cloud computing, the survey reveals that cloud computing is not subject to a specific framework in 14 member states (or 58% of jurisdictions). In 12 member states (or 50%) some specific frameworks apply.").
[34] Id., p. 4.
[35] Id., p. 5.

In light of the foregoing, the current EU regulatory framework now appears to be largely outdated and does not provide the necessary clarity in relation to the outsourcing process. The resulting uncertainty, in turn, leads to market inefficiency and entails a higher degree of operational risk in relation to outsourcing practices. In addition, the current regulatory framework does not fully cover important aspects such as data and systems security, confidentiality, legal and reputational risk and the exchange of information among the parties. The resulting lack of specific guidance, in turn, leads to a largely incomplete risk assessments of institutions in the prudential supervisory framework.[36]

In addition, the implementation of the CEBS guidelines 2006 varies significantly across jurisdictions, creating room for inconsistency in assessing outsourcing risk across EU jurisdictions. This, in turn, leads to a lack of comparability of supervisory practices (which is of significant importance given the cross-border nature of the cloud service),[37] does not facilitate the interpretation of the current supervisory expectations, and creates barriers to institutions using cloud services across EU jurisdictions.[38]

2.1.B EBA Consultation (May 2017) and Public Hearing (June 2017)

Against this scenario, on 18 May 2017, the European Banking Authority ("EBA") launched a public consultation setting out its guidance for the use of cloud service providers by financial institutions. [39] The proposed recommendations aim to address two core problems: the outdated framework on the process of outsourcing to cloud service providers; and the lack of harmonised regulatory practices across jurisdictions.

[36] Id., pp. 20-21.
[37] Ibidem.
[38] Id., p. 5 (noting that "[t]here are some differences in the national regulatory and supervisory frameworks for cloud outsourcing, for example with regard to the information requirements that institutions need to comply with.").
[39] See, European Banking Authority (EBA), *Consultation Paper - Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/20101*, cit.

The consultation period lasted for three months, from 18 May 2017 to 18 August 2017. A total of 47 responses were received, of which 37 were published on the EBA website. The Banking Stakeholder Group did not provide an opinion.[40] A public hearing also took place at the EBA's Canary Wharf, London premises on 20 June 2017.[41]

2.1.C EBA Final Recommendations (December 2017)

On 20 December 2017, the EBA published its final recommendations on outsourcing to cloud service providers ("Final Recommendations 2017").[42] The Final Recommendations 2017 apply from 1 July 2018 to credit institutions and investment firms as defined in Article 4(1) of Regulation (EU) No 575/2013 (Capital Requirements Regulation – CRR).[43]

The principle of proportionality applies throughout the Final Recommendations 2017, which should be employed in a manner proportionate to the size, structure and operational environment of the institution, as well as the nature, scale and complexity of its activities.

The Final Recommendations 2017 aim to: [44]

[40] See, European Banking Authority (EBA), *Recommendations on outsourcing to cloud service providers*, responses available at https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers/-/regulatory-activity/consultation-paper#responses_1848356.
[41] See, European Banking Authority (EBA) - Supervisory Convergence Unit, *EBA Recommendations on Outsourcing to Cloud Service Providers*, Public hearing (20 June 2017).
[42] See, European Banking Authority (EBA), *Final Report - Recommendations on outsourcing to cloud service providers*, EBA Final Report (20 December 2017).
[43] Unless otherwise specified, terms used and defined in Directive 2013/36/EU7 on capital requirements and in the CEBS guidelines have the same meaning in the Final Recommendations 2017. In addition, for the purposes of the Final Recommendations 2017 the following definitions apply:
- "cloud services" means "services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction";
- "public cloud" means "cloud infrastructure available for open use by the general public";
- "private cloud" means "cloud infrastructure available for the exclusive use by a single institution";
- "community cloud" means "cloud infrastructure available for the exclusive use by a specific community of institutions, including several institutions of a single group"; and
- "hybrid cloud" means "cloud infrastructure that is composed of two or more distinct cloud infrastructures".
[44] See, European Banking Authority (EBA), *Final Report - Recommendations on outsourcing to cloud service providers*, cit., pp. 20-22.

- Operational Objectives - Respond to the challenges arising from the current regulatory/supervisory framework by building on the guidance set forth in the CEBS guidelines 2006, update them and introduce more specific guidance on the use of cloud service solutions by credit institutions;
- Specific Objectives - Promote common EU-wide guidance for the use of cloud services by institutions and establish common practices across EU jurisdictions. These in turn would increase the risk assessment capabilities with respect to cloud services in the banking sector and would reduce uncertainty while providing enough room for flexibility to accommodate new challenges; and
- General Objectives - Ensure the consistent application of regulatory/supervisory criteria and strengthen prudential supervision.

The above would allow institutions to leverage the benefits of using cloud services, while ensuring that any related risks are adequately identified and managed.

The Final Recommendations 2017 focus on key areas for further supervisory alignment and/or clarification identified by stakeholders. These areas are discussed in detail below.

I) Materiality

The Final Recommendations 2017 contain specific directions on how to assess the materiality of cloud outsourcing. In particular, institutions should perform this assessment on the basis of guideline 1(f) of the CEBS guidelines 2006 and, with regard to outsourcing to cloud service providers, taking into account all of the following: [45]

[45] Id., p. 12.

a. the criticality and inherent risk profile of the activities to be outsourced, i.e. are those activities critical to the business continuity/viability of the institution and its obligations to customers;

b. the direct operational impact of outages, and related legal and reputational risks;

c. the impact that any disruption of the activity might have on the institution's revenue prospects; and

d. the potential impact that a confidentiality breach or failure of data integrity could have on the institution and its customers.

During the consultation period, a number of respondents have provided comments on the "materiality" requirement. The EBA acknowledges the comments and clarifies the following:[46]

- Qualitative and Quantitative Assessment Criteria - No qualitative or quantitative criteria for the materiality assessment are included in the Final Recommendations 2017 in line with the principle-based approach and to keep the recommendations future-proof. On the other hand, to facilitate convergence of regulation and supervision, the EBA agrees to provide advice on a more continuous basis after the publication of the Final Recommendations 2017 in the form of a Q&A including specific examples of what is regarded as material outsourcing in view of new developments;

- Repeat assessments - The materiality assessment should not be limited only to regulated activities;

- Application of new requirements - Institutions can rely and build on previous assessments in the case of very similar new cloud outsourcing activities;

[46] Id., pp. 33-35.

- Application of new requirements - The materiality assessments will apply as from the application date for any new cloud outsourcing arrangements or revisions of materiality assessments for existing arrangements as from that date;
- Risk appetite - Institutions remain responsible for setting their own risk appetites, as required by Article 76 of Directive 2013/36/EU and paragraph 23(b) of the EBA Guidelines on internal governance (EBA/GL/2017/11);
- Standalone basis - The Final Recommendations 2017 apply at the level of the entities indicated in the scope; and
- Assessment criteria – paragraph 1(b) - The outsourcing institution should consider the impact of potential outages when assessing the materiality of the outsourced activity.

II) Duty to Adequately Inform Supervisors

The materiality of cloud outsourcing determines whether an institution is required to adequately inform its competent authority about it. To foster convergence across Member States, in the Final Recommendations 2017 the EBA introduces specific guidance on the process that institutions should follow in informing their competent authorities about material cloud outsourcing and the information to be provided.[47]

The EBA clarifies that outsourcing institutions should adequately inform the competent authorities of material activities to be outsourced to cloud service providers on the basis of paragraph 4.3 of the CEBS guidelines 2006 and, in any case, make available to the competent authorities the following information:

a. the name of the cloud service provider and the name of its parent company (if any);
b. a description of the activities and data to be outsourced;

[47] Id., pp. 5-6, 12-13.

c. the country or countries where the service is to be performed (including the location of data);

d. the service commencement date;

e. the last contract renewal date (where applicable);

f. the applicable law governing the contract; and

g. the service expiry date or next contract renewal date (where applicable).

In addition to the foregoing, the competent authority may ask the outsourcing institution for additional information on its risk analysis for the material activities to be outsourced. [48]

The outsourcing institution should also maintain an updated register of information on all its material and non-material activities outsourced to cloud service providers at institution and group level[49] and should make available to the competent authority, on request, a copy of the outsourcing agreement and related information recorded in that register. Competent authorities retain the right to request *ad hoc* additional information.

Several respondents have provided comments on this requirement. Upon review of these comments, the EBA clarifies the following: [50]

- Timing - Consistent with CEBS guidelines, institutions should provide *ex ante* information to the competent authority about new material cloud outsourcing;

- Approval of material cloud outsourcing by competent authority - The information should be made available in a timely manner to allow the competent authority to

[48] Id., p. 13 (noting that "[t]hese include whether: (a) the cloud service provider has a business continuity plan that is suitable for the services provided to the outsourcing institution; (b) the outsourcing institution has an exit strategy in case of termination by either party or disruption of provision of the services by the cloud service provider; (c) the outsourcing institution maintains the skills and resources necessary to adequately monitor the outsourced activities.").
[49] Ibidem (providing a non-exhaustive list of information to be included in the register).
[50] Id., pp. 36-46.

consider whether the proposal raises prudential concern and take appropriate action if required;

- Applicability to new contracts and revision of legacy contracts – The requirements with regards to the register and the notification will apply as from the application date for any new materiality assessments or revisions of materiality assessments undertaken as from that date;
- Country where the service is performed (including location of data) – Both the country where the service is performed and the location where data are stored are deemed important information for the competent authority in view of transparency, the supervisory dialogue and supervisory access to these data;
- Group/entity level - The requirement to maintain the register applies at institution and group levels, although only for the European entities of the group. This will allow monitoring of the concentration risk;
- Notification - The requirement for institutions to adequately inform their competent authorities applies only to material cloud outsourcing. For non-material cloud outsourcing activities, institutions need to have the information referred to above available, but this information is not to be reported to the competent authorities; and
- Frequency of materiality assessment - The Final Recommendations 2017 do not prescribe any specific requirements in terms of the frequency for the review of materiality assessments for cloud outsourcing. This is to allow institutions sufficient flexibility in view of their specific requirements, taking into account the nature of the activities outsourced and the specificities of the arrangements and the cloud services context.

III) Access and Audit Rights

The Final Recommendations 2017 provide further guidance on how institutions and competent authorities can exercise access and audit rights in a risk-based and proportionate manner. [51]

The Final Recommendations 2017 clarify that the rights to audit and access should always be ensured contractually, regardless of the level of use of the cloud services. More specifically, outsourcing institutions should ensure that they have in place an agreement in writing with the cloud service provider whereby the latter agrees to provide to the institution (or any third party appointed for that purpose by the institution), the institution's statutory auditor and the competent authority supervising the outsourcing institution (or any third party appointed for that purpose by that authority):

a. full access to its business premises (head offices and operations centres), including the full range of devices, systems, networks and data used for providing the services outsourced (right of access); and

b. unrestricted rights of inspection and auditing related to the outsourced services (right of audit).

The Final Recommendations 2017 clearly indicate that the effective exercise of the rights of access and audit should not be impeded or limited by contractual arrangements. If the performance of audits or the use of certain audit techniques might create a risk for another client's environment, the Final Recommendations 2017 require that alternative ways providing a similar level of assurance should be agreed on. In addition, the outsourcing institution should ensure that the contractual arrangements do not impede its competent authority to carry out its supervisory function and objectives. [52]

[51] Id., pp. 12-13.
[52] Id., p. 15.

Although the audit and access rights should be contractually assured, the Final Recommendations 2017 clarify that these rights shall be exercised in a risk-based manner. The outsourcing institutions and cloud service providers should have the flexibility to agree on alternative ways to provide a similar level of assurance if certain audit techniques might create a risk for another client's environment or the cloud service provider's environment as well. In particular, where an outsourcing institution does not employ its own audit resources[53], it should consider using at least one of the following tools: (a) pooled audits organised jointly with other clients of the same cloud service provider, and performed by these clients or by a third party appointed by them; [54] or (b) third-party certifications and third-party or internal audit reports made available by the cloud service provider. [55] Depending on the circumstances of the case, the outsourcing institution should verify that the staff performing the audit or reviewing the third-party certification or service provider's audit reports have the right skills and knowledge to perform these activities.

The party intending to exercise its right of access (whether the institution, competent authority, auditor or third party acting for the institution or the competent authority) should provide prior notice in a reasonable time period of the onsite visit to a relevant business premise, unless this

[53] Id., p. 50 (noting that this "refers to both [the scenario] where an institution has the resources available but chooses not to employ them and [the scenario] where an institution does not have the resources and therefore cannot employ them.").
[54] Id., p. 14 (noting that this would help "use audit resources more efficiently and to decrease the organisational burden on both the clients and the cloud service provider").
[55] Id., p. 15 (clarifying that "the use of these certifications and reports is subject to the following conditions: (i) the outsourcing institution ensures that the scope of the certification or audit report covers the systems and the controls identified as key by the outsourcing institution; (ii) the outsourcing institution thoroughly assesses the content of the certifications or audit reports on an ongoing basis, and in particular ensures that key controls are still covered in future versions of an audit report and verifies that the certification or audit report is not obsolete; (iii) the outsourcing institution is satisfied with the aptitude of the certifying or auditing party; (iv) the certifications are issued and the audits are performed against widely recognised standards and include a test of the operational effectiveness of the key controls in place; and (v) the outsourcing institution has the contractual right to request the expansion of scope of the certifications or audit reports to some systems and/or controls that are relevant. The number and frequency of such requests for scope modification should be reasonable, and legitimate from a risk management perspective.").

is not possible due to an emergency or crisis situation. The cloud service provider, on the other hand, is required to fully cooperate with the relevant party in connection with the onsite visit.[56]

Respondents to the consultation have raised a number of comments with regards to access and audit rights. The EBA has reviewed these comments and clarifies that: [57]

- Feasibility of full access/audit – Proposed alternatives - Virtual/logical access is deemed to be *de facto* included in the audit tools both for institutions and competent authorities;
- Access to business premises - Access to business premises (head offices and operations centres) should include access to data centres; and
- Third-party certification/audits against widely recognised standards - Certification should be provided by an independent third party and cannot be fulfilled by self-assessment.

IV) Security of Data and Systems

Building on the CEBS guidelines 2006, the Final Recommendations 2017 clarify that the outsourcing institution should conduct through due diligence[58] and put in place written outsourcing contract arrangements and service level agreements that: oblige the outsourcing service provider to protect the confidentiality, integrity and traceability of the data, information and systems in the context of the intended cloud outsourcing; define an appropriate level of continuity of services provided by the outsourcing service provider; properly address the needs of the outsourcing institution with respect to quality and performance; and include specific

[56] Id., p. 16.
[57] Id., pp. 47 - 56.
[58] Id., pp. 16 - 17.

measures where necessary for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture.

The Final Recommendations 2017 further require that, following the execution of the relevant contractual arrangements, security aspects be monitored and reviewed on an ongoing basis and corrective measures be promptly undertaken as needed. [59]

In response to comments from various respondents to the consultation, the EBA notes that: [60]

- Risk-based approach - The risk-based approach should enable the outsourcing institution to exercise its responsibility to determine the adequate level of safety and define the necessary security measures, taking into account the specific outsourcing context and only then will engage with the cloud service provider; and
- Material and non-material outsourcing - The recommendations regarding security of data and system apply to both material and non-material cloud outsourcing arrangements.

V) Location of Data and Data Processing

Cloud service providers often operate a geographically dispersed computing infrastructure that entails the regional and/or global distribution of data storage and processing.[61] In this regard, the Final Recommendations 2017 set out specific requirements for data and data processing locations in the context of cloud outsourcing. Specifically, building on the CEBS guidelines 2006, the Final Recommendations 2017 clarify that institutions should take special care when entering into and managing outsourcing agreements undertaken outside the EEA because of possible data protection risks and risks to effective supervision by the supervisory authority. Further, the outsourcing institutions should adopt a risk-based approach to data and data

[59] Ibidem.
[60] Id., pp. 56 - 58.
[61] Id., p. 6.

processing location considerations when outsourcing to a cloud environment. The assessment should account for a number of factors, including legal risks and compliance issues, political and security stability of the jurisdictions in question, the laws (including laws on data protection and insolvency provisions) and the law enforcement provisions in place in those jurisdictions. The outsourcing institutions should ensure that these risks are kept within acceptable limits commensurate with the materiality of the outsourced activity. [62]

A few respondents to the consultation have raised comments on the location of data and data processing requirements. In response, the EBA clarifies that: [63]

- Risk-based approach - Institutions are requested to adopt a risk-based approach in considering data and data processing locations, taking into account the legal framework in force; and
- Additional references to data protection rules - Data protection is highlighted in the recommendations in view of its potential impact on prudential risks, the provisions are specifically linked to the outsourcing context and should not duplicate any other regulations.

VI) Chain Outsourcing (Sub-Contracting)

Cloud outsourcing is more dynamic in nature than traditional outsourcing set-ups and chain outsourcing (subcontracting) is often extensively used. The EBA recognises a need for greater certainty about the conditions under which subcontracting can take place in the case of cloud outsourcing.

In this regard, the Final Recommendations 2017 specify that the outsourcing institution should agree to chain outsourcing only if the subcontractor will also fully comply with the obligations

[62] Id., p. 17.
[63] Id., pp. 59 - 60.

existing between the outsourcing institution and the outsourcing service provider and should take appropriate steps to address the risk of any weakness or failure in the provision of the subcontracted activities having a significant effect on the outsourcing service provider's ability to meet its responsibilities under the outsourcing agreement. The EBA further requires the outsourcing institution should carefully delineate which type of activities are excluded from potential subcontracting and require the cloud service provider to retain full responsibility for and oversight of those services that it has subcontracted. The outsourcing agreement should also require *ex ante* notification by the cloud outsourcing provider of any planned significant changes to the subcontractors or the subcontracted services named in the initial agreement that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. The outsourcing institution's consent is not required, since this would be overly burdensome from a practical perspective. However, the institution should, in any case, retain the right to terminate the contract if planned changes to subcontracted services would have an adverse effect on the risk assessment of the agreed outsourced services. [64]

In response to comments raised by respondents to the consultation, the EBA further clarifies that:[65]

- Monitoring - The outsourcing institution remains responsible for monitoring the overall service it receives, regardless of whether it is provided by the cloud service provider or by a subcontractor further down the chain;
- Access and Audit Rights and Sub-Contractors - The outsourcing institution should make sure that access and audit rights can also be exercised at the level of the subcontractor; and

[64] Id., pp. 17 - 18.
[65] Id., pp. 53 - 55.

- Assessment - The outsourcing institution retains the flexibility to decide which activities should be excluded from subcontracting, what would constitute significant changes in subcontracting and what would be the most appropriate timeframe for the notifications, all in view of its particular requirements, risk assessments and the cloud service arrangement it has put in place with the cloud service provider(s).

VII) Contingency Plans and Exit Strategies

The Final Recommendations 2017 set forth specific guidance for institutions on the contractual and organisational arrangements for contingency plans and exit strategies that should be in place in the context of cloud outsourcing.

Specifically, the Final Recommendations 2017 provide that the outsourcing institution should: plan and implement arrangements (including a contingency planning and a clearly defined exit strategy) to maintain the continuity of its business in the event that the provision of services by an outsourcing service provider fails or deteriorates to an unacceptable degree; include a termination and exit management clause that allows transfer of the activities being provided by the outsourcing service provider to another outsourcing service provider or back to the outsourcing institution; and ensure that it is able to exit cloud outsourcing arrangements, if necessary, without undue disruption to its provision of services or adverse effects on its compliance with the regulatory regime and without detriment to the continuity and quality of its provision of services to clients. [66]

Several respondents have raised comments on the above requirements. Upon review of this comments, the EBA clarifies that: [67]

[66] Id., pp. 18 - 19.
[67] Id., pp. 66 - 71.

- Material and non-material outsourcing - The requirement to develop contingency plans and exit strategies, apply to both material and non-material cloud outsourcing;
- Flexibility - The recommendations allow sufficient flexibility for outsourcing institutions to determine the appropriate continuity arrangements, taking into account the nature of the activities outsourced and the specificities of the arrangements and the cloud services context. Any backup solutions should be practical and sufficiently tested where appropriate;
- Testing - The testing of exit strategies is to be performed only "where appropriate" and can be done in the form that the outsourcing institution deems most appropriate, whether it be a desktop exercise, live testing or some other form; and
- Triggering of an exit plan - It is important that there are key risk indicators in place that can trigger an exit. The design and setting of such indicators is critical and needs to sufficiently take into account actual impact.

2.2 Guidelines on Outsourcing to Cloud Providers

2.2.A EBA Consultation (June 2018)

The Final Recommendations 2017 discussed in prior paragraphs constitute a first step towards the creation of a EU shared cloud outsourcing framework. Following their publication in December 2017, the EBA has further engaged with the sector and provided additional guidance to assist convergence in the implementation of the recommendations.

Significantly, on June 22, 2018, the EBA launched a consultation on draft Guidelines on outsourcing arrangements, which integrate the Final Recommendation 2017 and are intended to update and replace the CEBS Guidelines 2006 ("Proposed Guidelines 2018"). [68] Comments

[68] See, European Banking Authority (EBA), *Consultation Paper - EBA Draft Guidelines on Outsourcing arrangements*, EBA Consultation Paper 2018/11 (22 June 2018).

on the Proposed Guidelines 2018 are invited by September 24, 2018. The EBA will hold a public hearing on the proposed Guidelines on September 4, 2018. Following closure of the consultation, the EBA will then finalize the draft guidelines and the CEBS Guidelines 2006 will be repealed once the new guidelines take effect.

While the CEBS guidelines 2006 apply to outsourcing by credit institutions, the Proposed Guidelines 2018 have a wider scope, aiming at establishing a more harmonised framework for outsourcing arrangements of all financial institutions that are within the scope of the EBA's mandate. These include credit institutions, investment firms, payment institutions and electronic money institutions.

The Proposed Guidelines 2018 take into account and are consistent with the current requirements under the Capital Requirements Directive (CRD), Markets in Financial Instruments Directive (MiFID), E-money Directive, Revised Payment Services Directive (PSD2) and Bank Recovery and Resolution Directive (BRRD), as well as the respective delegated regulations. The Proposed Guidelines 2018 should be read in conjunction with and without prejudice to the EBA guidelines on internal governance, the EBA guidelines on common procedures and methodologies for the supervisory review and evaluation process and the EBA guidelines on ICT risk assessment under the Supervisory Review and Evaluation process (SREP). For payment institutions, the Proposed Guidelines 2018 should also be read in conjunction with the EBA guidelines on the information to be provided for the authorisation of payment institutions under PSD2, the EBA guidelines on security measures for operational and security risks under PSD2 and the EBA guidelines on major incident reporting under PSD2.

The Proposed Guidelines 2018 cover five main areas: (1) proportionality and group application; (2) the nature of outsourcing arrangements; (3) the applicable governance framework; (4) the outsourcing process; and (5) guidelines on outsourcing addressed to

competent authorities. A separate Annex provides an illustrative template that could be used for complying with the requirement in the Proposed Guidelines 2018 to maintain a register of all outsourcing arrangements at institution and group level where applicable.

All requirements within the Proposed Guidelines 2018 are subject to the principle of proportionality. This means that they are to be applied in a manner that is appropriate, taking into account in particular the institution's and payment institution's size, internal organisation and the nature, scope and complexity of their activities.

The Proposed Guidelines 2018 provide a clear definition of outsourcing (that is in line with the related Commission delegated regulation (EU) 2017/565 supplementing MiFID II).[69] They further specify the criteria to determine whether an outsourced activity, service, process or function (or part of it) is "critical or important" to ensure a more harmonised assessment of the criticality or importance of functions.[70]

With regard to intra-group outsourcing, the Proposed Guidelines 2018 clarify that intra-group outsourcing is subject to the same regulatory framework as outsourcing to service providers outside the group and that institutions and payment institutions should: ensure that the selection of a group entity to which a function is outsourced is based on objective reasons; the conditions of the outsourcing arrangement are set at arm's length; explicitly deal with conflicts of interest; clearly identify all relevant risks and detail the mitigation measures and controls to ensure that the outsourcing arrangements with affiliated entities do not impair the institution's or payment institution's ability to comply with the relevant regulatory and legislative framework. [71]

[69] Id, p. 18 (The term "outsourcing" is defined as "an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity, or parts thereof that would otherwise be undertaken by the institution, the payment institutions or the electronic money institution itself.").
[70] Id, pp. 33 – 34.
[71] Id, pp. 11 – 12, 21 – 22.

With regard to outsourcing to service providers located outside the EU, the Proposed Guidelines 2018 clarify that these must be subject to additional safeguards that ensure that they do not lead to an undue increase of risks both for institutions and payment institutions and their competent authorities or impair the ability of competent authorities to effectively supervise institutions and payment institutions. [72]

Institutions and payment institutions should have sound internal governance arrangements which include a clear organisational structure. The Proposed Guidelines 2018 include requirements which aim at ensuring that:

- there is effective day-to-day management by the management body;
- there is effective oversight by the management body;
- there is sound outsourcing policy and outsourcing processes;
- institutions and payment institutions have an effective and efficient internal control framework, including with regard to their outsourced functions;
- all the risks associated with the outsourcing of critical or important functions are identified, assessed, monitored, managed, and reported and as appropriate mitigated;
- there are appropriate plans for exit from outsourcing arrangements of critical or important functions; and
- competent authorities remain able to effectively supervise institutions and payment institutions, including the functions that have been outsourced.

Moreover, the Proposed Guidelines 2018 clarify that the responsibility of the institutions' and payment institutions' management body cannot be outsourced and outsourcing must not lead

[72] Id, pp. 7 – 11.

to a situation where an institution or a payment institution becomes an "empty shell" or a "letter-box entity". [73] In particular, institution or a payment institution should:

- meet all the conditions of their authorisation at all times;
- retain a clear and transparent organisational framework and structure that enable them to comply with all of their regulatory obligations;
- exercise appropriate oversight and be able to manage the risks that are created by outsourcing arrangements of critical or important functions; and
- retain sufficient resources and capacities to perform the foresaid activities.

In addition, the Proposed Guidelines 2018 clarify aspects related to the due diligence process and risk assessment before entering in such arrangements, the contractual arrangements, the monitoring and documentation of outsourcing arrangements.

Specifically, the Proposed Guidelines 2018 provide that before entering into any outsourcing arrangement, institutions and payment institutions should: assess whether the planned outsourcing concerns a critical or important function; undertake appropriate due diligence on the prospective service provider; identify and assess all relevant risks and conflicts of interest of the outsourcing arrangement; consider the consequences of where the service provider is located (within or outside the EU); consider whether the service provider is part of the institution's accounting consolidation group and, if so, the extent to which the institution controls it or has the ability to influence its actions.[74]

A number of factors shall be considered when conducting due diligence on a potential service providers, including whether: it has appropriate and sufficient ability, capacity, resources, organisational structure and, if applicable, required authorisations and permissions to perform

[73] Id, pp. 24 – 26.
[74] Id, pp. 32, 35 – 37.

its activities; it implements appropriate technical and organisational measures for the transfer, processing and storing of personal or confidential data in accordance with applicable data protection laws; it acts in a manner consistent with the institution's values and code of conduct.[75]

In addition, the Proposed Guidelines 2018 specify a set of aspects that should be encoded within the written outsourcing agreement. These include: a clear description of the outsourced function; the term of the agreement; applicable laws; whether the sub-outsourcing of a critical or important function is permitted; the location(s) where the critical or important function will be provided and/or where relevant data will be kept; notice periods; and audit and access rights both for the outsourcing institution and for competent authorities. For the outsourcing of critical or important function, contractual arrangements should also cover, among others: the right of the institution or the payment institution to monitor the service provider's performance on an ongoing basis; the agreed service levels; the reporting obligations of the service provider to the institution or payment institution; the respective parties' financial obligations; insurance arrangements; business continuity plans; termination rights; and insolvency or discontinuing of business operations arrangements.[76]

Furthermore, institutions and payments institutions are required to maintain a register of all outsourcing arrangements at institution and group level as applicable and should make available the register to the competent authority in a common data base format within each supervisory review and evaluation process, but at least every 3 years and in any case on request by competent authority. [77]

[75] Id, pp. 34 – 35.
[76] Id, pp. 37 – 45.
[77] Id, pp. 30 – 32, 45.

The Proposed Guidelines 2018 further specify that in case of outsourcing of critical or important functions, sub-outsourcing (or material changes thereto) requires *ex ante* notification to the institutions and payment institutions. The outsourcing arrangements should also ensure, where appropriate, that the institution or the payment institution has the right to object against intended sub-outsourcing or that an explicit approval is required and that has the right to terminate the agreement in case of undue sub-outsourcing. In addition, institutions and payment institutions should only agree to sub-outsourcing if the subcontractor undertakes to: comply with all applicable laws, regulatory requirements and contractual obligations; oversee the services being sub-contracted to ensure that all contractual obligations between the service provider and the institution or the payment institution are still met; obtain prior approval from the institution and the payment institution before sub-outsourcing data subject to General Data Protection Regulation (GDPR); and grant the institutions, payment institutions and competent authority the same contractual rights of access and audit as those granted by the service provider.[78]

Finally, institutions and payment institutions should ensure that service providers comply with appropriate information security standards. Where relevant, institutions and payment institutions should also define data and system security requirements within the outsourcing agreement and monitor compliance therewith on an ongoing basis. Where cloud outsourcing involves the handling or transfer of sensitive data, institutions and payment institutions should adopt a risk-based approach to data storage and data processing location(s) and information security considerations. [79]

[78] Id, pp. 39 - 40.
[79] Id, p. 40.

2.3 European Commission's Fintech Action Plan (March 2018)

On 8 March 2018, the European Commission ("Commission") published its FinTech Action Plan for a more competitive and innovative European financial sector ("Fintech Action Plan 2018"). [80] The Fintech Action Plan 2018 has three main objectives:

- Enabling innovative business models to reach EU scale;
- Supporting the uptake of technological innovation in the financial sector; and
- Enhancing security and integrity of the financial sector.

For each of these objectives, the Fintech Action Plan 2018 sets out a number steps. One of the key steps under the second objectives is the proposal of removing existing obstacles that hinder the greater use of outsourcing to cloud services.

In this regard, the Commission acknowledges that cloud computing can increase the efficiency of the digital infrastructure which underpins financial services. In particular, the Commission notes that outsourcing data processing and storage capacity to cloud service providers can reduce the cost of hosting, infrastructure and software for firms and can help streamline IT expenditure. At the same time, it can ensure greater performance, flexibility and adaptability.

Regulated firms that outsource activities to a cloud service provider must comply with all applicable legal and regulatory requirements. These includes proper risks management, data protection and appropriate oversight by supervisors.

Following its consultation with a number of stakeholders, the Commission recognizes that the absence of harmonisation of national rules and different interpretations of outsourcing rules have resulted in significant uncertainties over financial supervisory authorities' expectations with regard to cloud outsourcing, which in turns have limited and discouraged the use of cloud

[80] See, European Commission, *FinTech Action Plan: For a More Competitive and Innovative European Financial Sector*, European Commission Report (8 March 2018).

computing services by regulated firms. As a result, cloud providers and regulated firms increasingly need legal clarity, improved supervision and a convergence in oversight practices across Europe.

Against the describe scenario, the Commission recognises the importance of developing a regulatory framework that facilitate greater and secure use of outsourcing to cloud services, which goes beyond the scope of existing sectorial initiatives driven by the EBA,[81] the European Supervisory Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA), and expresses the view that the additional certainty could be achieved if supervisory expectations were expressed in the form of formal guidelines of the European Supervisory Authorities (ESAs). To this end, the Commission invites the ESAs to provide guidelines on outsourcing to cloud service providers in 2019.

In parallel, in the context of the Communication on Building the European Data Economy,[82] the Commission invites cloud stakeholders to develop cross-sectoral self-regulatory codes of conduct to facilitate switching between cloud service providers, as well as representatives from the financial sector to enable easier data porting also for financial institutions. In particular, the Commission encourages the development of standard contractual clauses for cloud outsourcing by financial institutions to address, among others, audit requirements, reporting requirements and the determination of materiality of the activities to be outsourced. This work should build on cross-sectorial cloud stakeholder efforts and ensure financial sector involvement to, and close collaboration through, this process.

[81] See paragraphs 2.1 and 2.2.
[82] See, European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – "Building a European Data Economy"*, European Commission 2017/9 (10 January 2017).

Further, in line with the proposed regulation establishing a framework for the free flow of non-personal data in the EU,[83] the Commission expresses the intention to gather and liaise with relevant stakeholders (including cloud users, cloud providers and regulatory authorities) in 2018, which will be tasked to develop information and communications technology standards to improve the interoperability and portability of the cloud.

[83] See, European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union*, European Commission 2017/0228 (13 September 2017).

CHAPTER 3. FRAMEWORK FOR OUTSOURCING TO THE CLOUD – THE UNITED KINGDOM (UK)

3.1 FCA Guidance on Using the Cloud in Financial Services (Revised July 2018)

In November 2015, the Financial Conduct Authority ("FCA") issued its draft guidance to help firms and service providers understand the FCA's expectations when outsourcing to the cloud and other third-party IT services ("FCA Draft Guidance 2015").[84] The consultation closed on 12 February 2016. [85] The FCA published the final guidance in July 2016, which has been further updated in July 2018 to reflect the publication of the EBA Final Recommendations 2017 discussed above and changes to relevant legislation ("FCA Final Guidance 2018").[86]

The FCA Final Guidance 2018 is consistent with the FCA's effort to promote greater innovation and competition in the financial services sector which, in turn, can create better services for consumers. In developing the guidance, the FCA has worked in close cooperation with Project Innovate to identify areas where the regulatory framework needs to adapt to enable further innovation in the interests of consumers.[87]

---

[84] See, Financial Conduct Authority (FCA), *Proposed guidance for firms outsourcing to the 'cloud' and other third-party IT services*, FCA GC 15/6 (November 2015).

[85] The main points from feedback received by the FCA on the FCA Draft Guidance 2015, along with the FCA's responses, are summarised in Annex – Feedback Statement to the FCA Final Guidance 2018.

[86] See, Financial Conduct Authority (FCA), *Guidance for firms outsourcing to the 'cloud' and other third-party IT services*, FCA FG 16/5 (Revised July 2018). The FCA Final Guidance 2018 is not binding and is intended to illustrate ways in which firms can comply with the relevant rules. The FCA expects firms to take note of the FCA Final Guidance 2018 and, where appropriate, use it to inform their systems and controls on outsourcing. Furthermore, the guidance is not exhaustive, nor should it be read in isolation. Firms should consider the FCA Final Guidance 2018 in the context of their overarching obligations under the regulatory system. Compliance with the FCA Final Guidance 2018 will generally indicate compliance with the FCA outsourcing requirements. The Prudential Regulation Authority (PRA) has different statutory objectives and so firms that are subject to PRA regulation should confirm their approach with the PRA. The FCA Final Guidance 2018 does not bind the PRA or the courts. The FCA has further clarified that the FCA Final Guidance 2018 has been designed in the context of the existing UK and EU regulatory framework and will be monitored to assess whether any changes would be required due to any intervening changes in the UK regulatory framework, including as a result of any Brexit negotiations.

[87] Pursuant to its statutory mandate to promote competition in financial services, in October 2014 the FCA established Project Innovate to encourage innovation in the interests of consumers and to promote competition and growth in the financial and banking services industry by supporting small and large businesses that are developing products that could genuinely improve services for consumers. Three of the most important initiatives launched under Project Innovate are the Innovation Hub, the Regulatory Sandbox, and the Advice Unit. See, Financial Conduct Authority (FCA), *Project Innovate: Call for Input*, FCA (July 2014); Financial Conduct

The FCA has successfully supported both new and existing firms to use cloud and other IT service solutions in a compliant manner. In the FCA Final Guidance 2018, the FCA clearly acknowledges that there is no fundamental reason why cloud services (including public cloud services) cannot be implemented, with appropriate consideration, in a manner that complies with the FCA's rules. The FCA views the proper use of outsourcing to the cloud and other third-party IT services as a way to increase flexibility to the service that firms receive, enable innovation and bring benefits to firms, their consumers, and the wider market. As the market continues to evolve rapidly, with frequent new innovative offerings, using cloud and other third-party IT providers, may bring benefits to firms such as cost efficiencies, increased security, and more flexible and cost-effective infrastructure capacity. These benefits, in turn, can help promote the emergence of new entrants and support more effective competition.[88]

On the other hand, in the FCA Final Guidance 2018 the FCA acknowledges (following extensive discussions with various stakeholders) that cloud outsourcing can also introduce risks that need to be properly identified, monitored and mitigated. These risks primarily affect the degree of control exercised by the firm and specific issues such as data security. [89]

The FCA Final Guidance 2018 is relevant to firms who are interested in outsourcing to the cloud and other third-party IT services. It may also be of interest to third party IT providers (including cloud providers), trade associations and consumer groups, law firms and other advisers, and auditors of financial services firms. The FCA Final Guidance 2018 does not apply to a bank, building society, designated investment firm or IFPRU investment firm as defined

Authority (FCA), *Project Innovate: Call for Input - Feedback Statement*, FCA (October 2014). For additional information on the initiatives launched under Project Innovate, visit the FCA's website at https://www.fca.org.uk/firms/fca-innovate.

[88] See, Financial Conduct Authority (FCA), *Guidance for firms outsourcing to the 'cloud' and other third-party IT services*, cit., pp. 2-3.

[89] Ibidem (noting that "cloud customers may have less control of the supplier, for example the degree to which they can tailor the service provided, and of the data, such as where data are stored.").

in the FCA Handbook to whom the EBA Final Recommendations 2017 on outsourcing to cloud service providers discussed in prior sections are addressed.

For the purposes of the FCA Final Guidance 2018, "cloud" is defined as to encompass "a range of IT services provided in various formats over the internet. This includes, for example, private, public or hybrid cloud, as well as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)." [90] In this regard, the FCA Final Guidance 2018 clarifies that from a regulatory perspective, the exact form of the service used does not, in itself, alter the regulatory obligations placed on firms. Moreover, where a third party delivers services on behalf of a regulated firm – including a cloud provider – this is considered outsourcing and firms need to consider the relevant regulatory obligations and how they comply with them.[91]

The FCA Final Guidance 2018 sets out a detailed list of considerations for firms covering the full lifecycle from pre-contract tasks, to contract management and exit planning. The key principles underpinning these considerations are the identification and management of operational risks associated with using third parties. Key areas of consideration are discussed in detail below.

First, with regard to legal and regulatory considerations, firms should undertake a variety of pre-contractual due diligence tasks. These include:[92]

- compiling a business case supporting the outsource;
- verifying the service is suitable for the firm and considering any relevant legal or regulatory obligations;
- reviewing the contract to ensure it complies with the FCA's rules and does not adversely affect operational risk;

[90] Id., pp. 2, 4.
[91] Id., pp. 4 - 5.
[92] Id., p. 5.

- maintaining an accurate record of contracts between the firm and its service provider(s);
- determining which jurisdiction(s) the service provider's business premises are located in and how that affects the firm's outsource arrangements;
- determining whether the contract with the service provider is governed by the law and subject to the jurisdiction of the UK. If it is not, it should still ensure effective access to data and business premises for the firm, auditor and relevant regulator;
- determining any additional legal or regulatory obligations and requirements that may arise, including under GDPR; and
- identifying all the service providers in the supply chain and ensuring that the requirements on the firm can be complied with throughout the supply chain. Similarly, where multiple providers form part of an overall arrangement (as distinct from a chain) the requirements should be complied with across the arrangement.

Second, the FCA Final Guidance 2018 provides further considerations covering risk management activities which must be completed pre-contract and during the terms of the outsourcing agreement.[93] Specifically, the firms should, among others:

- carry out, and properly document, a risk assessment to identify relevant risks and identify steps to mitigate them;
- identify current industry good practice, relevant regulator's rules and guidance to support their decision making;
- assess the overall operational risks associated with the regulated service for which the firm is responsible and assign responsibility for managing them;
- monitor concentration risk and consider what action it would take if the outsource provider failed;

[93] Id., pp. 6 - 7.

- require prompt and appropriately detailed notification of any breaches or other relevant events arising including the invocation of business recovery arrangements; and
- ensure the contract(s) provide for the remediation of breaches and other adverse events.

Third, the FCA recommends firms to take account of the provider's adherence to international standards (e.g., the ISO 27000 series) as relevant to the provision of IT services both when conducting initial due diligence and as part of ongoing monitoring of service provision, the logic being that a service provider's adherence to such standards indicates robust data security processes.[94]

Fourth, in the FCA Final Guidance 2018, the FCA clearly indicates that, when engaging in outsourcing arrangements, regulated firms retain full responsibility and accountability for discharging all of their regulatory responsibilities.[95] Because of this, the FCA recommends that firms should:

- be clear about the service being provided and the allocation of responsibility and accountability between the firm and its service provider(s);
- allocate responsibility for the day-to-day and strategic management of the service provider;
- ensure staff have sufficient skills and resources to oversee and test the outsourced activities;
- identify, monitor and mitigate against the risks arising;
- properly manage an exit or transfer from an existing third-party provider; and
- verify that suitable arrangements for disputes resolution exist.

[94] Ibidem.
[95] Id., pp. 7 - 8.

Fifth, the FCA recommends a separate data security risk assessment of the firm's technology assets and the service provider. [96] In this context, the FCA Final Guidance 2018 provides that a firm should:

- agree, and review periodically, a data residency policy with the service provider at the outset, which sets out the jurisdictions in which the firm's data can be stored, processed and managed;
- ensure the service provider's data loss and breach notification processes are aligned with the firm's risk appetite and legal or regulatory obligations;
- consider how data will be segregated (if using a public cloud);
- take appropriate steps to mitigate security risks so that the firm's overall security exposure is acceptable; and
- consider data sensitivity and how the data are transmitted, stored and encrypted, where necessary.

Sixth, the FCA Final Guidance 2018 reiterates that cloud outsourcing is subject to data protection law, and that specific ICO guidance on this point should apply. [97]

Seventh, with regard to effective access to data, the FCA Final Guidance 2018 aligns with the FCA's existing rules in the FCA Handbook (i.e. SYSC 8.1.8(9)) and Article 31(2)(i) MiFID Org Regulation. Specifically, the FCA defines "data" widely to include "firm, personal, customer and transactional data". This includes for example HR vetting procedures or system audit trails and logs. [98] In this context, firms should:

- ensure that notification requirements on accessing data, as agreed with the service provider are reasonable and not overly restrictive;

[96] Id., p. 8.
[97] Ibidem.
[98] Id., pp. 8 - 9.

- ensure there are no restrictions on the number of requests the firm, its auditor or the regulator can make to access or receive data;
- advise the service provider that the regulator will not enter into a NDA with the service provider but will treat any information disclosed in accordance with the confidentiality obligation set out in the Financial Services and Markets Act (FSMA), sections 348 to 349;
- ensure that, where a firm cannot disclose data for any reason, the contract enables the regulator or the firm's auditor to contact the service provider directly; and
- ensure that data are not stored in jurisdictions that may inhibit effective access to data for UK regulators.

Eighth, the FCA Final Guidance 2018 addresses the issue of accessing business premises, which constitutes a largely debated point with service providers being very sensitive to any access to premises such as data centres.[99] In this regard, the FCA clarifies that "business premises" has a broad meaning and covers premises such as head offices, operations, but does not necessarily includes data centres. It further indicates that for firms where the business premises access requirements apply as rules, their contracts must allow for access to business premises. The focus should be on which business premises are relevant for the exercise of effective oversight. As the FCA clarifies, this does not necessarily require access to all business premises. For example, service providers may, for legitimate security reasons, limit access to some sites – such as data centres. [100]

Ninth, the FCA Final Guidance 2018 further acknowledges that outsourcing supply chains are often complex. In this regard, the FCA recommends that regulated firms that do not directly contract with the outsource provider should review sub-contracting arrangements relevant to

[99] Id., pp. 9 - 10.
[100] Ibidem.

the provision of the regulated activity to determine whether these enable them to continue to comply with applicable regulatory requirements. In addition, the regulated firms should consider how the service providers work together and how easily a service provider's services will interface with a firm's internal systems or other third-party systems (e.g., agency banking arrangements for payments). [101]

Tenth, the FCA Final Guidance 2018 requires firms to agree comprehensive change management process to govern changes to processes and procedures so that new risks are not introduced as services are changed. [102]

Eleventh, the FCA Final Guidance 2018 clarifies that a firm should have in place, and regularly update and test, appropriate arrangements to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption of the outsourced services.[103] Firms should also have documented and fully tested exit plans, termination arrangements, and migration plans to ensure that they are able to exit outsourcing plans, should they wish to, without undue disruption to their provision of services, or their compliance with the regulatory regime. [104]

Finally, the FCA Final Guidance 2018 provides that outsourced services should be organised in a way that does not create additional complexity or a barrier to the resolution or orderly wind-down of the firm. [105]

[101] Id., pp. 10 - 11.
[102] Id., p. 11.
[103] Ibidem.
[104] Id., p. 12.
[105] Id., p. 11.

CHAPTER 4. FRAMEWORK FOR OUTSOURCING TO THE CLOUD – THE UNITED STATES (US)

4.1 FFIEC Statement on Outsourced Cloud Computing (July 2012)

On 10 July 2012, the Federal Financial Institutions Examination Council ("FFIEC") issued a statement cautioning financial institutions to undertake thorough due diligence and risk assessment for outsourced cloud computing arrangements (the "FFIEC Statement").[106]

Although a financial institution's use of outsourced cloud computing can have many potential benefits, such as cost reduction, flexibility and speed, the FFIEC statement indicates that the fundamentals of risk and risk management defined in the FFIEC Information Technology Examination Handbook (IT Handbook), particularly the Outsourcing Technology Services Booklet (Outsourcing Booklet), are as applicable to cloud computing as to other forms of information technology outsourcing.[107]

In particular, the FFIEC Statement highlights six key elements of outsourced cloud computing implementation and risk management: (i) due diligence; (ii) vendor management; (iii) auditing; (iv) information security; (v) legal, regulatory and reputational considerations; and (vi) business continuity planning. The FFIEC Statement reiterates the importance of these elements, while identifying particular areas of concern for each with respect to outsourced cloud computing, including data handling and storage.

In the context of due diligence activities, the FFIEC Statement identifies data classification, data segregation and recoverability as potential issues in outsourced cloud computing arrangements.[108]

---

[106] See, Federal Financial Institutions Examination Council (FFIEC), *Outsourced Cloud Computing*, Federal Financial Institutions Examination Council Statement (10 July 2012).
[107] Id., p. 1.
[108] Id., p. 2.

With regard to information security controls, the FFIEC Statement advises that financial institutions should implement and maintain a comprehensive data inventory and suitable data classification process, appropriate access restrictions to customer data through identity and access management, effective monitoring of security security-related threats, incidents, and events on both financial institutions' and servicers' networks, comprehensive incident response methodologies and appropriate forensic strategies for investigation and evidence collection.[109]

According to the FFIEC Statement, verifying data handling procedures, the adequacy and availability of backup data and whether providers share facilities are important considerations. Vendors that are unfamiliar with regulatory requirements may require additional controls, and multi-tenant deployments may increase the need for data protection through encryption and assurances that proper controls are in place to restrict tenant access solely to their respective data.[110]

The FFIEC expects financial institutions to identify, mitigate, understand and appropriately address attendant legal, regulatory and reputational risks, noting that assessing compliance may be more complex and difficult in an environment where the cloud computing service provider processes and stores data overseas or comingles the financial institution's data with data from other customers that operate under diverse legal and regulatory jurisdictions.[111]

Consistent with these statements, in the context of vendor management, the FFIEC also identifies a number of factors that should be specifically addressed in outsourced cloud computing agreements. These include: (a) ownership, location(s) and format(s) of data; (b) dispute resolution; (c) the ability of the cloud-computing service provider to remove non-public personal information ("NPPI") from all locations where it is stored at the conclusion of a

[109] Id., p. 3.
[110] Ibidem.
[111] Id., p. 4.

service contract to be assessed before entering into a relationship with any such service provider; and (d) the vendor's obligations with respect to the financial institutions' responsibilities for compliance with privacy laws, for responding to and reporting security incidents, and for fulfilling regulatory requirements to notify customers and regulators of any breaches.[112]

In light of the foregoing, the FFIEC Statement concludes that, while the fundamentals of risk and risk management defined in the IT Handbook apply to cloud computing as they do to other forms of outsourcing, "[c]loud computing may require more robust controls due to the nature of the service." [113]

4.2 FED, OCC and FDIC Joint Advance Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards (October 2016)

In October 2016, the U.S. Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Board and the Office of the Comptroller of the Currency (OCC) jointly issued an advanced notice of proposed rulemaking seeking comments on a new set of enhanced cyber risk management standards for large and interconnected entities under their supervision and those entities' service providers.[114] A number of leading financial firms and technology companies submitted comment letters in response to this joint advance notice of proposed rulemaking and the various questions set forth therein.[115] Among them of particular interest are the responses submitted by Amazon Web Services ("AWS") and Microsoft Corporation ("Microsoft").

[112] Ibidem.
[113] Id., p. 4.
[114] The advance notice of proposed rulemaking on enhanced cyber risk management standards was published in the Federal Register on 26 October 2016. See, Board of Governors of the Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), *Joint Advance Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards*, Federal Reserve System Docket No. R-1550 and RIN 7100-AE-61, OCC Docket ID OCC-2016-0016 and RIN 1557-AE06, FDIC RIN 3064-AE45 (October 19, 2016).
[115] Comments were due by February 17, 2017. See, Board of Governors of the Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), *Proposed*

AWS provided responses to three specific sections applicable to commercial cloud providers: sector-critical systems; internal and external dependency; and incident response, cyber resilience, and situational awareness.[116] In its response, AWS notes that, in evaluating the scope of applicability for future rulemaking, the FFIEC should consider that cloud service providers already comply with stringent cyber security requirements and that AWS customers (including entities regulated by the FFIEC already) have the freedom necessary under the AWS services to control and maintain their own cybersecurity posture in the cloud. [117] Further, AWS expresses the view that the FFIEC should leverage a risk-based, outcome-focused approach to classifying systems as critical. This type of classification should depend on: (i) purpose for which it is used, (ii) impact to the financial services institution or sector from a prolonged disruption, failure and/or compromise, and (iii) risk posture of the system or function. When considering these three factors, according to AWS, cloud services do not rise to the threshold established for sector-critical systems.[118] Moreover, AWS observes that any final rule should leverage existing industry and where appropriate governmental standards that establish best practices for cyber security governance[119] and a requirement should allow for a risk assessment of the chances of a disruption to the service and a time frame commensurate with the risk. [120]

Similarly, in its response, Microsoft recommends that the proposed standards expressly recognize that covered entities may use third-party service providers to support sector-critical systems, and the standards be appropriately tailored in their application to such third-party

Rulemaking on Enhanced Cyber Risk Management Standards – Extension of Comment Period, Joint Press Release (January 13, 2017). Comments submitted in response to the Proposed Rulemaking on Enhanced Cyber Risk Management Standards are available on the Federal Reserve's website at https://www.federalreserve.gov/apps/foia/ViewComments.aspx?doc_id=R%2D1550&doc_ver=1.

[116] See, Amazon Web Services, *Commentary to the Advance Notice of Proposed Rulemaking (ANPR) on Enhanced Cyber Risk Management Standards* (February 17, 2017).

[117] Id., p. 3.

[118] Id., p. 5.

[119] Ibidem.

[120] Id., p. 6.

service providers.[121] Further, Microsoft suggests that identification of covered services and sector-critical systems be based on whether those services and systems perform functions that are truly critical within the financial services industry, and sector-critical standards be applied in a manner that recognizes the inherent capabilities of the underlying technologies. Microsoft also recommends that the standards be implemented as a combination of a regulatory requirement for covered entities to maintain a risk management framework for cyber risks, along with a policy statement or guidance that describes minimum expectations for such a framework. As per the FFIEC Cybersecurity Assessment Tool, Microsoft notes that it could be an appropriate measurement instrument for quantifying cyber risk, subject to some improvement. In the context of cloud and other online services, Microsoft recommends that the proposed standards recognize that service provider commitments regarding service availability and downtime can provide covered entities with assurance concerning service resilience. Finally, with regard to mitigation strategies to address black swan scenarios, Microsoft encourages the agencies to consider the significant security and resilience advantages that cloud services can offer in relation to managing and responding to constantly evolving cyber risks.

4.3 U.S. Department of the Treasury Report (July 2018)

Following extensive consultation with a wide range of stakeholders, including financial services firms, federal and state regulators, consumer and other advocacy groups, experts and investors, the U.S. Department of the Treasury (the "U.S. Treasury") released a report titled "A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation" in July 2018 (the "Report July 2018").[122] The report is the fourth in a series of

[121] See, Microsoft Corporation, *Comments on Joint Advance Notice of Proposed Rulemaking, Enhanced Cyber Risk Management Standards* (February 17, 2017).
[122] See, U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*, cit.

reports produced in response to Executive Order 13772, which sets out seven core principles for regulating the U.S. financial system (the "Core Principles").[123]

In the Report July 2018, the U.S. Treasury notes emerging trends in financial intermediation, such as rapid advances in technology, increased efficiencies from the rapid digitalization of the economy and the abundance of capital available to propel innovation. Against this scenario, the Report July 2018 provides recommendations for the regulation of nonbank financial companies, the fintech sector and other forms of financial market innovation through the lens of the Core Principles and identifies opportunities to accelerate innovation in the United States consistent with those principles.

Cloud technology is one of the key areas the Report July 2018 identifies for positive development.[124] Significantly, similarly to the UK and EU regulators, the U.S. Treasury recognises the potential for cloud to help companies:

- Scalability, Speed, and Cost – Innovate more rapidly and bring product and services to market quickly by reducing barriers to entry to acquire high quality computing; and rapidly scale up and down the use of computing capacity to meet changing needs;
- Security and Resilience – Enhance their security by leveraging large cloud service providers' resources and expertise in building and maintaining state-of-the-art and comprehensive IT security and deploying it on a global basis across their platforms; enhance their strategies for business continuity and operational resilience by

[123] The U.S. Department of the Treasury previously delivered three reports related to the Executive Order. The first report covers the depository system, including banks, savings associations, and credit unions of all sizes, types, and regulatory charters. See, U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Banks and Credit Unions*, Report (June 2017). The second report covers capital markets: debt, equity, commodities and derivatives markets, central clearing, and other operational functions. See, U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Capital Markets*, Report (October 2017). The third report covers the asset management and insurance industries, and retail and institutional investment products and vehicle. See, U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Asset Management and Insurance*, Report (October 2017).

[124] See, U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*, cit., pp. 44 seq.

leveraging large cloud service providers' ability to rapidly re-distribute data across geographically diverse storage and processing centers; and

- Enabling Large-Scale Data Storage and Management – Store and process vast amounts of data at scale; extract and analyse usable insights from large datasets with greater agility and effectiveness in line with firms' business models and strategies.

On the other hand, and consistent with the views expressed by the UK and EU regulators, the U.S. Treasury acknowledges that the growth of cloud services raises a number of new challenges, including potentially high transitioning costs, security and data privacy considerations, regulatory compliance standards, unrealized or over-sold cost savings compared to in-house IT management, and connectivity speed. Nevertheless, the U.S. Treasury notices that many of these challenges can be addressed through appropriate adaptation of cloud computing services, such as deployment of a private or hybrid cloud, choice of service model, provision of data availability and resilience measures, and other appropriate risk management of outsourcing contracts.

In addition, the U.S. Treasury notes that financial institutions have been adopting cloud computing in a variety of ways. Many firms have deployed private cloud or hybrid cloud structures, which help them gain the benefits of cloud while also retaining greater control of their IT and satisfying regulatory or other requirements; whilst other financial institutions have adopted public cloud, including for volatile workloads associated with periodic stress testing, risk modelling and simulations, or other requirements where computing resources may need to rapidly scale (e.g., payments).[125]

[125] See, BBVA, *Banking Analysis - Cloud banking or banking in the clouds?*, cit.

All three types of cloud service models – SaaS, IaaS and PaaS - are also being deployed within financial services. [126]

Similar to UK and EU regulators, the U.S. Treasury acknowledges that financial institutions in the U.S. have been slower to adopt cloud than other sectors, but there is an expectation that cloud adoption will increase.[127]

In this context, the U.S. Treasury recognises that financial services firms currently face several regulatory challenges related to the adoption of cloud, which are driven by a number of factors including: a regulatory regime that has yet to be sufficiently modernized to accommodate cloud and other innovative technologies; regulatory fragmentation with a large number of regulators regulating the use of cloud in financial services; inconsistent regulatory requirements; and inconsistencies in regulators' experience with cloud computing and in the knowledge base at the examiner level.[128]

In particular, with regard to cloud outsourcing and in line with the UK and EU's views discussed in prior chapters, the U.S. Treasury notes that financial services are hesitant to adopt or migrate to cloud services due in part to inconsistent and/or unclear regulatory outsourcing guidance. For example, significant uncertainty arises over whether regulators' third-party service provider guidance applies to all or only some cloud deployment models (IaaS, PaaS, and SaaS) and whether regulators would accept a broader migration to the cloud for core activities of critical relevance for the economy and involving the processing of highly sensitive

[126] See, U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*, cit., p. 48.
[127] Id., pp. 48 - 49 (quoting a study by Citi foreseeing large U.S. banks to process the vast majority of their computing needs on cloud platforms within the next 5-10 years. See, Citi Research, *U.S. Banks: Transformational Changes Unfolding in Journey to the Cloud*, Citi Report (January 10, 2018)).
[128] Id., p. 50 (quoting a study published by the industry group Cloud Security Alliance in March 2015, reporting that 71% of respondents to a survey on cloud adoption by financial services firms cited "regulatory restrictions" as a key reason for their delay in adopting cloud technology, second only to "data security concerns" that was cited by 100% of respondents. See, Cloud Security Alliance, *How Cloud is Being Used in the Financial Sector*: Survey Report (March 2015), p. 10.).

and important customer data. In addition, the U.S. Treasury acknowledges that some of the regulatory guidance is not well adapted to cloud. For example, compliance with regulatory guidance that requires financial institutions to maintain physical access audit rights can present significant challenges. Similarly, "chain outsourcing" issues can present challenges to banks looking to partner with third parties that use cloud services.

Against this scenario, the U.S. Treasury recommends that federal financial regulators modernize their requirements and guidance (e.g., vendor oversight) to better provide for appropriate adoption of cloud computing, with the aim of reducing unnecessary barriers to the prudent and informed migration of activities to the cloud. Specific actions that U.S. regulators should take include: formally recognizing independent U.S. audit and security standards that sufficiently meet regulatory expectations; clarifying how audit requirements may be met; setting clear and appropriately tailored chain outsourcing expectations; and providing staff examiners appropriate training to implement agency policy on cloud services.

Finally, the U.S. Treasury recommends that financial regulators should: establish a cloud and financial services working group so that cloud policies can benefit from deep and sustained understanding by regulatory authorities; support potential policies by engaging key industry stakeholders, including providers, users, and others impacted by cloud services; seek to promote the use of cloud technology within the existing U.S. regulatory framework to help financial services companies reduce the risks of noncompliance and the costs associated with meeting multiple and sometimes conflicting regulations; and seek supervisory or appropriate technological solutions to potential data security, privacy, availability, and access issues in connection with the use of cloud.[129]

[129] Id., p. 51 footnote 131 (arguing that "[o]ngoing work by industry groups and other public-private sector partnerships can perhaps be instructive in helping regulators achieve harmonization, within and across jurisdictions, of standards and requirements to provide greater regulatory certainty". In this sense, see National Institute of Standards and Technology, *NIST Cloud Computing Standards Roadmap*, Special Publication 500-291, Version 2 (July 2013).

CHAPTER 5. BUILDING A NEW DIGITAL BANK ON THE CLOUD

While the majority of incumbent banks and long-established institutions have been hesitant in implementing cloud infrastructure models (particularly for core operations) and still tackle cloud on a piecemeal basis, a new wave of challenger banks is now transforming banking systems and business models by leveraging the power of the cloud and taking a more comprehensive, enterprise-wide approach to cloud strategies.

5.1 Starling Bank and AWS Cloud

An interesting example is UK-based challenger bank Starling Bank ("Starling"), which is built on Amazon's cloud.[130] Starling's CEO Anne Boden says processes that once cost $30 million can be done for $30,000, thanks in large part to the cloud.[131] Starling uses Amazon Web Services (AWS) Cloud to deliver and scale a secure infrastructure automatically and on demand, to release new features every day, to grow and evolve quickly. The challenger bank primarily uses Amazon CloudFormation to provision and manage its AWS services, and Amazon EC2 to run its applications on virtual machines in the Amazon cloud. It also uses S3 to assist with data storage and retrieval, Amazon RDS to run its relational and scalable database in the cloud, and AWS Lambda to help build a responsive and on-demand application and run code without provisioning or managing servers. "[AWS]'s been a large part of what's enabled us to essentially build a bank in a year," says Starling's former chief technology officer and now Senior Technical Advisor Greg Hawkins tells Techworld.[132]

When questioned about the key challenges in their journey to the cloud, Starling's CEO Anne Boden acknowledges that the challenger bank has made a big effort in explaining to regulators

[130] See, AWS, *Breaking the Banking Mould - How Starling Bank is disrupting the banking industry*, AWS Case Study (2017).
[131] See, Martin Veitch, *AWS: Bigger than Diageo or BA… and with more to come*, IDG (27 November 2017).
[132] See, Thomas Macaulay, *How Starling Bank uses AWS to run its platform in the cloud*, TechWorld (14 December 2017).

and auditors about the benefits, resilience and security of the cloud. But, as she notes "… when people realise what is possible in the cloud then great things happens."

5.2 Monzo Bank and AWS Cloud

Another interesting example is UK's leading digital challenger bank Monzo Bank ("Monzo"). Founded in 2015, Monzo has grown into a fully regulated bank handling over £1 billion worth of transactions for almost a million customers in the UK. In 2017 alone, Monzo grew from 65 to 275 employees and added 400,000 new customers.[133]

Two key technical decisions that Monzo has taken in its early days have been critical to its exponential growth: running its core banking services in the AWS Cloud and opting for a microservices architecture. With regard to the former, Monzo runs more than 400 core-banking microservices on AWS, using services including Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), and Amazon Simple Storage Service (Amazon S3). Monzo also segregates parts of its infrastructure using separate AWS accounts, so if one account is compromised, critical parts of the infrastructure in other accounts remain unaffected. The challenger bank uses one account for production, one for non-production, and one for storing and managing users' login information and roles within AWS. The privileges that are assigned in the user account then allow users to read or write to production and non-production accounts. Using AWS CloudTrail, Monzo logs activity to Amazon S3 buckets in another separate audit account. Nobody can log in to that account, so the records remain immutable. Amazon S3 is also used in a final backup account to store encrypted backups from the production account. Monzo migrated from its old account to a multi-account setup in less than a day and "[i]n the future, routine management will be even easier", says Vans-Colina engineer at Monzo.[134] With regard to the latter, microservices have always been the lifeblood

[133] See, AWS, *How Monzo built a digital bank on AWS for over 500,000 customers,* AWS Case Study (2017).
[134] Ibidem.

of Monzo's core banking application. As Matt Heath, a distributed systems engineer at Monzo, explains "[Monzo] currently runs 400 of them, and the list is set to grow exponentially". Each service runs on Kubernetes, a platform that deploys, scales, and manages containerized applications. Kubernetes itself runs on a cluster of Amazon EC2 instances in the AWS EU (Ireland) Region across three Availability Zones.[135]

One of the initial reasons Monzo chose AWS was the need to comply with banking regulations. Monzo's Founder and CEO Tom Blomfield notes "AWS differentiates itself as a forward-thinking cloud vendor that understands enterprise concerns and works with regulators and customers to launch new features. To allay regulators' fears, it has services such as AWS CloudTrail, which produce AWS API call logs to enable security analysis, resource change tracking, and compliance auditing."[136] Blomfield further observers that "[a] lot of people have taken existing core banking software and deployed it to the cloud. Instead, we've written it from scratch and deployed it to the cloud. Taking a monolithic software package and sticking it on AWS, you lose a lot of the benefits of containerization and enormous scale of infrastructure." [137]

5.3 Metro Bank and Rackspace Cloud

A further example of a new digital bank built on cloud is the UK-based challenger bank Metro Bank, which has moved its IT infrastructure to a Rackspace managed cloud solution.[138] Founded in 2010, Metro Bank has already launched more than 45 stores and has now the ambitions plan to reach 100 stores by 2020, providing banking services for both personal and business customers. Metro Bank uses a Rackspace Dedicated Server Solution. It also uses

[135] Ibidem.
[136] Ibidem.
[137] Ibidem.
[138] See, Rackspace, *Metro Bank - First new high street bank in 100 years chose a Rackspace solution to support its rapid growth*, Rackspace Case Study (2016).

DevOps to roll out new services as it moves towards automated management. The infrastructure includes disaster recovery capabilities.

According to Raspace, Metro Bank was able to "seamlessly" migrate its entire infrastructure, including its core banking operations (run on Temenos' T24), digital offerings (Backbase) and ATMs, to Rackspace's cloud offering. The migration project took 12 months and was delivered on time, on budget and without any costly downtime. As reported by Rackspace, this migration process has reduced the challenger bank's close-of-business processing time by 50% and report production time by two-thirds.[139]

Metro Bank's CTO David Young explains: "… [w]e grow exponentially every year and the biggest risk is not being able to match demand. Rackspace ensures we have the capability to horizontally scale our infrastructure and applications, and they do it in such a way that I never need to worry about IT maintenance."[140]

[139] Ibidem.
[140] Ibidem.

CONCLUSION

Banks and other financial institutions are increasingly exploring the transformative power of cloud computing to evolve and innovate their enterprise at high speed. This transformation, which took place slowly at first, is accelerating and is now targeting central applications and core operations and systems.

However, regulatory inefficiencies, inconsistencies in oversight, lack of clear guidance by regulators and uncertainty as per the application of existing regulation to cloud outsourcing still prevent banks and other financial institutions from taking full advantage of cloud's ability and capabilities. New guidance and recommendations on cloud recently issued across the EU, UK and the U.S. aim at overcoming these obstacles by establishing a clear framework and increasing homogeneity in supervisory expectations regarding the technical security, risk and operational requirements of cloud services.

Looking ahead, as regulators work to keep pace with cloud technologies and further refine their guidance, greater collaboration among financial institutions, cloud service providers and regulators will be needed. On one hand, regulators will need to strike the right balance between regulation and allowing innovation to flourish. On the other hand, banks and financial institutions will need to improve their engagement with various stakeholders and strengthen their interactions with policymakers and regulators to help them navigate the complexities of, and educate them around opportunities associated with, the use of cloud technologies. This, in turn, is expected to lead to a more efficient and sound regulatory environment for the cloud, which will offer increased security while encouraging further innovation.

REFERENCES

A. Industry Reports

Accenture, *Moving to the Cloud, A Strategy for Banks in North America*, Accenture Consulting Report (2017).

BBVA, *Banking Analysis - Cloud banking or banking in the clouds?*, BBVA Research U.S. Economic Watch (29 April 2016).

AWS, *Breaking the Banking Mould - How Starling Bank is disrupting the banking industry*, AWS Case Study (2017).

AWS, *How Monzo built a digital bank on AWS for over 500,000 customers*, AWS Case Study (2017).

Bommadevara, Nagendra, Andrea Del Miglio, and Steve Jansen, *Cloud adoption to accelerate IT modernization*, Digital McKinsey Report (April 2018).

BSA | The Software Alliance, *Moving to the Cloud, A Primer on Cloud Computing*, Research Insights (2017).

Capgemini Financial Services, *Cloud Computing in Banking. What banks need to know when considering a move to the cloud*, Financial Services Report (2011).

Cisco Global Cloud Index: Forecast and Methodology 2016–2021, White Paper (2018).

Citi Research, *U.S. Banks: Transformational Changes Unfolding in Journey to the Cloud*, Citi Report (January 10, 2018).

Citi Research, *Opportunities from Cloud Computing*, Citi Insights (2012).

Cloud Security Alliance (CSA), *Cloud Computing Vulnerability Incidents: A Statistical Overview*, Cloud Vulnerabilities Working Group (2013).

Cloud Security Alliance (CSA), *How Cloud is Being Used in the Financial Sector: Survey Report*, Report (March 2015).

Cloud Security Alliance, *How Cloud is Being Used in the Financial Sector: Survey Report* (March 2015).

Ernst & Young (EY), *The digital bank: tech innovations driving change at US banks*, Ernst & Young LLP (2016).

Gartner, Inc., *Press Release – Gartner Forecast Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018*, Gartner (12 April 2018).

HTF Research, *Cloud Adoption*, HFT Research Paper – Sponsored by GFT (June 2018).

IBM, *Cloud computing for banking - Driving business model transformation*, IBM White Paper (2013).

International Data Corporation (IDC), *Worldwide Public Cloud Services Spending Forecast to Reach $160 Billion This Year*, According to IDC, IDC (18 January 2018).

Kaplan, James and Ishaan Seth, *Banking on the cloud – Interview at Don Duet, Global Head of the Technology Division at Goldman Sachs*, McKinsey Interview (April 2016).

McKinsey, *Making a Secure Transition to the Public Cloud*, Digital McKinsey Report (2018).

Mell, Peter and Timothy Grance, *The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology (NIST), Special Publication 800-145 (September 2011).

Microsoft, *UBS taps Microsoft Cloud to power business-critical tech*, Microsoft News Center (26 April 2017).

Microsoft, *Bank of America chooses the Microsoft Cloud to support digital transformation*, Microsoft News Center (2 October 2017).

Microsoft, *Redwood Bank puts business customers first with Microsoft Azure*, Microsoft News Center (16 May 2018).

National Institute of Standards and Technology, *NIST Cloud Computing Standards Roadmap*, Special Publication 500-291, Version 2 (July 2013).

Ponemon Institute, *Data Breach: The Cloud Multiplier Effect*, Research Effect (2014).

PWC, *Financial Services Technology 2020 and Beyond: Embracing disruption*, PWC Report (2016).

PWC, *The changing landscape - How to use RegTech and make regulatory compliance your strategic advantage*, PWC (2016).

PWC, *How bankers can become innovation leaders again*, PWC Report (February 2017).

PWC, *Get on my cloud: Banks head to the public cloud for unexpected reasons*, PWC Publication (2017).

Rackspace, *Metro Bank - First new high street bank in 100 years chose a Rackspace solution to support its rapid growth*, Rackspace Case Study (2016).

RightScale Inc., *RightScale 2018 State of the Cloud Report, Data to Navigate Your Multi-Cloud Strategy*, Report (2018).

Salesforce UK, *Why Move To The Cloud? 10 Benefits Of Cloud Computing*, Salesforce UK (17 November 2015).

B. Articles and Blog Posts

American Banker, *Banks Look Up to the Cloud as Computer Security Concerns Recede*, American Banker (28 July 2016).

Campbell, Lee, *SaaS vs On-Premise and what that means for everyone involved*, Finextra (23 August 2018).

Charley, Jonathan, *The Cloud is ready for Banks but are Banks ready for the Cloud?*, Finextra (22 August 2017).

Crosman, Penny, *Why Banks Are Finally Embracing Cloud Computing*, American Banker (12 August 2013).

Crosman, Penny, *Why the Hybrid Cloud Matters to Banks*, American Banker (11 October 2013).

Crosman, Penny, *Banks Pushed Toward Cloud Computing by Cost Pressures*, American Banker (10 March 2014).

Crosman, Penny, *What If Cloud Providers Are More Secure than Banks?*, American Banker (29 January 2015).

Crosman, Penny, *Small Banks Take a Test Flight in the Cloud*, American Banker (21 June 2015).

Crosman, Penny, *Banking Apps that Matter Will Head to the Cloud in 2016*, American Banker (24 December 2015).

Donnelly, Caroline, *AWS public cloud - Barclays Bank reveals details of its plans to go all-in on the AWS public cloud through adopting the principles of DevOps*, ComputerWeekly.com (25 June 2018).

Finextra, *BBVA travels deeper into the cloud*, Finextra (21 October 2016)

Gaudin, Sharon, *Capital One rides the cloud to tech company transformation*, ComputerWorld (5 December 2016).

Kelly, Mervyn, *Embracing cloud culture: Why the financial sector must migrate*, Finextra (23 August 2018).

Macaulay, Thomas, *How Starling Bank uses AWS to run its platform in the cloud*, TechWorld (14 December 2017).

Nicholls, Mark, *Heads in the cloud: banks inch closer to cloud take-up - Regulatory guidance helps clear the way for greater adoption of cloud computing*, RiskNet (30 August 2017).

Rossiter, Andrew, *Cloud adoption - how to truly maximise the benefits*, Finextra (28 July 2018).

Schaus, Paul, *Regulatory Ambiguity Is Slowing Bank Adoption of Cloud Services*, American Banker (30 August 2016).

Sherif, Nazneen, *Cloud set to replace in-house tech for banks 'No other way' to meet demands of FRTB, XVA and other changes, claim proponents*, RiskNet (5 February 2018).

Veitch, Martin, *AWS: Bigger than Diageo or BA… and with more to come*, IDG (27 November 2017).

Violino, Bob, *The Real Costs of Cloud Computing*, Computerworld (5 December 2011).

C. Regulations and Policy Initiatives - European Union

Committee of European Banking Supervisors (CEBS), *Guidelines on Outsourcing* (14 December 2016).

European Banking Authority (EBA), *Consultation Paper - Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/20101*, EBA Consultation Paper 2017/06 (17 May 2017).

European Banking Authority (EBA) - Supervisory Convergence Unit, *EBA Recommendations on Outsourcing to Cloud Service Providers*, Public hearing (20 June 2017).

European Banking Authority (EBA), *Final Report - Recommendations on outsourcing to cloud service providers*, EBA Final Report (20 December 2017).

European Banking Authority (EBA), *EBA Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech*, EBA Report (3 July 2018).

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – "Building a European Data Economy"*, European Commission Report (10 January 2017).

European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union*, European Commission 2017/0228 (13 September 2017).

European Commission, *FinTech Action Plan: For a More Competitive and Innovative European Financial Sector*, European Commission Report (8 March 2018).

European Union Agency for Network and Information Security (ENISA), *Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations*, ENISA Report (7 December 2015).

D. Regulations and Policy Initiatives – The United Kingdom

Financial Conduct Authority (FCA), *Project Innovate: Call for Input*, FCA (July 2014).

Financial Conduct Authority (FCA), *Project Innovate: Call for Input - Feedback Statement*, FCA (October 2014).

Financial Conduct Authority (FCA), *Proposed guidance for firms outsourcing to the 'cloud' and other third-party IT services*, FCA GC 15/6 (November 2015).

Financial Conduct Authority (FCA), *Guidance for firms outsourcing to the 'cloud' and other third-party IT services*, FCA FG 16/5 (Revised July 2018).

E. Regulations and Policy Initiatives – The United States

Board of Governors of the Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), *Joint Advance Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards*, Federal Reserve System Docket No. R-1550 and RIN 7100-AE-61, OCC Docket ID OCC-2016-0016 and RIN 1557-AE06, FDIC RIN 3064-AE45 (October 19, 2016).

Board of Governors of the Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), *Proposed Rulemaking on Enhanced Cyber Risk Management Standards – Extension of Comment Period*, Joint Press Release (January 13, 2017).

Selected Responses:

Amazon Web Services, *Commentary to the Advance Notice of Proposed Rulemaking (ANPR) on Enhanced Cyber Risk Management Standards* (February 17, 2017).

Microsoft Corporation, *Comments on Joint Advance Notice of Proposed Rulemaking, Enhanced Cyber Risk Management Standards* (February 17, 2017).

Federal Financial Institutions Examination Council (FFIEC), *Outsourced Cloud Computing*, Federal Financial Institutions Examination Council Statement (10 July 2012).

U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Banks and Credit Unions*, Report (June 2017).

U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Capital Markets*, Report (October 2017).

U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Asset Management and Insurance*, Report (October 2017).

U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*, Report (July 2018).