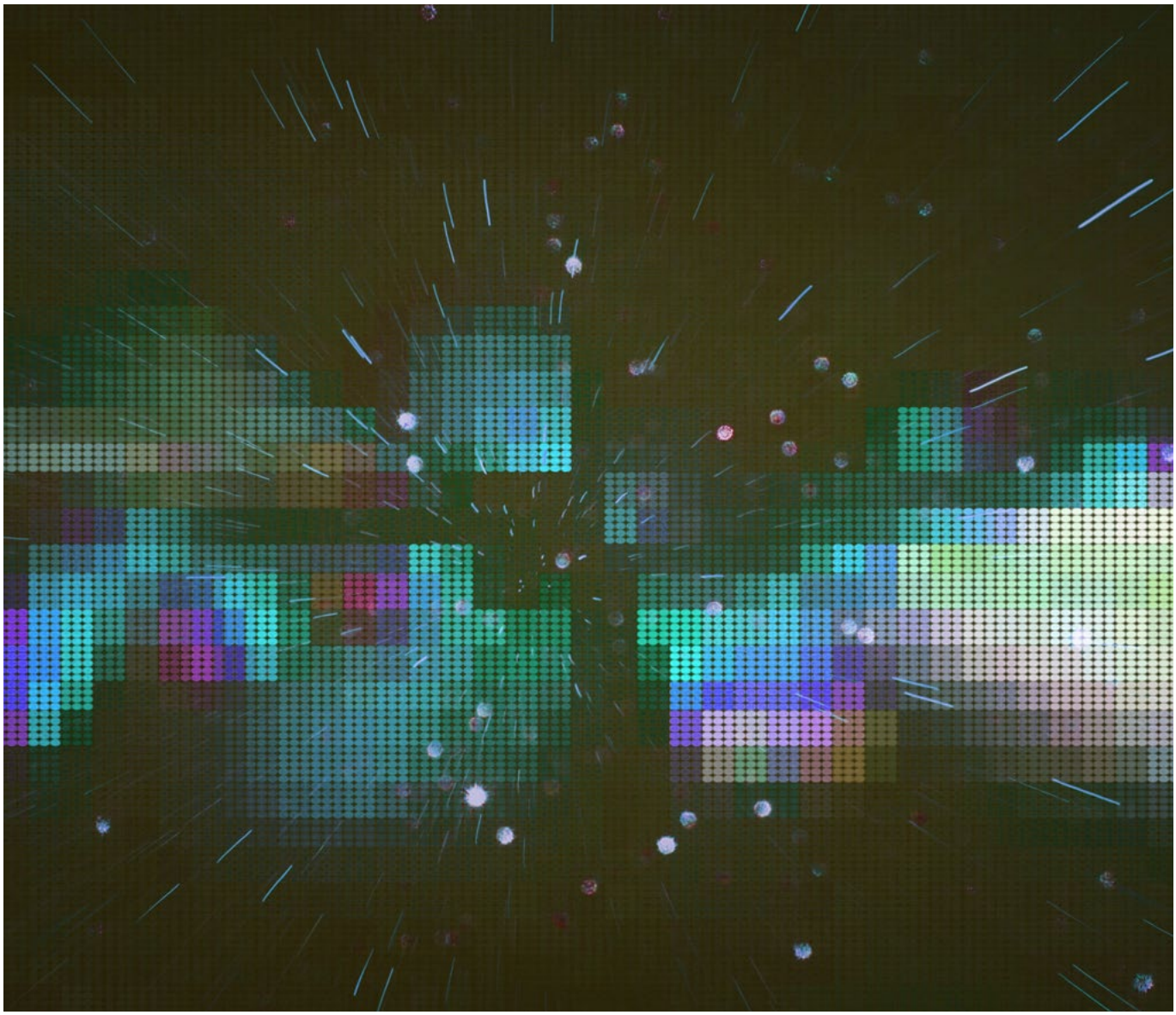
afme/
Finance for Europe

protiviti®
Global Business Consulting

State of Cloud Adoption in Europe

Preparing the path for cloud as a critical third-party solution

December 2022



/ Association for Financial Markets in Europe
www.afme.eu

Disclaimer

AFME's *State of Cloud Adoption in Europe* (the "Report") is intended for general information only and is not intended to be and should not be relied upon as being legal, financial, investment, tax, regulatory business, or other professional advice. AFME does not represent or warrant that the Report is accurate, suitable, or complete and none of AFME, or its respective employees shall have any liability arising from, or relating to, the use of this Report or its contents.

Your receipt of this document is subject to paragraphs 3, 4, 5, 9, 10, 11 and 13 of the Terms of Use which are applicable to AFME's website (available at http://www.afme.eu/en/about-us/terms-conditions) and, for the purposes of such Terms of Use, this document shall be considered a "Material" (regardless of whether you have received or accessed it via AFME's website or otherwise)..

December 2022

Contents

Executive Summary

Since the publication of AFME's initial cloud paper in November 2019[1] and subsequent paper on cloud resilience in 2021[2], cloud adoption has continued to increase, with the use of Cloud Service Providers (CSPs) and cloud technology becoming more integral to the continued growth of Financial Institutions (FIs).

However, overly complex and fragmented regulation is hampering FIs' further cloud adoption and will affect competition in the cloud marketplace. This environment could lead to less efficient and resilient solutions being adopted, resulting in downstream implications for innovation, as well as the safety and security of the financial sector.

This paper sets out recommendations in four key areas to address these challenges:

Challenge 1: Concentration of Cloud Services

1. We urge policymakers to consider how CSPs could be encouraged to provide greater transparency on resiliency, dependency and security issues within cloud services, specifically greater visibility and analysis of dependencies between regions and the underlying control plane[3] within each CSP.

2. We recommend that the adoption of multi-cloud strategies should remain at the discretion of individual FIs and should not be mandatory, as such a mandate could increase, rather than address, systemic concentration risk.

Challenge 2: Regulatory Complexity

3. We request that authorities consider an approval model for deploying services to the cloud at a platform level or remove time requirements for notifications, in order to reduce delays in the approval process.

4. We encourage greater co-ordination between the European Central Bank (ECB), European Supervisory Authorities (ESAs) and National Competent Authorities (NCAs) to ensure a consistent application of the outsourcing and Information and Communication Technologies (ICT) third-party registers to ensure minimum duplication for FIs and supervisors.

Challenge 3: Data Localisation

5. We request that policymakers and regulators refrain from requiring localisation of data or cloud hosting solutions, as it challenges resilience, inhibits innovation, and increases operational complexity.

Challenge 4: Management of Disruption in the Cloud

6. We encourage CSPs to proactively help FIs understand their tools, resources, and configuration settings and ensure that workloads and data running within the CSPs infrastructure are properly secured. In addition, CSPs should help FIs understand the Service Level Objectives (SLO) across each service provided and the resiliency and recovery metrics.

7. We request that CSPs aid FIs in proactively architecting for greater resilience by providing dependency mapping between services and geographies, for example, that two different services share a single point of failure or how an outage that occurs in one region may affect the underlying CSP control plane.

8. We encourage CSPs to provide greater transparency and detail of Root Cause Analysis (RCA) for incidents and outages within a CSP and create a library of previous RCAs, so that incident trends can be tracked, understood and better managed moving forward.

9. We ask CSPs to provide sufficient education and notice to FIs for service updates that may impact FIs' responsibilities and obligations in areas such as security or resilience.

AFME and its members look forward to discussing the findings and recommendations from this paper with regulators and industry participants and continue to support cloud adoption in capital markets.

1 The Adoption of Public Cloud Computing in Capital Markets. https://www.afme.eu/Publications/Reports/Details/The-Adoption-of-Public-Cloud-Computing-in-Capital-Markets

2 Building Resilience in the Cloud https://www.afme.eu/Publications/Reports/Details/Building-Resilience-in-the-Cloud

3 This refers to the part of a network which carries the necessary information for controlling the network

Introduction: Cloud as a Critical Enabler

Cloud services provide agile, highly available and scalable technology platforms that significantly alleviate the effort required for FIs to manage their infrastructure (e.g. data centres), while enabling greater levels of digitisation and security across technology services. This can allow FIs to deliver more innovative, unique and client-focused services.

CSPs leverage economies of scale through their extensive user bases to build new technologies and innovative products and services.[4] They invest significant amounts in research and development (R&D), advancing their core technology offerings, resulting in more specialised and advanced services than any single FI could economically develop on its own.[5] This specialisation is expected to further incentivise FIs to turn to cloud computing to support and accelerate their digital transformation efforts.

In addition to technology infrastructure, the software market is also moving rapidly to the cloud. Many software providers now distribute their products through a cloud-based model called "software as a service" (SaaS). This shift makes using the cloud increasingly necessary for any FI needing to remain digitally competitive.

As a result, many FIs are already adopting a 'cloud-first' approach, with cloud becoming a core element of how FIs design, build and deliver technology services. As noted in a recent Bank for International Settlements (BIS) paper, "*Financial institutions' cloud adoption, and hence their dependence on big techs providing these services, is likely to increase going forward.*"[6]

Adoption of cloud has also become necessary to maintain competitiveness, both for individual FIs and the European Union (EU) financial services market, a point also recognised by regulators and policymakers. For instance, the ECB states that *"... digital transformation is a must..."* and *"digitalisation is a key element in creating a future-proof business model. Banks that are not following this development or lagging behind may struggle to succeed in this competitive environment."* [7]

However, despite the growing number of workloads in the cloud and the well-understood benefits of cloud technologies, FIs continue to face challenges that slow down overall adoption.

This paper sets out four key challenges that FIs are experiencing in their cloud adoption journey, which impact their ability to fully leverage the potential of cloud technology.

1. **Concentration of cloud services;**
2. **Regulatory complexity;**
3. **Localisation; and**
4. **Management of disruption in the cloud.**

For each challenge, we set out recommendations to address the issues at an industry level.

4 BigTech in Financial Services: Regulatory Approaches (Parma Bains, Nobuyasu Sugimoto, and Christopher Wilson Jan 2022) p1. https://www.imf.org/en/Publications/fintech-notes/Issues/2022/01/22/BigTech-in-Financial-Services-498089

5 R&D Spending for Cloud Providers. https://redmonk.com/rstephens/2017/09/26/cloud_rd/

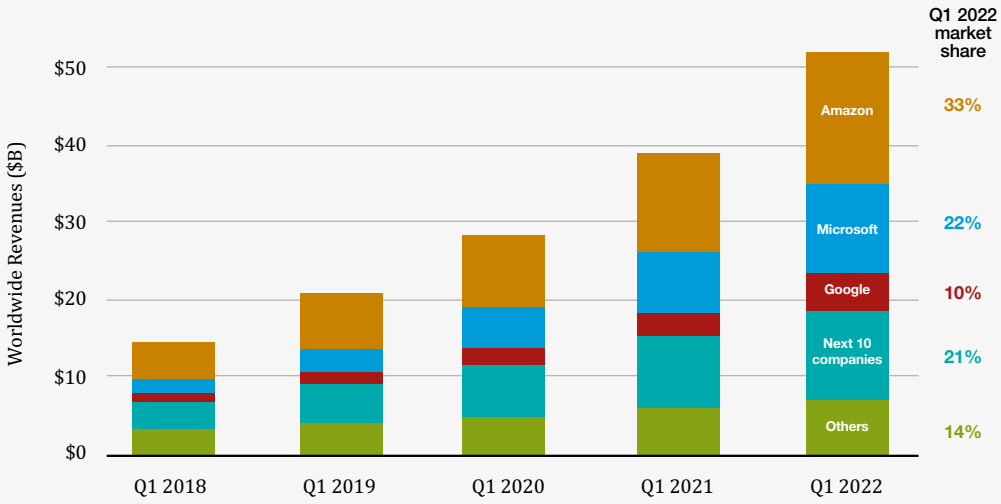
6 Cristanto, Ehrentraud, Fabian & Monteil, Big tech interdependencies – a key policy blind spot, July 2022, p17, https://www.bis.org/fsi/publ/insights44.pdf

7 The digital transformation of the European banking sector: the supervisor's perspective, Speech by Pentti Hakkarainen (Jan 2022) https://www.bankingsupervision.europa.eu/press/speeches/date/2022/html/ssm.sp220113~8101be7500.en.html

Challenge 1: Concentration of Cloud Services

Globally, almost two thirds of cloud infrastructure services (as shown in Figure 1 below) are provided by three CSPs.

Figure 1: **Cloud Services Infrastructure Market Share[8] (IaaS (Infrastructure as a Service), PaaS (Platform as a Service), Hosted Private Cloud)**



Source: Synergy Research Group

The dominance of a small number of CSPs within the global cloud marketplace is raising regulatory concerns around the risk of concentration. There are two distinct types of concentration risk:

1. Institutional – the risk associated with one firm using one CSP for a significant amount of critical services; and

2. Systemic – the risk associated with a significant proportion of a sector using the same one or small number of CSPs.

In this paper, we are considering only systemic concentration risk, as this is the type of concentration that cannot be managed by individual FIs. The key risk of systemic concentration is that, where a small number of CSPs provide a significant amount of market services, an incident at one CSP could have a wider impact on market integrity or financial stability.

Systemic concentration risk is not a new issue within financial services. It exists with other areas where there is one or only a small number of service providers, such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT), certain Financial Market Infrastructures (FMIs), stock exchanges, etc. It is also important to highlight that concentration can provide benefits, such as: critical mass and scale; highly specialised services; a reduction in complexity and therefore in operational risk for FIs; and ease of monitoring for regulators when compared to a distributed market.

In addition, we note that CSPs already contribute to the management of concentration risk via local distribution of data centres across regions in which they operate. This reduces the risk that a service disruption or failure would have market-wide implications.

The CSP market is likely to remain concentrated due to high barriers to entry including R&D costs, compliance requirements, expertise, and competitive advantages of incumbents. Therefore, the focus should be on identifying and mitigating the risks through effective controls.

8 Synergy Research :Huge Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total (April 2022); https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues

Working with CSPs to Address Systemic Concentration Risk

As noted above, systemic concentration risk requires management at an overall policy level. Given that each individual FI can only make decisions based on their individual needs and risk appetite, it is not feasible for systemic concentration risk to be addressed through information requests or reporting obligations on individual FIs.

We welcome the initiatives underway in the EU[9] and the United Kingdom (UK)[10] to manage systemic concentration risk through proposed oversight frameworks of critical/material cloud deployments. To facilitate these initiatives, we would welcome policymaker and regulator support for greater collaboration between FIs and CSPs. In particular, greater information sharing and transparency requirements for CSPs, to increase the extent to which information from CSPs is made available to FIs. This should include material/critical services such as contingency procedures (including internal failure scenarios and the scope of testing and results), dependencies between services and the cloud control plane, security testing and recovery, and restoration capabilities.

Proportionate oversight of CSPs is welcomed; one that carefully considers the impact of this oversight on cloud resiliency, adoption journeys and innovation.

The Limitations of Multi-Cloud Strategies

As discussed in AFME's 2021 paper "Building Resilience in the Cloud", some FIs may choose to adopt multi-cloud/multi-vendor strategies as part of their journey to cloud adoption. However, using multiple CSPs is typically a strategic decision to access a wide range of services across CSPs or access specific geographic regions rather than a mechanism to mitigate concentration risk.

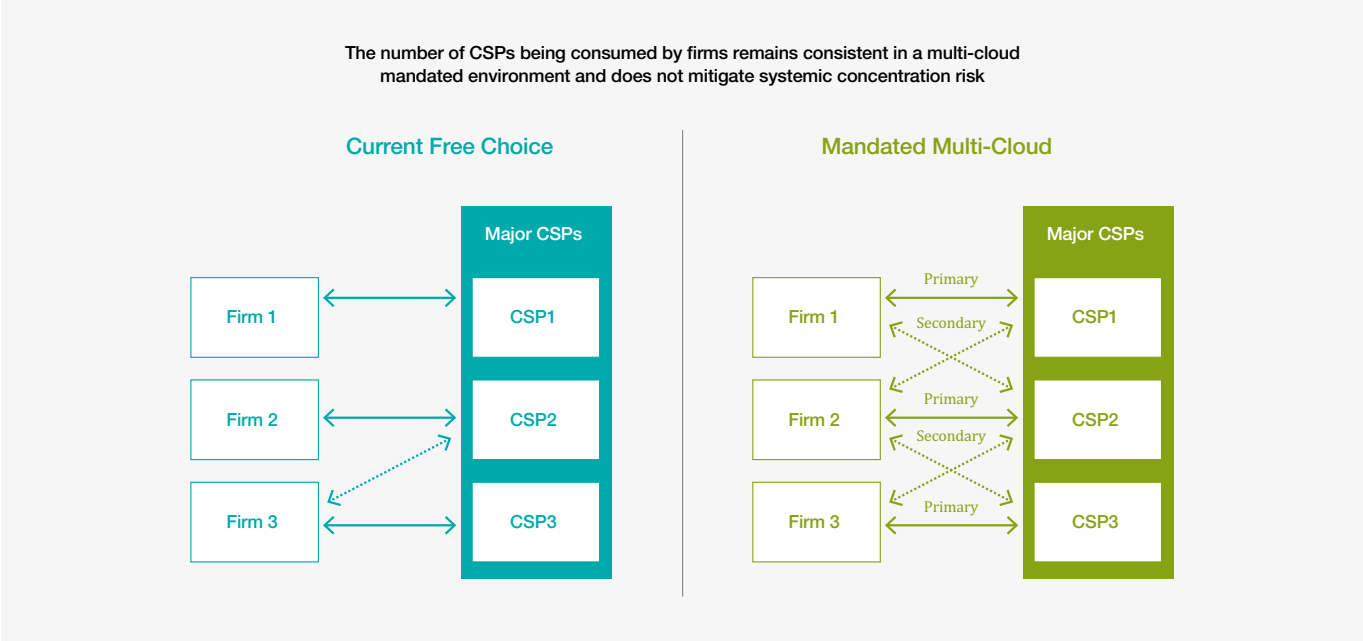
Indeed, it should not be mandated as a tool to address systemic concentration risk for two key reasons. First, this would reduce the flexibility available to FIs to implement cloud in a way that maximises the benefits to each FI and is tailored to their own needs and risk appetite. Second, unless the number of CSPs offering suitable services were to increase significantly, overall the sector would remain reliant on the same small number of CSPs.

"We welcome the initiatives underway in the EU and UK to manage systemic concentration risk through proposed oversight frameworks of critical/ material cloud deployments"

9 Regulation of the European Parliament and of the council on digital operational resilience for the financial sector and amending regulations, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

10 PRA Discussion Paper 3/22 | FCA Discussion Paper 22/3; DP3/22 – Operational resilience: Critical third parties to the UK financial sector | Bank of England

Figure 2: **Impact of Mandating Multi-Cloud Strategies**



In addition, we note that multi-cloud strategies impose greater technical complexity upon FIs and require FIs to hire and retain staff specialising in the implementation of multiple CSPs, a challenge which should not be underestimated in the current labour market.

We therefore believe that multi-cloud strategies should not be imposed as part of any package of policies to address concentration risk, but should remain at the discretion of individual FIs.

Recommendations

1. We urge policymakers to consider how Cloud Service Providers (CSPs) could be encouraged to provide greater transparency on resiliency, dependency and security issues within cloud services, specifically greater visibility and analysis of dependencies between regions and the underlying control plane within each CSP.
2. We recommend that the adoption of multi-cloud strategies remain at the discretion of individual Financial Institutions (FIs) and not be mandatory, as such a mandate could increase, rather than address, systemic concentration risk.

Challenge 2: Regulatory Complexity

In parallel to the increase in broader cloud adoption, many jurisdictions are developing and revising rules related to outsourcing, third-party risk management, security and resilience. Regulators, policymakers and FIs have a common interest in getting the regulatory framework right to enable secure and resilient digitisation. Indeed, the unique features and constantly evolving nature of cloud technology mean that historical regulatory approaches to computing may need to be adapted and regulation should be designed to be future-proof and innovation-friendly.[11]

However, regulatory complexity within the EU, as well as globally, will adversely affect the continued adoption of cloud by FIs, particularly as many pursue a group-wide technology strategy rather than per jurisdiction. A recent CSP survey[12] indicated that:

- **Regulatory fragmentation:** The pace of cloud adoption is *"cautious and controlled,"* with respondents noting that "*regulatory fragmentation, uncertainty and barriers to the use of Public Cloud*" are preventing FIs from "*putting their appetite for innovation into practice*."
- **Regulatory approvals:** The time required for regulatory reviews/approvals negatively impacts the adoption of the public cloud. 88% of the survey respondents in France, and 83% in Germany and the UK, noted that regulatory reviews and approvals took a long time because of regulatory fragmentation. 78% of respondents indicated that regulatory uncertainty over the use of public cloud is hindering their firm from innovating.
- **Resourcing:** Additionally, the research highlighted that, of the FIs that have not adopted cloud technology, the most common reason cited for this is *"the large investment of resources for the regulatory approval process."*

Table 1 below highlights various proposed policies that impact on FIs' cloud operational models. Subtle differences between each of these policies create operational complexity that reduces resilience and increases assurance requirements.

"Many jurisdictions are developing and revising rules related to outsourcing, third-party risk management, security and resilience"

11 Deloitte. Financial services on the Cloud: the regulatory approach. https://www2.deloitte.com/lu/en/pages/financial-services/articles/financial-services-on-the-cloud-the-regulatory-approach.html

12 Google Cloud The Financial Services Industry Sees Increasing Public Cloud Adoption as Driving Innovation and Compliance, p9; https://services.google.com/fh/files/blogs/report_on_cloud_adoption_in_fsi_google_cloud_08_2021.pdf

Table 1: **Recent Global Policy Developments with Implications for Cloud Services**

Published	Jurisdiction	Authority	Policy Proposal
2021	UK	Financial Conduct Authority (FCA) / Bank of England (BoE) / Prudential Regulation Authority (PRA)	Operational Resilience: Impact Tolerances for Important Business Services
	UK	PRA	Outsourcing and Third-party Risk Management
	EU	European Banking Authority (EBA)	Recommendations on Outsourcing to Cloud Service Providers
	Global	Basel Committee on Banking Supervision	Revisions to the Principles for the Sound Management of Operational Risk
	Global	Basel Committee on Banking Supervision	Principles for Operational Resilience
2022	EU	European Commission	Digital Operational Resilience Act (DORA)
	EU	European Commission	Data Act Proposal
	EU	European Commission	Directive on Measures for a High Common Level of Cybersecurity across the Union (revised NIS Directive)
	EU	European Commission	Digital Services Act (DSA)
	EU	European Commission	Digital Markets Act (DMA)
	UK	HM Treasury / BoE / PRA	Critical Third Parties to the UK Financial Sector[13]

In addition to the policy developments outlined above, global authorities, for example the Financial Stability Board (FSB), are exploring the development of global standards and the right approach for oversight of cloud providers deemed critical to the functioning of the broader financial system. The evident interest in international alignment and regulatory cooperation in this area is encouraging and strongly supported by industry.

Examples of Regulatory Challenges

For instance, some jurisdictions require FIs to seek prior regulatory approval before deploying an application or data to the cloud. In other jurisdictions, FIs are required to report to supervisors periodically, or provide a notification in certain scenarios. NCAs have struggled to scale this model to meet demand from FIs who are regulated entities, resulting in delays to FIs' digital transformation plans.

AFME would welcome innovative ways to supervise the cloud adoption process, so that EU Financial Services can remain competitive. For example, pre-approval or pre-notification requirements for cloud deployments create significant backlogs for FIs, slowing down innovation and creating business uncertainty. At the same time, such requirements are highly duplicative between deployments. Authorities should consider a platform approval model or removing time requirements for notifications.

In addition to the regulatory requirements mentioned above, regulatory and security compliance reporting is a friction point for FIs across Europe. FIs are subject to different regulations from multiple regulators that may ask for the same information in different formats and through different channels. This is most evident in the degree of variation between the various EU outsourcing registers, which could undermine the ability of competent authorities to effectively track dependence and concentration risk (e.g. Germany, Ireland).

13 We note that this discussion paper mentions two further consultations that will be issued in 2023 on related topics, as well as the BoE's initiative on Data Transformation, which will also be relevant here

We therefore encourage the ECB, ESAs and NCAs to work together to apply the outsourcing registers consistently. The standardization will minimize duplication of work by FIs and supervisors. Ideally, FIs should be able to report the requisite information once – to either the ECB or an NCA – through CASPER[14]. The authorities would then manage the information flow between themselves. The exercise recently developed by the ECB to compile the outsourcing registers of significant institutions could be the starting point for harmonizing registers at EU level.[15]

While there are efforts to mitigate the effect of localised implementations of central regulations, the EU's approach to legal entity supervision has complicated the regulatory landscape. For instance, the approach to criticality, which considers an application's importance to operations within a specific jurisdiction rather than its importance to the FI overall, increases the number of critical applications a FI has and, therefore, the compliance burden of moving those applications to the cloud.

Recommendations

3. We request that authorities consider an approval model for deploying services to the cloud at a platform level or remove time requirements for notifications, in order to reduce delays in the approval process.
4. We encourage greater co-ordination between the European Central Bank (ECB), European Supervisory Authorities (ESAs) and National Competent Authorities (NCAs) to ensure a consistent application of the outsourcing and Information and cCommunication Technologies (ICT) third-party registers to ensure minimum duplication for Financial Institutions (FIs) and supervisors.

"While there are efforts to mitigate the effect of localised implementations of central regulations, the EU's approach to legal entity supervision has complicated the regulatory landscape"

14 The ECB's Centralised Submission Platform; https://www.bankingsupervision.europa.eu/banking/portal/casper/html/index.en.html

15 https://www.ecb.europa.eu/ecb/access_to_documents/document/pa_document/shared/data/ecb.dr.par2022_0010_public_consultation_reporting_instructions.en.pdf?e46250e0da618b637b2e7ac973d11b9f

Challenge 3: Localisation

The EU Cybersecurity Act[16] creates a framework for European cybersecurity certification for products, processes and services that will be valid throughout the EU. This framework paves the way for the European Union Cybersecurity Certification Scheme on Cloud Services (EUCS),[17] a certification framework that aims to harmonise the security of cloud services with EU regulations and with existing EU Member States certifications. A common framework for EU-wide cybersecurity or security certification is a good step toward reducing fragmentation and barriers between the Member States.

However, the EUCS certification framework could have far-reaching negative implications if the proposals to achieve *"immunity against third-country law"* via EU control requirements[18] are adopted, as these will create significant impediments to security, innovation, and competitiveness of European Financial Services.

Specifically, the new EU control requirements include:

- Mandatory data localisation in the EU;
- That CSPs must have their global/group headquarters and main establishment in the EU;
- That non-EU shareholders are not permitted – directly or indirectly, individually, or jointly – to control the cloud provider; and
- That cloud services must be supported by staff located in the EU.

Some Member States have written a non-paper[19] highlighting that the new proposals to the EUCS certification framework could introduce inconsistencies and contradictions with related draft EU regulations (e.g. NIS Directive, Data Act, Artificial Intelligence Act, General Data Protection Regulation etc.) and recommending that alignment is needed.

EU regulation that limits access to global CSPs will adversely impact profitability, innovation and agility in the EU financial services sector. If the regulatory environment for digital services within the EU becomes too cumbersome, investment will reduce and the market will become less competitive, impacting consumers.

Limiting FI's access to diversely located CSPs will also result in increasingly complex IT infrastructures, with a variety of CSPs being used to provide similar services for each region separately. As previously noted by AFME, *"increased regulatory requirements towards localisation would require banks to replicate or duplicate operations and technology services in specific locations. This localisation would limit the economies of scale and benefits of global approaches and impact EU and global markets client service and resilience."* [20]

16 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

17 UC- Cloud Certification Scheme; (2020) https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

18 Non-paper by DE, ES, FR and IT on the EUCS requirements for immunity to non-EU laws (2021) p7 https://onlinetrustcoalitie.nl/wp-content/uploads/2021/11/20210716_Non-Paper-by-DE-ES-FR-IT-on-immunity-in-EUCS_vf.pdf

19 NL opinion on the Non-paper by DE, ES, FR, and IT on the EUCS requirements for immunity to non-EU laws (2021) p1. https://onlinetrustcoalitie.nl/wp-content/uploads/2021/11/NL-opinion-on-the-non-paper-immunity-to-non-EU-law-v1.0-20211007.pdf

20 AFME, "Global operating approaches ensure the development of resilient, innovative, and efficient operations and technology in capital markets p11. https://www.afme.eu/Publications/Reports/Details/Global-Operating-Approaches-in-Capital-Markets

Examples of the risks of localisation are outlined in Table 2 below.

Table 2: **Examples of Localisation Risks for Banks, Clients, and EU and Global Markets**

Focus Area	Use-Case	Impact of Localisation
Operations	Client Operations	• Reduced client service, quality, efficiency, and product opportunities (e.g. increased costs of funding or an inability to facilitate cross-border services) • Reduced resilience in the event of a service disruption (e.g. disaster recovery event) or market change (e.g. increased volatility)
Technology	Cybersecurity	• Increased competition for scarce skills in each entity location • Reduced capacity to respond to a disruption (e.g. reduced single view of risks and event monitoring) • A wider attack surface for threat actors to exploit (e.g. duplicate IT infrastructure, roles, and functions across locations)
Technology	Cloud Computing Adoption	• Duplication of controls across on-premises and cloud services (e.g. reduced resiliency benefits of cross-border deployment models for managing data and workloads) • Reduced ability to store and transmit data cross border (e.g. producing consolidated group compliance or regulatory reports to identify and remediate issues)
Technology and Operations	Operational Resilience and Risk Management	• Reduced resilience in the event of a disruption due to the concentration risk of operations or technology service localisation (e.g. a disaster recovery event)

Reducing operational complexity is important as it enables operational efficiencies that improves assurance of resiliency and security controls across technology estates.

Recommendation

5. We request that policymakers and regulators refrain from requiring localisation of data or cloud hosting solutions, as it challenges resilience, inhibits innovation, and increases operational complexity.

"EU regulation that limits access to global CSPs will adversely impact profitability, innovation and agility in the EU financial services sector"

Challenge 4: Management of Disruption in the Cloud

The occurrence of some recent high-profile cloud service outages has highlighted the need for greater visibility of, and confidence in, CSPs' abilities to predict, manage and communicate disruptions to their clients on availability of their services.

When using cloud services, FIs remain responsible for mitigating threats to their operational resilience, guarding against service disruptions and recovering quickly when incidents occur. This requires FIs and CSPs to clearly set out their respective responsibilities and expectations when entering into contracts, known as the "shared responsibility model."

The shared responsibility model is a core enabler of cloud adoption with responsibility of the cloud services residing with the CSPs and responsibility for workloads in the cloud remaining with tenants or users. However, the difficulty in establishing a clear understanding of the shared responsibility between a CSP and its user has long been acknowledged.

To help provide additional clarity, the Cyber Risk Institute in the United States of America worked with the Cloud Security Alliance to produce a cloud addendum "Cloud Profile" to the financial sector profile, a widely used cybersecurity compliance framework for the financial sector.[21] The Cloud Profile provides guidance to FIs and CSPs on commonly understood responsibilities related to Cloud deployment across different delivery models. This guidance is designed to enable FIs and CSPs to come to a contractual agreement more easily and should also facilitate more streamlined and secure processes for deploying cloud services. Moving forward, we expect to see these cross-entity collaboration efforts further reduce issues around managing disruption.

Figure 3 depicts the responsibility model which CSPs follow.

Figure 3: **A Common Shared Responsibility Model**[22]

Source: Microsoft Azure and Amazon Web Services

21 The financial sector profile is a unified approach for assessing cybersecurity risk which consolidates 2,300 + regulations into 277 diagnostic statements with 4 tiers of use. For more information see: https://cyberriskinstitute.org/the-profile/

22 Microsoft Azure, https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
Amazon Web Services, https://aws.amazon.com/compliance/shared-responsibility-model/
Google Cloud, https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

In the EU, DORA and the NIS directive set requirements for cyber/ICT risk management, incident reporting, resilience testing, and third-party outsourcing. The shared responsibility model encourages a joint undertaking between CSPs and FIs, so that these regulatory expectations can be met.

It is acknowledged that confidentiality and market integrity are important considerations in implementing any of these actions. However, we believe that greater collaboration with CSPs is key in preventing and managing disruption. With that in mind, we make the following recommendations:

Recommendations

6. We encourage CSPs to proactively help Financial Institutions (FIs) understand their tools, resources, and configuration settings and ensure that workloads and data running within the CSPs infrastructure are properly secured. In addition, CSPs should help FIs understand the Service Level Objectives (SLO) across each service provided and the resiliency and recovery metrics.
7. We request that CSPs aid FIs in proactively architecting for greater resilience by providing dependency mapping between services and geographies, for example, that two different services share a single point of failure or how an outage that occurs in one region may affect the underlying CSP control plane.
8. We encourage CSPs to provide greater transparency and detail of Root Cause Analysis (RCA) for incidents and outages within a CSP and create a library of previous RCAs, so that incident trends can be tracked, understood and better managed moving forward.
9. We ask CSPs to provide sufficient education and notice to FIs for service updates that may impact FIs' responsibilities and obligations in areas such as security or resilience.

"The difficulty in establishing a clear understanding of the shared responsibility between a CSP and its user has long been acknowledged"

Conclusion

By removing the challenges to adoption, FIs would benefit further from greater levels of digitisation and security, as well as increased use of specialised services developed by CSPs. This paper has outlined four areas that are currently creating friction to cloud adoption and innovation within FIs.

For each of these areas, we have set out key specific recommendations for policymakers, regulators and CSPs to work with the industry, with the aim of removing barriers to cloud adoption.

AFME members would welcome further discussion with policymakers, regulators and CSPs on the actions that can be taken.

"By removing the challenges to adoption, FIs would benefit further from greater levels of digitisation and security, as well as increased use of specialised services developed by CSPs"

Contributors

We are grateful to our Cloud Computing Working Group Member Firms and the individuals who contributed their time and input for producing this paper.

AFME Technology and Operation

AFME's Technology and Operations Division brings together senior technology and operations leaders to influence and respond to current pan-European market drivers and policy. Find out more at www.afme.eu/Divisions-and-committees/Technology-Operations.

About Protiviti

Protiviti is a global consulting firm that provides consulting in internal audit, risk and compliance, technology, business processes, data analytics and finance. Protiviti and its independently and locally owned Member Firms serve clients through a network of more than 85 locations in over 27 countries.

Contacts

AFME

Ian Waterworth
Director, Technology and Operations
ian.waterworth@afme.eu
+44 (0)20 3828 2685

Fiona Willis
Associate Director
fiona.willis@afme.eu
+44 (0)20 3828 2739

Protiviti

Thomas Lemon
Managing Director
Technology Consulting
thomas.lemon@protiviti.co.uk
+44 (0)20 7024 7526
+44 (0)774 748 7649

James Fox
Director
Enterprise Cloud
james.fox@protiviti.co.uk
+44 (0)782 393 8786

/ About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work.

Focus
on a wide range of market, business and prudential issues

Expertise
deep policy and technical skills

Strong relationships
with European and global policymakers

Breadth
broad global and European membership

Pan-European
organisation and perspective

Global reach
via the Global Financial Markets Association (GFMA)

afme/
Finance for Europe

London Office
39th Floor
25 Canada Square
London, E14 5LQ
United Kingdom
+44 (0)20 3828 2700

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0) 2 883 5540

Frankfurt Office
Neue Mainzer Straße 75
Bürohaus an der Alten Oper
60311 Frankfurt am Main
Germany
+49 (0) 69 710 456 660

Press enquiries
Rebecca Hansford
Head of Communications and Marketing
rebecca.hansford@afme.eu
+44 (0)20 3828 2693

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

Follow AFME on Twitter
@AFME_EU