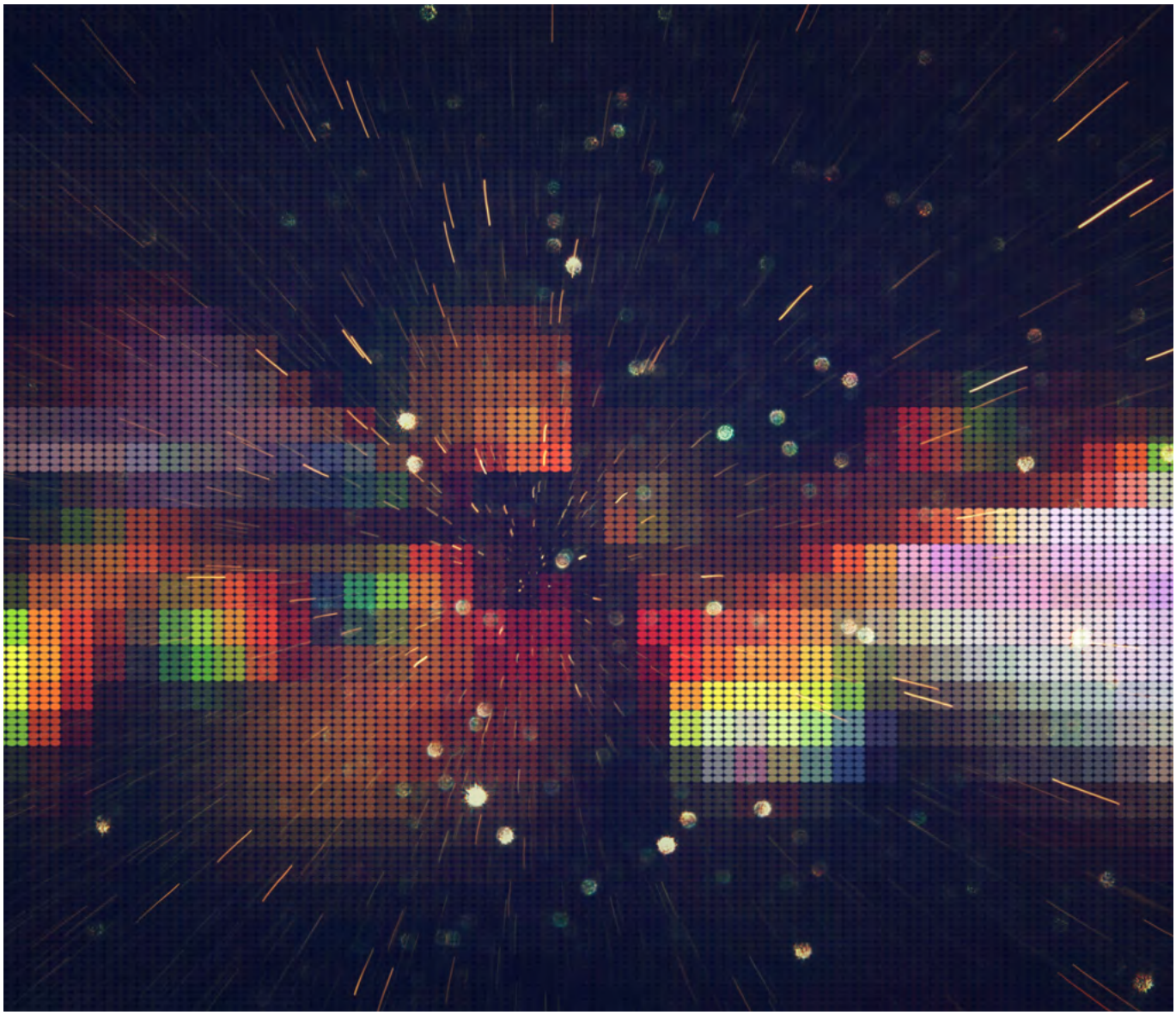
afme/
Finance for Europe

protiviti®
Face the Future with Confidence

Building Resilience in the Cloud

September 2021



Association for Financial Markets in Europe
www.afme.eu

Disclaimer

AFME's *Building Resilience in the Cloud* (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 doesn't 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).

September 2021

Contents

Executive Summary

In 2019, AFME published its first paper on the adoption of public cloud in capital markets[1]. Since then, the adoption of cloud has continued to progress, along with focus from policymakers and regulators.

Though the use of cloud and Cloud Service Providers (CSPs) offers a significant uplift in resilience and security compared to banks' on-premise environments, the regulatory focus continues to expand from concerns over the security of CSP platforms to the implications for resilience.

This focus has been part of a broader regulatory narrative covering outsourcing/third-party risk management, concentration risk, and operational resilience over the last three years. However, banks continue to use a wide range of criteria to assess their cloud resilience needs and identify solutions to mitigate these risks.

This paper, developed with members of the AFME Cloud Computing Working Group (Members) and in collaboration with Protiviti, explores two main solutions that often emerge in discussions between regulators and policymakers for cloud resilience[2]. These are the portability of data/applications/workloads amongst different CSPs and multi-cloud strategies.

While banks increase migration to the cloud and seek to identify the appropriate solutions, there are concerns that recommendations towards portability and the use of multi-cloud to achieve outcomes sought by regulators (increasing cloud resilience and mitigating concentration risk) will introduce further limitations on adoption:

- **Portability** poses significant technical limitations and a loss of differentiated cloud benefits as a mechanism for increasing resilience (e.g. limited benefit in a CSP stressed exit where a bank may have reduced or no access to its data, or limiting cloud-use to CSP foundational services only).

- **Multi-cloud strategies**, while used for contingency and resilience, are primarily adopted for accessing unique services across CSPs. While multi-cloud can reduce concentration risk to some extent, the technical, process and resource complexity needed to support multiple CSPs can lead to decreased resilience overall.

Instead, regulators should support banks adopting a risk-based approach which would provide them with flexibility based on their usage and technical needs. This should involve the choice to adopt multiple complementary solutions for resilience, rather than specific solutions being mandated for all.

We have identified four areas where additional support from policymakers and regulators and engagement from CSPs can assist banks with the resilient adoption of cloud services:

- Ensure regional and global alignment on cloud resilience and risk expectations;

- Enhance information sharing and transparency requirements for CSPs;

- Promote increased comparison amongst CSP service offerings; and

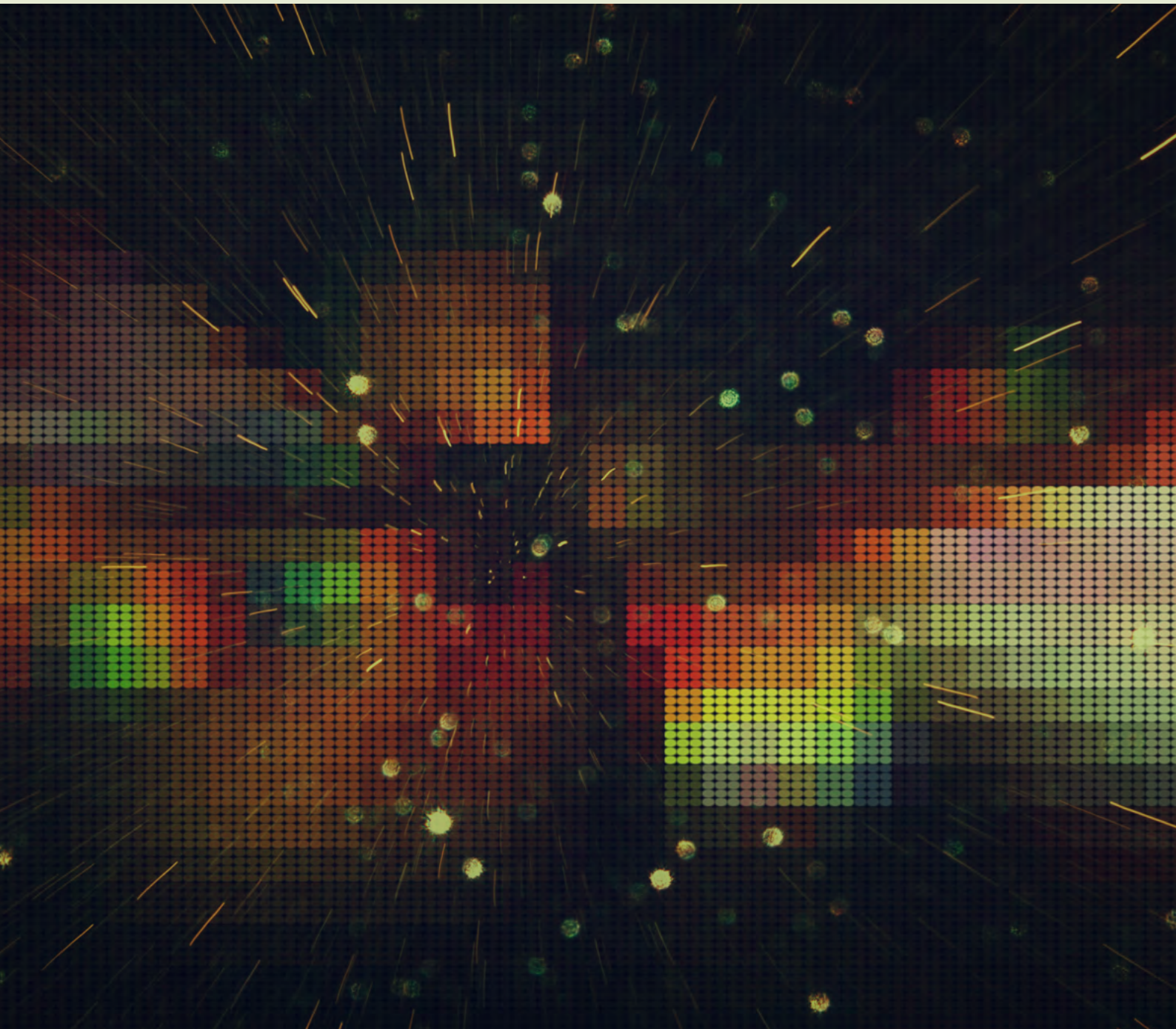
- Encourage cloud cross-border data flows and storage.

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

1 https://www.afme.eu/Publications/Reports/Details/the-adoption-of-public-cloud-computing-in-capital-markets

2 A definition of cloud resilience has been developed for this paper in Section 1 to explain its broader meaning beyond the two solutions discussed in this paper

Building Resilience in the Cloud



Introduction

This paper, developed with members of the AFME Cloud Computing Working Group (Members) and in collaboration with Protiviti, explores risk mitigation approaches to increase the resilience of cloud services. The paper focuses on two main solutions (portability and multi-cloud) that are the basis of current discussions with regulators, policymakers, and the wider industry. The paper is divided into three main sections:

1. **Drivers of cloud adoption:** Background on the current adoption of cloud in capital markets following our first paper in 2019 and the main barriers that remain. This section also outlines the increasing focus of policymakers and regulators on the resilience of cloud services.

2. **Achieving cloud resilience:** How banks assess the need for resilience in the cloud (using a scenario-based approach) and the relevance of portability and multi-cloud solutions. This section also outlines other approaches and solutions that banks consider for building resilience in the cloud.

3. **The challenges for cloud resilience:** The challenges for achieving cloud resilience through the solutions of portability and multi-cloud.

The paper concludes with four recommendations where additional support from policymakers and regulators and engagement from CSPs can assist banks with the resilient adoption of cloud services.

"Additional support from policymakers and regulators and engagement from CSPs can assist banks with the resilient adoption of cloud services"

1. Drivers of Cloud Adoption in Capital Markets

This section provides background on the current adoption of cloud in capital markets following our first paper in 2019[3] and summarises the main barriers that remain for banks. This section also outlines an increasing focus from policymakers and regulators on the resilience of cloud services as adoption continues to increase.

In line with our 2019 paper on public cloud adoption in capital markets, banks are motivated to adopt cloud services to provide greater business agility, opportunities for innovation, modernise existing IT infrastructure, and increase security and resiliency. Further, cloud adoption has increased in response to the global COVID-19 pandemic with many banks seeking to quickly enable remote working and access to core IT services via a range of cloud services. This shift has required a rapid change in how banks provision secure access to their core applications, provide collaboration and remote access capabilities for staff, and manage their data and services[4].

Through a survey of Members conducted for this paper, a hybrid cloud model[5] (the use of both private and public cloud platforms) remains the preferred approach for the majority of banks as they begin their adoption journey (63% of members surveyed), which is consistent with our 2019 findings. A hybrid cloud model is a step that enables rapid but thoughtful deployment of services into the cloud - balancing sensitive workloads while using existing on-premise environments. Some banks were also adopting 'cloud first' strategies, whereby all new projects and changes to existing technology and process were being considered in the cloud before on-premise environments.

The strategic placement of workloads into the most suitable cloud environment (public or private) continues to be determined by banks' internal assessment frameworks that consider various factors (e.g. IT strategy, compliance, investment, regulation). For example, some banks may look to Software as a Service (SaaS) for commoditised business services (such as email) and use Infrastructure as a Service (IaaS) to build and deploy differentiating services (such as business applications)[6].

Many banks are now also using a multi-cloud strategy as part of the hybrid model. The multi-cloud approach allows banks to deploy IT workloads across multiple CSPs, take advantage of each CSPs unique service offerings and strengths, and support contingency and resilience requirements. However, Members noted that a multi-cloud approach can create other challenges, such as increased costs, technical complexity, and additional specialist skillsets required to onboard and manage multiple CSPs. Members also identified clear limitations on a multi-cloud approach to mitigate concentration risk or increase resilience (discussed further in Section 3).

The survey for this paper also found that most banks continue to have less than 10% of overall production workloads in the public cloud (consistent with findings in our 2019 paper). However, overall workloads moving to the cloud (public and private) has continued to increase across most banks as anticipated, (with some banks now targeting more than 50% of workloads in the cloud long-term)[7]. Where cloud is used for material[8] workloads, Members cited use cases such as Customer Relationship Management platforms (CRM), Data Analytics, Fraud and Risk, Collaboration Tools, Infrastructure Utilities, and Enterprise Services.

3 https://www.afme.eu/Publications/Reports/Details/the-adoption-of-public-cloud-computing-in-capital-markets

4 In a 2021 Nutanix Enterprise Cloud Index Report, more than three quarters of financial services respondents said that COVID-19 had caused IT to be viewed more strategically in their organisations, with 50% of respondents saying they had increased their investment in cloud as a direct result.

5 See Annex 1 for a summary of different cloud models from our 2019 paper

6 See Annex 1 for a summary of different cloud models from our 2019 paper

7 AFME-PwC, 2020, Trends in Technology and Innovation: https://www.afme.eu/Portals/0/AFME_TechnologyInnovation_FINAL.pdf?ver=2020-11-13-135131-297

8 Material workloads for the purposes of this paper will use the PRA Rulebook definition from material outsourcing: 'services of such importance that weakness, or failure, of the services would cast serious doubt upon the firm's continuing satisfaction of the threshold conditions or compliance with the Fundamental Rules.'

Barriers to Greater Adoption

Although the adoption of cloud within the industry is expected to continue increasing, Members agreed that significant barriers identified in the 2019 paper remain, including:

- Variations in the understanding of public cloud (by banks, regulators and policymakers) and the risks and security implications for the industry;
- The high level of regulatory focus on public cloud and outsourcing, combined with regional or national variations in regulatory requirements, leading to complex compliance obligations;
- A lack of standardisation, both contractual and technical, in CSP services offered; and
- The perceived risk of regulatory action in response to resilience and concentration risk of cloud services within a limited number of CSPs.

The Increasing Regulatory Focus on Cloud Resilience

For this paper, a definition of resilience was developed with Members, which is aligned to the changes that policymakers and regulators are encouraging banks to make to their technology[9] [10]:

In line with increasing cloud adoption, recent regulatory developments have included specific recommendations or requirements on business continuity, portability of applications, data and workloads, vendor lock-in and resilience of cloud services (see Annex 3). This increasing regulatory focus on cloud is also due to a broader regulatory focus on outsourcing, third-party risk management, concentration risk, and operational resilience. Industry welcomed many of these developments as a positive effort to increase the consistency of the existing regulatory framework applicable to the cloud, enhancing the resilience of the financial system and supporting further innovation.

However, many newly proposed requirements related to cloud resilience could inadvertently inhibit adoption across the industry if they are not practical or appropriate in all instances, (e.g. if they present additional challenges to banks by mandating cloud portability or service model requirements, such as multi-cloud). For example, the 2021 EU Data Act consultation proposed legislative requirements for the portability of cloud services[11]. However, at this early stage of cloud adoption, we highlighted in our response[12] that legislating for portability could reduce competition for cloud services, create barriers for smaller providers, and limit the flexibility and service offerings available for banks (discussed further in Section 3). Further, CSP concentration (e.g. the use of a limited number of providers within financial services) extends beyond banks and the sector as a perceived risk and requires a broader policy discussion at the regional and global level.

Resilience

Resilience is the ability to resist and/or recover from failures to a known state and continue to function. It isn't about avoiding failures but accepting that failures will happen and responding to them in a way that either avoids or minimises downtime or data loss. The goal of resilience is to return applications to a fully functioning known state after a failure.

9 ECB, 2019 SSM perspective. “banks should aim to simplify their IT landscape. This is not just because simpler IT landscapes have a smaller attack surface. It is also because the easier these complex systems are to understand and maintain the better they can be protected”.)

10 AFME definition adapted from Microsoft: https://docs.microsoft.com/en-us/dotnet/architecture/cloud-native/infrastructure-resiliency-azure

11 https://ec.europa.eu/info/law/better-regulation/13045-Data-Act/public-consultation_en

12 https://www.afme.eu/Portals/0/DispatchFeaturedImages/20200626%20AFME%20EC%20CP%20Data%20Act%20(FINAL).pdf

Cloud as an Enabler for Resilience

Members identified the benefits of adopting cloud services to enhance resilience over traditional on-premise environments. These included:

- CSPs investment in facilities and security to maintain modern data centres with physical security features;
- The resilience and security of CSP platforms, such as regular patching of the underlying infrastructure, renewal of underlying hardware and auto-scaling automated recovery;
- Access to functionality, such as built-in security, logging and monitoring capabilities, secure backup and restore, compliance and auditing services, that can be activated through quick integration and provide transparency and reporting across cloud platforms;
- A global spread of CSPs infrastructure facilities that provide geographic redundancy to customers;
- The ability to quickly establish high-availability environments (e.g. by using Availability Zones[13]) on-demand to minimise disruption.

These benefits provide banks with improved capabilities in the cloud to support resilience by:

- Allowing banks to be both reactive and pro-active in detecting and responding to failures;
- Returning to a known state when recovering to allow users to continue accessing and using applications, data, and services; and
- Designing for a range of scenarios to detect and respond quickly to disruption and avoid downtime or data loss (recognising that issues and failures will occur).

"Cloud services enhance resilience over traditional on-premise environments"

13 An explanation, illustration and the benefits of Availability Zones is provided in Annex 2

2. Achieving Cloud Resilience

This section outlines how banks and regulators should use failure scenarios to plan for resilience in the cloud. Five example failure scenarios are outlined in Table 1 below and considered against the solutions of portability and multi-cloud (which are discussed further in Section 4). This section also outlines a broader range of other initiatives and approaches that banks use to build resilience into their cloud services.

The section finds that regulators, like banks, can use failure scenarios, such as the examples provided in Table 1, to provide greater transparency into their cloud resilience concerns. A scenario-based approach can drive objectives-based solutions rather than prescriptive requirements (such as portability and multi-cloud). This approach would also allow regulators to quantify and manage a macro view of which cloud workloads across banks could be impacted by each failure scenario (e.g. concentration risk) and how banks plan to address these risks.

Criteria and Scenarios to Assess Cloud Resilience

At a high level, Members identified that building resilience in the cloud covers a wide range of criteria:

- The overall risk profile and appetite of the bank;
- The materiality of workloads being migrated or developed on cloud services;
- The type of workload being migrated (production or non-production);
- The amount and type of data being migrated; and
- The need for remote access to the application or data.

Considering the example criteria above, banks seek to build resilient cloud services with a risk or scenario-based approach that is in line with regulatory guidelines, e.g. banks identify various scenarios in assessing the need for resilience across cloud environments to determine how they are positioned to respond to potential disruption. Members noted that the use of hybrid and multi-cloud models allows for a diversification of services in any one CSP, in some cases, and a reduction in the risk profile in the event of a major failure.

In developing this paper, Members identified five example failure scenarios to illustrate the need for building resilience into their cloud platforms based on the likelihood of occurrence. Table 1 below outlines each scenario in order of decreasing likelihood, the approaches banks are taking to mitigate the risk and the relevance of multi-cloud and portability solutions. The decision to employ any given approach to resilience is informed by the levels of actual risk determined by the bank in its scenario assessment e.g. a bank may choose not to build multiple CSP instances across Availability Zones for an application that is deemed non-material and has a high downtime tolerance.

Table 1: **Scenarios Requiring Resilience in the Cloud**

Scenario 1 – Technical Component or Single Availability Zone Failure		
In the event of failure or one or more services, or technical components, across a single CSP Availability Zone		
Bank Approach to Resilience	**Multi-Cloud and Portability Use**	**Likelihood**
• As a best practice, most CSPs deploy services of their clients in multiple Availability Zones (unless precluded by data localisation laws) in the event of this failure within any of the CSPs used. Cloud services would be failed over to the next Availability Zone as part of the resilient architecture design with minimum to no impact to end-users depdendent on resiliency patterns (failover vs continuous availability) • Should a failure occur, the bank would establish a root cause analysis and a performance improvement plan with the CSP, with lessons learned for the future	• Built-in failover capability in the CSP platforms would obviate the need to use multi-cloud and or portability to maintain service continuity	Medium (*plausible*)
Scenario 2 –Multi-Regional Availability Zone Failure		
In the event of a cloud services or technical failure across multiple Availability Zones (one or more regions).		
Bank Approach to Resilience	**Multi-Cloud and Portability Use**	**Likelihood**
• Building on scenario 1, by using CSP regional Availability Zones, banks create service resilience across geographies • An advantage to using CSPs is the ability to manage workloads and data cross-border to provide resiliency to a disruption (e.g. a power grid failure or natural catastrophe). • Should a failure occur, the bank would establish a root cause analysis and a performance improvement plan with the CSP, with lessons learned for the future	• Availability and regional redundancy would obviate the need for multi-cloud and or portability to maintain service continuity	Medium to Low (*plausible*)
Scenario 3 – Breakdown in CSP Commercial Relationship or Regulatory Intervention		
In the event of a breakdown in a commercial or legal relationship with a CSP or regulatory intervention on the use of a specific cloud service (non-stressed exit).		
Bank Approach to Resilience	**Multi-Cloud and Portability Use**	**Likelihood**
• This non-stressed scenario would typically allow time for a bank to migrate services and/or meet regulatory requirements (e.g. plan, design, and implement a move of cloud services to an alternative CSP) • Contractual considerations would be required to recover long-term commitment (i.e. pre-paid services) where possible, but the continuity of services could be maintained through Disaster Recovery (DR) and Business Continuity (BCP) plans as well as through a contractual agreement with the CSP	• Operating in a multi-cloud model with an established platform and contracts in place would allow for quicker migration to an alternate provider (where comparable services exist); however, Members noted that doing so would increase cost and complexity and potentially negate cloud benefits • A non-stressed exit would allow time for porting of cloud services from one CSP to another or identify a substitutable solution	Low (*implausible*)

Scenario 4 –Sudden CSP Commercial Failure		
In the event of an immediate commercial or underlying failure of a CSP (a stressed exit).		
Bank Approach to Resilience	**Multi-Cloud and Portability Use**	**Likelihood**
• Banks would enact their exit management and contingency plans to an alternative CSP (where comparable services exist) or on-premise platforms. There may be short term business impact and service level degradation as services, applications and data are migrated to an alternate provider or restored from backups • The use of open standards and open-source solutions would enable quicker migration and recovery of impacted services in the failed CSP	• The use of multi-cloud may allow for quicker technical recovery into an alternate "warm" platform. However, significant time and effort would be required to establish technical continuity in a new CSP • The use of multi-cloud also increases costs and complexity and potentially negate cloud benefits • Lack of access to the failed CSP would inhibit a banks ability to port cloud services to a new CSP or on-premise solutions	Very Low (*implausible*)
Scenario 5 - Catastrophic CSP Technical Failure		
In the event of a technical failure of a CSP causing the complete failure of services (a stressed exit).		
Bank Approach to Resilience	**Multi-Cloud and Portability Use**	**Likelihood**
• A catastrophic technical failure that cannot be recovered within a suitable timeframe would trigger a stressed exit from the CSP, with DR and BCP plans enacted as in scenario four above (with a focus on service recovery)	• The use of multi-cloud (where comparable services exist) may allow for quicker technical recovery into an alternate "warm" platform. However, significant time and effort would be required to establish technical continuity in a new CSP • The use of multi-cloud also increases costs and complexity and potentially negate cloud benefits • Lack of access to the failed CSP would inhibit a banks ability to port data/applications/ workloads to new CSP or on-premise solutions	Very Low (*implausible*)

Approaches for Building Resilience in the Cloud

Members identified a wide range of other elements to building resilience in the cloud, beyond portability and multi-cloud strategies discussed in the scenarios above. Table 2 below, whilst not exhaustive, outlines these elements across governance, architecture, operations, and security. At a high level, each element will have different responsibilities or implications for banks, CSPs, and the types of cloud services used (SaaS, PaaS and IaaS[14]).

"Members identified a wide range of other elements to building resilience in the cloud, beyond portability and multi-cloud strategies"

14 See Annex 1 for a summary of cloud service types from our 2019 paper

Table 2: **Building Resilience in the Cloud**

Governance	
Defined Roles and Responsibilities in Support of the Shared Responsibility Model	• Defining an overarching governance model for the cloud with roles and responsibilities assigned and communicated • Defining roles and responsibilities within the IT Department to manage risk with a clear understanding of responsibility in the cloud (i.e. by the firm) vs of the cloud (i.e. by the CSP) • Defining the roles and responsibilities across the broader bank to support effective and efficient governance of the cloud platforms (e.g. internal audit, risk and compliance functions)
Documented Operational Planning	• Defining an operating model for the cloud and considering centralised and decentralised functions across banks (e.g. the requirements for cloud services within a specific location or region)
Documented and Regularly Tested Recovery Approaches and Instructions	• Defining and documenting recovery approaches in the event of failure, with regular tests to ensure success and continued relevance
Architecture	
Designing for Resiliency Using Best Practice	• Redundant Availability Zones - Designing for the use of multiple Availability Zones (where necessary) to provide enhanced availability for workloads • Redundant Regions – Considering the use of multiple Regions to allow for enhanced redundancy and geographic localisation and restoration capability to rebuild services/data • Redundant CSPs - Considering the use of architectures that balance applications and data between on-premise and cloud services
Identifying Metrics to Measure	• Identifying resilience, security, performance, and business metrics to measure cloud services that will evolve based on demand and consumption within the bank
Defining Availability, Backup and Retention Approaches	• Defining availability and retention (e.g. backup) strategies to allow for the retrieval of data in a timely and efficient manner and to a known state in the event of outages or failures
Operations	
Use of Operational Best Practices	• Monitoring and Alerting – Establishing alerting throughout the cloud platform to provide awareness of issues and remediation • Auto-Recovery/Healing –Establishing auto-recovery/healing to automate restoration rapidly, where possible, in the event of a failure • Auto-scaling –Enabling auto-scaling to allow for planned or un-planned peaks in demand and maintaining the availability of applications, where possible • Data attributes – The classification, labelling, codification of rules for the use and transfer of data • Assurance – Continuous assurance of controls and audit for the access to data
Use Immutable Infrastructure	• Use of standard configurations (that do not change once deployed) to allow for rapid recovery to known points, with reduced risk of missed changes when recovering in pressurised situations
Golden Images to Provide Known States for Recovery	• Use of endorsed baseline images with security patches installed to provide a trusted known state to recover servers in the cloud quickly
Data Compliance	• Adoption of data classification, labelling, and codification of rules to control the movement of data amongst cloud platforms
Security	
Manage Identity and Access Privileges and use Least Privilege Approaches	• Ensuring a strategic and pro-active approach to managing all identities across cloud platforms, using least privilege access permissions to reduce the risk of unapproved access.
Enforce Network Isolation and Use Endpoints to Keep Traffic Private	• Isolation from other cloud service customers to keep data secure and protected, whilst endpoints minimise inbound and outbound intrusion in the bank network
Deploy Proactive Patching to Minimise risks of Infiltration	• Using golden images and immutable infrastructure to regularly deploy patches across the cloud environment to minimise the risks of infiltration or malware

3. The Challenges for Cloud Resilience

This section discusses the challenges for achieving cloud resilience through the two common solutions being discussed in the industry and cited by policymakers and regulators: portability and multi-cloud strategies. While these solutions have benefits for achieving cloud resilience, there are also important limitations to what is possible to mitigate risk. Both solutions should not be viewed as appropriate or mandated as primary mechanisms to address regulatory concerns regarding cloud resilience and risk.

Adopting a Multi-Cloud Strategy

"While portability and multi-cloud strategies have benefits for achieving cloud resilience, there are also important limitations to what is possible to mitigate risk"

At a high level, a multi-cloud strategy uses multiple CSPs and/or on-premise environments, which can help to reduce concentration risk and increase the resilience of cloud services in specific extreme scenarios (see Section 2). However, discussions with Members identified that using multiple CSPs is typically a strategic decision to access a wide range of services across CSPs or access specific geographic regions rather than being seen as a mechanism to mitigate concentration risk and increase resilience. In our survey for this paper, 40% of Members stated that they are currently using a model of multiple CSPs for workloads rather than balancing workloads across multiple CSPs. Demanding cross-CSP resiliency was not deemed feasible in the current environment. This is because interoperability between CSPs is minimal, if existent at all, and it would limit either cloud usage overall or limit cloud usage to commonly available services (effectively stifling innovation and reducing the ability to derive business value from using CSPs).

Instead, Members identified a range of challenges regarding multi-cloud strategies for increasing resilience, which include:

- **Multi-cloud could reduce concentration risk for an individual bank but may not address portability:** Banks acknowledge that the use of multi-cloud solutions may reduce levels of concentration risk through a strategic selection of CSPs for particular workloads (e.g. one CSP for core applications and another CSP for data analytics). However, at an aggregate industry level, concentration of cloud services could remain high if a particular service is being used by multiple banks for speciality or geographic reasons (e.g. data localisation requirements). Further, the technical and cost challenges involved for a bank mean that implementing portable workloads amongst multiple CSPs remains complex or not practical in many cases (e.g. not all data should be seen as portable or interoperable without a trade-off in efficiency and capability of the overall cloud service).

- **Establishing multi-cloud requires significant investment:** Adding new cloud platforms requires additional financial investment for their design, build and operation. Additional complexities include the connectivity and integration required with existing IT service management platforms and workflows and processes, often underestimated in initial business cases for multi-cloud approaches. Further, additional cybersecurity risk may need to be mitigated by virtue of multi-cloud increasing the attack surface of technology in use.

- **The people aspects of multi-cloud are often neglected:** If banks are encouraged to adopt multi-cloud at pace, they would need to establish new, skilled teams to support a new cloud platform, requiring investment and time to recruit and upskill existing teams. Often, resources from existing cloud teams within the bank are transitioned to support establishing a new platform, which strains resources overall. This can create risks for resilience or change activities, as any issues in the original cloud platform could take longer to resolve due to initial resourcing constraints.

Portability of Workloads

For the purpose of this paper, portability is defined as:

- *The ability to quickly and seamlessly move applications and data from one computing environment to another whilst allowing for equivalency of functions*[15].

Discussions with Members acknowledge the potential benefits of portability for increasing cloud resilience, e.g. using tooling such as containers[16] to move workloads across different cloud platforms (for both public cloud and on-premise). However, the concept of portability has significant technical limitations when seeking to utilise it as a primary mechanism for increasing resilience (particularly in a stressed exit from a CSP). This is of particular concern regarding a perceived regulatory trend towards encouraging, or even potentially mandating, portability of cloud workloads between CSPs and on-premise facilities and/or between CSPs[17].

Members identified a range of challenges regarding portability for increasing resilience, which include:

- **Technical complexity introduced into cloud environments:** Portability between multiple CSPs introduces significant technical complexity from the additional services and integration required, the increased need for new architectural patterns between CSPs and banks (for areas such as service management, onboarding, processes development and reporting), and the need for banks to monitor and test CSPs service-parity. With increased technical complexity, the ability of banks to recover from failures quickly and seamlessly can be inhibited due to the number of systems, services, and technical components involved.

- **Variation based on cloud service type (SaaS, PaaS, IaaS)**[18]**:** Portability requirements and their feasibility differ by cloud service type. For example, portability may be considered relatively less challenging for an IaaS service in comparison to PaaS and SaaS, depending on the product used. However, challenges will remain for managing and controlling the underlying infrastructure between a bank and a CSP (e.g. availability in an extreme scenario, such as a catastrophic CSP failure discussed in Section 2). Portability for SaaS will depend on the alternative providers and services available, as the user does not manage the underlying infrastructure (e.g. networks, storage) and typically has limited application management capabilities (e.g. beyond user-specific application configuration). Portability for PaaS services is more challenging based on the service offering and configuration. Banks must identify the dependencies for the infrastructure (e.g. compute, storage, database, network, security) and the platforms usage (e.g. other applications that may be hosted on the platform). Further, the ability to port to an alternative CSP will be based on the programming languages, libraries, services, and tools required to support the platform.

- **Loss of differentiated service benefits:** Banks that seek to achieve portability amongst CSPs would be restricted to cloud services where there are comparable services amongst CSPs. Comparable services tend to be more foundational (i.e. compute and storage services), excluding many differentiated services that banks seek to take advantage of when looking to adopt cloud services. (e.g. AI, machine learning, text services, data analytics).

- **Lack of comparable services to achieve portability:** There are few directly comparable cloud services for banks to achieve worthwhile levels of portability, particularly with SaaS. In many cases, banks have engaged a particular SaaS provider due to its competitive or unique offering. Any attempt to enforce portability would lead to a loss of access to differentiated or innovative services in the market. In addition, geographic discrepancies exist between CSPs that may prevent comparable services in particular locations.

15 AFME definition adapted from NIST Cloud Computing Standard Roadmap (NIST Cloud Computing Standards Roadmap SP 500-291)

16 Containers are technical tools which can orchestrate and manage cloud resources such as networking, load-balancing, security, and scaling.

17 The EU 2021 public consultation for a Data Act includes legislative options for mandating cloud data portability into EU law: https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-data-act

18 See Annex 1 for a summary of cloud service types from our 2019 paper

- **Portability would not address stressed exits from CSPs:** Banks consider portability and document exit strategies when contracting with a CSP (e.g. data availability across multiple CSPs in the event of a failure). However, in the event of a stressed exit from a CSP due to significant technical or commercial failure, there could be limited or zero access to data, applications, or services (i.e. the ease and timeline in which data could be extracted). This restricted access could prevent the ability for firms to port data, applications, or workloads to a secondary CSP or on-premise platform, offering no additional resilience to firms in this event.

- **Capacity constraints:** In the event of a CSP failure, there could be the need for the bank to fail over to a second CSP. However, it would be unlikely that the second CSP would have capacity available, as this would only be possible if capacity was already reserved. This would require banks to double operational costs to account for the very rare scenario of a CSP failure.

- **Significant investment required:** Introducing a new CSP requires significant investment (e.g. cost and resourcing) for a bank to complete integration with an existing CSP and perform onboarding into existing service management processes and workflows. New CSP specific skillsets will be required on an ongoing basis in addition to existing resources, leading to increased technical and non-technical costs. This increased investment can radically alter the initial business case for cloud, leading to slower modernisation of a banks' IT infrastructure, resulting in degraded services to clients and lower security and resilience.

"Increased investment can radically alter the initial business case for cloud, leading to slower modernisation of a banks IT infrastructure"

4. Recommendations to Support the Continued Adoption of Resilient Cloud Services

This paper has highlighted how banks proactively assess, design, and implement resilient approaches to their cloud platforms. Discussions with Members emphasised the significant focus within banks to achieve greater cloud service resilience and the increasing focus from policymakers and regulators on this topic.

However, this paper has identified practical concerns and challenges regarding the viability of portability and multi-cloud strategies as primary mechanisms for increasing resilience. Any future regulatory requirements that could mandate banks use of portability and multi-cloud strategies would not be feasible given the technical limits this could impose on the use of cloud. In addition, it could further contribute to the existing burden on banks (and regulators) regarding cloud pre-approval requirements (as opposed to banks maintaining an inventory of cloud arrangements that can be made available to regulators).

Further, any specific limitations on the use of CSPs to address concentration risk could risk impacting the ability of banks to increase their resilience overall (e.g. being able to balance workloads over CSP and on-premise environments). Ultimately, this could either limit cloud usage or limit cloud usage to commonly available services, impacting innovation and reducing the ability to derive value from cloud.

Ongoing collaboration with policymakers, regulators and CSPs is needed to prevent requirements or solutions towards cloud resilience from being mandated, introducing further barriers to cloud adoption in capital markets. This collaboration should also actively promote cross-border data flows to prevent further limits on cloud being imposed at a regional level[19]. The ability for banks to continue taking a risk or scenario-based approach, using a wide range of approaches and solutions outlined in this paper (including multi-cloud and portability), will be necessary for building resilience and realising the benefits of cloud computing for financial services.

We have identified four recommendations where additional support from policymakers and regulators and engagement from CSPs can assist banks with the resilient adoption of cloud services. These are:

- **Ensure regional and global alignment on cloud resilience and risk expectations.** To provide banks with a common baseline to align on a cross-border basis, such as the scenarios and metrics (e.g. capacity, performance, availability), which will reduce the burden for evidencing and proving cloud resilience and allow regulators to quantify any macro-concentration risk across the industry.

- **Enhance information sharing and transparency requirements for CSPs.** To increase the ease to which CSP required information, such as contingency procedures (including internal failure scenarios, and the scope of testing and results), and security testing and recovery and restoration capabilities, are made available to banks for regulatory authorities.

- **Promote increased comparison amongst CSP service offerings.** To support banks in developing portability and exit planning approaches by having available a clear mapping of products, services, and capabilities across providers in a common format and promoting the use of standards (such as security testing and reporting), and opensource technologies.

- **Encourage cloud cross-border data flows and storage.** To prevent further technology and data-related regulatory requirements being introduced that could segment banks adoption of cloud services regionally, as opposed to adopting globally, increasing geographic concentration and cyber and resilience risks.

We believe that these recommendations provide practical guidance for building further confidence, trust, transparency, and capability in cloud services within capital markets as adoption increases. AFME and its Members will continue to proactively engage with regulators, CSPs, and the broader industry in achieving this aim and realising the benefits of cloud services for innovation and resilience in EU and global financial services.

19 For example, European Data Protection Supervisor (EDPS) ongoing determination of data transfer contracts under the 2020 Schrems II ruling and the potential impact on non-EU cloud service provider use.

Annex 1: Cloud Services and Models

AFME's 2019 paper[20] discussed cloud computing as a technology and the different types of services and models. Table 3 and Figure 1 below illustrate some of the key terms used in this paper.

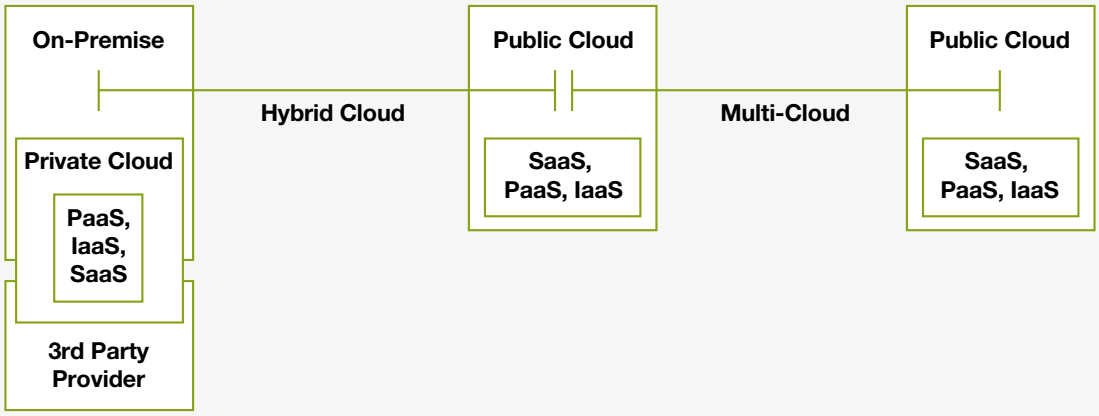
Table 3: **Types of Cloud Computing Service**[21]

Cloud services	Description of services	Example
IaaS (Infrastructure-as-a- Service)	Consumers can provision fundamental computing resources where they are able to deploy and run arbitrary software. 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.	Grid or High- Performance Computing (HPC)
CaaS (Container-as-a-Service)	Consumers can use containers to upload, organise, scale, manage applications and clusters. Containers enable these processes by using a container-based virtualization, an application programming interface (API) or a web portal. The consumer does not manage or control the underlying cloud infrastructure including network, servers and operating systems, but has control over storage, the deployed applications and possibly configuration settings for the application-hosting. environment.	Build and deploy multi-tenant testing environments for application development
PaaS (Platform-as-a- Service)	Consumers can deploy onto the cloud infrastructure consumer-created or acquired applications 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.	Managed Database Platform
SaaS (Software-as-a- Service)	Consumers can use the cloud provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.	Customer Relationship Management (CRM) application or Collaboration Services e.g. MS Teams or Zoom
FaaS (Function-as-a-Service)	Consumers can use the cloud provider's infrastructure to execute applications. The consumer can execute applications without the need to build and manage the underlying infrastructure. This enables rapid deployment of applications and lower infrastructure costs. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage and applications.	Running a machine learning algorithm for a trading applications

20 https://www.afme.eu/Publications/Reports/Details/the-adoption-of-public-cloud-computing-in-capital-markets

21 National Institute of Standards and Technology (NIST)

Figure 1: **Models of cloud computing**



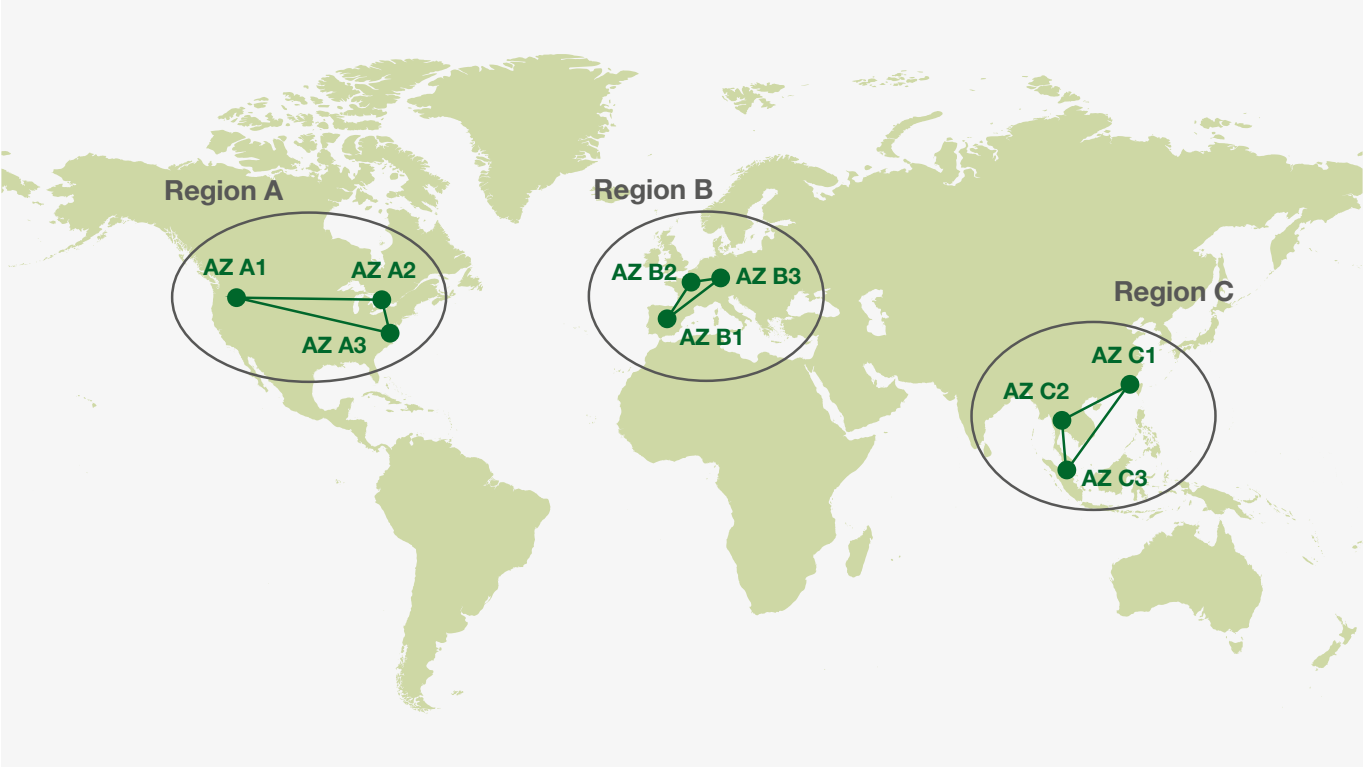
Annex 2: Availability Zones

At a high level, Availability Zones (AZs) are the physical locations of CSPs datacentres within a specific location (typically called a Region). For example, a CSP may have a European region with three AZs in Spain, France, and Germany. See Figure 2 below for a high-level illustration.

The customers of a CSP can benefit from greater resilience by managing applications or data across multiple AZs within one or across global regions. This global infrastructure approach can reduce the geographic concentration risk of services for customers and provide resiliency benefits outlined in this paper (e.g., data availability in the event of a failure). This use of CSPs is an advantage over more traditional organisational approaches to having a primary and disaster recovery datacentre pairing typically in a single region.

"A global infrastructure approach can reduce the geographic concentration risk of services for customers and provide resiliency benefits"

Figure 2: **High-level overview of a CSP region and AZ architecture**



Source: AFME/Protiviti

Annex 3: Key Developments in Cloud Regulation post 2019

Table 4 below provides an overview of regulatory developments and their impact on cloud adoption since the publication of the AFME 2019 paper.

A complex regulatory landscape was cited as a critical barrier to cloud adoption in AFME's 2019 paper. Even before implementing public cloud services, increased varying and often duplicative guidelines has made the regulatory landscape more complex for banks, with significant upfront regulatory engagement required. In the last five years, European and global authorities have published a significant number of new guidelines that banks must assess and implement. Further, in 2020 the European Commission published a legislative proposal for a digital operational resilience act (DORA) which has introduced further uncertainty on the alignment to existing guidelines on cloud.

Table 4: **Key Developments in Cloud Regulation post-2019 (Global, EU, UK)**

Region	Authority	Regulatory development and barriers for cloud adoption
International Standards Setting Bodies	FSB	November 2020 discussion paper on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships[22] • Using cloud, as part of outsourcing or third-party service, could be an automatic indication of risk and lead to overly prescriptive regulatory requirements • Data localisation measures that could impact cross-border use and scale of cloud
	IOSCO	May 2020 updated Principles on Outsourcing[23] • Data access and localisation measures that would restrict cross-border use of cloud • Requires banks to monitor and manage global concentration risk of third-party providers (such as CSPs)
EU	ESMA[24]	December 2020 Guidelines on Outsourcing to CSPs[25] • More granular requirements and contractual arrangements between banks and CSPs which can be challenging for parties to negotiate • Requirements for banks to monitor and manage global concentration risk of third-party providers (such as CSPs) • Plans for the collection and storage of outsourcing information which could lead to duplicate and conflicting reporting requirements for banks
	European Commission	September 2020 proposal for a Digital Operational Resilience Act (DORA)[26] • Prescriptive requirements for banks cloud strategies, models and risk assessments • Direct supervisory oversight of CSPs that could require banks to terminate or suspend cloud services • Requirements on resilience and business continuity for contracts between banks and CSPs
		June 2021 Proposal for an EU Data Act • Proposing to legislate for cloud portability which could introduce further technical, commercial, and contractual complexity for banks adoption of of cloud services
UK	PRA	March 2021 Supervisory Statement on Outsourcing and Third Party Risk Management'[27][28] • Shared Responsibility Model requirements which introduces broad expectations on banks to define, document and understand their respective responsibilities with a CSP • Requirements on banks to consider cloud resiliency and business continuity options which adds further complexity to banks ongoing assessment of UK operational resilience requirements • Requirements to plan and test stressed exits of cloud services for risk mitigation which can be burdensome for low-risk cloud deployments or scenarios

22 https://www.fsb.org/2020/11/fsb-consults-on-regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships/

23 https://www.iosco.org/news/pdf/IOSCONEWS567.pdf

24 We note that the ESMA Guidelines followed an EBA release in 2019 and an EIOPA release in 2020, meaning that in some cases firms are working to compliance with Guidelines from all 3 of the ESAs

25 https://www.esma.europa.eu/press-news/esma-news/esma-publishes-cloud-outsourcing-guidelines

26 IMMC.COM%282020%29595%20final.ENG.xhtml.1_EN_ACT_part1_v8.docx (europa.eu)

27 https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss

28 The PRA 2021 Supervisory Statement on Outsourcing and Third Party Risk Management' recognised the resilience benefits for firms using cloud to distribute their data and applications across multiple zones, provided that the risks are also considered.

Contributors

We are grateful to the AFME Member firms and the individuals who contributed their time and thoughts in producing this report. We also wish to thank our Premium Associate Members.

AFME Technology and Operations

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. The AFME Cloud Working Group developed this paper as an initiative within the broader Technology and Operations Division.

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

Andrew Harvey
aharvey@afme.eu
Managing Director
Technology and Operations
+44 (0)20 3828 2694
+44 (0)774 748 7649

Tola Gbadebo
tola.gbadebo@afme.eu
Interim Associate Director
Technology and Operations
+44 (0)20 3828 2739

Protiviti

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

James Fox
james.fox@protiviti.co.uk
Director
Enterprise Cloud
+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)2 788 3971

Frankfurt Office
Neue Mainzer Straße 75
Bürohaus an der Alten Oper
60311 Frankfurt am Main
Germany
+49 69 153 258 963

Press enquiries
Rebecca Hansford
Head of Media Relations
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