Supervisory Risk Division
Central Bank of Ireland
Via e-mail: outsourcingfeedback@centralbank.ie

26 July 2021

AMAZON WEB SERVICES (AWS) RESPONSE TO THE CENTRAL BANK OF IRELAND'S CONSULTATION PAPER 138 – CROSS INDUSTRY GUIDANCE ON OUTSOURCING

AWS welcomes the opportunity to provide comments on the Central Bank of Ireland's ('the Central Bank') Consultation Paper 138 – Cross Industry Guidance on Outsourcing. Our response provides views from the perspective of a Cloud Service Provider ("CSP") and reflects our experiences providing cloud services to a global customer base and adhering to the highest international security standards, including compliance within existing financial services (FS) certifications and accreditations.

In 2006, AWS began offering IT infrastructure services to businesses in the form of web services – now commonly known as IaaS cloud computing. Today, AWS provides highly reliable, secure, scalable, and low-cost cloud infrastructure that powers a wide range of businesses and public sector entities around the world. In particular, AWS financial services customers vary in size from fintech startups to global systemically important banks (or G-SIBs) and operate in every industry segment including asset management, banking, capital markets, and insurance. The AWS cloud enables these customers to innovate faster and more cheaply while improving their security posture and operational resilience. Our infrastructure technologies encompass compute, storage, databases, and networking, and we also offer technology services such as machine learning.

We welcome the efforts by the Central Bank in terms of aligning its approach to that of the European Supervisory Authorities ('ESAs'), which is already being broadly implemented across the EU financial services sector. These efforts, we believe, provide a consistent regulatory approach to financial firms based in Ireland and across the EU looking to move workloads to the cloud. Further, we believe the establishment of an internationally consistent and fair regulatory framework for the use of cloud services is critical in order to support the long-term competitiveness of the EU financial services sector by enabling its digitalization.

While we are broadly supportive of the Guidance, there are specific areas of concern from a CSP perspective. For ease of read, we have addressed these in Annex 1, and have also included suggested alternatives for your consideration. In addition to this, and specifically in relation to the issue of systemic risk, we would like to set out some views we believe are important in terms of the ongoing policy discussions in Ireland, but also in the EU and at the international level. These are based on our response to the Financial Stability Board's Consultation on "Regulatory and Supervisory Issues Relating to Outsourcing and third party relationships"[1].

[1] https://www.fsb.org/2020/11/regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships-discussion-paper/

First, we strongly believe financial entities (FEs) can decrease their operational risk by running well-architected applications on the AWS cloud. Indeed, the cloud helps FEs to ensure better operational resilience than legacy IT systems; and by helping individual FIs decrease individual operational risk, address and manage threats, cloud helps ensure stability of the overall financial system and minimize systemic risk.

Further, the robustness of AWS' cloud services and infrastructure, together with our security, services and tools help customers to ensure continuity of their services, which is a key prerequisite for financial stability. It is worth noting that every customer's workload deployment on AWS is different, which means that virtually no two customers are exposed to the exact same set of technology when using AWS as their service provider. For example, two customers who run their websites using AWS services will most likely be using different physical data center buildings, hardware, and different core services to build their solution.

AWS and the FS industry share a common interest and responsibility in maintaining operational resilience. Indeed, CSPs like AWS make it easier for FEs to manage operational resilience than legacy IT systems. FIs benefit from an infrastructure that has been designed for resiliency and integrates multiple levels of redundancy. To avoid single points of failure, AWS minimizes interconnectedness within our global infrastructure. AWS's global infrastructure is geographically dispersed over five continents, with 81 availability zones (AZs) in 25 Regions[2]. The AZs, which are physically separated and independent from each other, are built with highly redundant networking to withstand local disruptions. Regions are isolated from each other and designed so that a disruption in one Region does not result in contagion in other Regions. Compared to global FEs' on-premises environments today, the locational diversity of AWS's infrastructure greatly reduces geographic concentration risk. In addition, although the likelihood of such incidents is very low, AWS is prepared to manage large-scale events that affect our infrastructure and services. The AWS core infrastructure also provides FEs with the ability to monitor their resources 24/7 to help ensure the confidentiality, integrity, and availability of their customer data.

At the firm level, to most effectively manage operational risks (including technology risk), AWS encourages FEs to establish an enterprise-wide, holistic understanding of their business activities in order of priority (e.g., mission critical, business critical, operational) along with the associated people, processes, and technologies that enable FEs to meet their desired business outcomes. This comprehensive approach enables FEs to effectively manage and mitigate risk utilizing key performance indicators and key risk indicators to appropriately escalate, as necessary. This also aligns with an Enterprise Risk Management (ERM) approach, which evaluates Operational Risk Management (ORM) risks together with all other risk areas that may impede or impair a FE from achieving its business objectives (e.g., governance, financial, human resources, reputational, operational, technology).

We note the Central Bank also refers to multicloud as an option to enhance operational resilience. For clarity, by multicloud we refer to the idea of building workloads that can run/are interoperable across any cloud provider or a customer's own data centers. Requirements related to the adoption of a multicloud environment would increase operational complexity and risks, as well as costs. Further, this approach commoditizes cloud providers, forcing financial organizations to standardize on the lowest common denominator, and preventing them from taking advantage of higher-level security services and other technical enhancements offered by certain providers. Any requirements in this regard would necessarily make the assumption that all providers are the same, whereas in reality providers vary significantly in terms of their implementation, security, operational performance, and rate of innovation. Also, and as stated in our response to the FSB's Consultation, any measures which, deliberately or not, restrict the ability of

[2] See more on AWS Global Cloud Infrastructure, including existing and announced regions, here: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

financial entities to select their provider strictly on the basis of a risk assessment and preferred service offerings, including mandatory multicloud requirements, would be counterproductive to the aim of enhancing the resiliency and security of the financial system.

We thank again the Central Bank for the opportunity to comment, and would appreciate the opportunity to discuss the responses included in the submission.

Kind regards,

Maria E. Tsani
Head of Financial Services Public Policy – EMEA

Annex: Comments and suggested changes

I) **Part A: Introduction**

- **Section 3 - Purpose and Scope (Page 9)**

> *"The Central Bank's Guidance (the Guidance) as set out in this document is therefore in keeping with the requirements set out in the EBA Guidelines and the EIOPA and ESMA Guidelines. The Guidance will apply in a proportionate manner, to all regulated firms and not just those covered by the scope of the EBA, EIOPA and ESMA Guidelines. "*

AWS comment: Nothwistanding the objective of the Central Bank to align its requirements with those set out in the ESAs Guidelines, we would suggest clearly setting out the areas where the Central Banks wishes to introduce new or different requirements. For instance in Part B, section 7, the proposed requirements largely reflect section 78 of the EBA Guidelines, however it also introduces entirely new requirements. Hence, to facilitate compliance, and for the benefit of both in-scope financial entities and Outsourced Service Providers (OSPs), we would suggest establishing a framework that facilitates the assessment of those requirements that deviate from the ones included in the ESA's Guidelines.

II) **Part B: Cross-Industry Guidance on Outsourcing Risk**

- **Section 5.1 - Sub-Outsourcing Risk (Pages 20-21)**

AWS Comments: In order to align the Central Bank's approach to sub-contracting with that under the ESA's Guidelines, we suggest introducing the concept of material threshold to ensure there is a risk-based and proportional application of monitoring, approval and other requirements. We also suggest adding the concept of "material chain outsourcing" to ensure financial entities focus on issues that could raise risks to its operational resilience and avoid an overly burdensome regime that requires them to dedicate resources to non-material issues.

- **Section 7 - Contractual Arrangements and Service Level Agreements (Pages 30-32)**

AWS comments: We would suggest the Central Bank to reconsider some of the required contractual provisions as these could lead to increased operational risk and compromised security. In particular:

> *"**7.1.g.** The location(s) (i.e. towns/cities, regions, and countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the regulated firm, in advance, if the OSP/CSP proposes to change the location(s);"*

In some cases, this may give away the location of a provider's data centers, leading to potential security challenges. This is particularly relevant in a cloud multi-tenant environment, as security risks would affect not a specific financial entity but other customers within as well as beyond the financial services industry.

> *"**7.1.h.** Where control/custody of data is being outsourced, requirements regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data. (These should provide for appropriate and proportionate information security related objectives and measures including*

requirements such as minimum cybersecurity requirements, specifications of firms' data life cycle, and any requirements regarding data security management, network security and security monitoring processes, operational and security incident handling procedures including escalation and reporting);"

It is worth noting that AWS financial services customers have the ability to choose where to store their data. In the EU in particular, our customers can choose one or more of our regions in including in France, Germany, Ireland, Italy, Sweden; and in Spain from 2022. AWS services and tools that allow customers to determine where their data is, how it is secured, and who has access to it. Services such as AWS Identity and Access Management (IAM) allow customers to securely manage access to AWS services and resources. AWS services, such as AWS CloudTrail and Amazon Macie enable governance, compliance, detection, and auditing, while AWS CloudHSM and AWS Key Management Service (KMS) allow customers to securely generate and manage encryption keys.

*"**7.1.i**. Regulated firms should, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes;"*

It is worth noting that the key objective of the Threat Intelligence-Based Ethical Red Teaming (TIBER) framework is to enable the financial institutions to learn and evolve based on test outcomes. AWS has been supportive of the work of the European Central Bank (ECB) to develop a consistent approach, the TIBER-EU framework published in May 2018. In line with some of the proposals being considered in the ongoing negotiations on the Digital Operational Resilience Act (DORA), we believe efforts are needed to enhance the TIBER-EU framework, looking to standardize and harmonize the way for all financial institutions to perform intelligence- led red team tests across the euro-area. This would facilitate cross-border, cross-regulatory tests on pan-European institutions to find the weak spots across jurisdictions. These efforts would also prevent overlapping or incompatible national testing standards being developed by individual EU Member States. It is worth mentioning that the first set of tests carried out by EU regulators and financial institutions, which began in 2016, did not involve ICT TPPs, such as AWS. While we are supportive of the inclusion of third-party providers, the subject of the testing itself should remain the institutions and not the providers. Further, we urge the Central Bank to support an approach whereby results concerning providers could be re-used for the purposes of testing of different institutions.

- **Section 7.2 - Termination Rights (Pages 32-33)**

AWS comments: AWS' customers can effectively terminate contracts for any reason at any given time. However, in some cases, customers may wish to introduce specific clauses to suit their own business considerations. Hence, we kindly suggest the Central Bank to reconsider this provision to introduce some flexibility and effectively make it less restrictive.

- **Section 9 - Disaster Recovery and Business Continuity Management (Page 38)**

AWS comment: Specifically with regards to the requirement 9.h "Conduct coordinated testing of these arrangements on a regular basis and report the results to the boards of both the regulated firm and the OSP". We urge the Central Bank to consider the major security risks attached to this requirement for third

parties, such as AWS. Additionally, this is a significant departure from the EBA Guidelines which provide at section 104(c) that institutions should "**review** all other relevant information received from the service provider, including reports on business continuity measures and testing". In this sense, we urge the Central Bank aligns with the EBA in this respect.