Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland
Via e-mail: *fsb@fsb.org*

13 January 2021

AMAZON WEB SERVICES (AWS) RESPONSE TO THE FINANCIAL STABILITY BOARD'S PUBLIC CONSULTATION "OUTSOURCING AND THIRD-PARTY RELATIONSHIPS"

Dear Madame/Sir,

Amazon Web Services ("AWS") welcomes the opportunity to offer comments on the Financial Stability Board (FSB) consultation on "Outsourcing and third party relationships". 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 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, resilient, secure, scalable, and low-cost cloud infrastructure that powers a wide range of businesses and public sector entities around the world. AWS customers in the financial services industry vary in size from fintech startups to the largest global institutions, 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 cost-effectively 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 FSB's efforts to advance the discussions on the issue of outsourcing, and cloud in particular, on the international regulatory agenda. Given the global nature of both finance and technology, coordination and harmonization across jurisdictions is critical in order to secure a level playing field and avoid market fragmentation. Further, we believe these efforts could contribute towards the establishment of an internationally consistent and fair regulatory framework for the use of cloud services that supports the digital transformation of the sector globally. In addition, given the rapid level of technological innovation, we strongly believe any regulatory initiatives should remain flexible enough to handle increasingly dynamic complexities in the financial and technology spaces. In this sense, we support the FSB's call for further analysis and discussion to address emerging cross-border challenges.

We also urge the FSB and its members to consider the need to develop a regulatory framework suitable for the digital world. Legacy policies, procedures, tools, and resources may be insufficient to manage the

evolving risks faced by Financial Institutions (FIs) as they adopt new technologies at scale, such as cloud infrastructure computing. We believe regulatory and supervisory practices should take into account the evolving technology landscape, for example, by requesting FIs to periodically reassess their technology risk and security methods. The aim would be to consider the emerging risks, as well as technological advances that can improve the effectiveness by which these risks are mitigated. Incorporating the principle of "modernization" into risk management would incent FIs to leverage available resources, including those offered by their third party service providers which may help them to improve their security posture and effectively govern the use of technology across their organizations.

We thank the FSB for the opportunity to comment and would also appreciate the opportunity to discuss the responses included in the submission.

Kind regards,

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

Questionnaire

1. What do you consider the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships, including risks in sub-contractors and the broader supply chain?

We welcome the FSB's reference to cloud as an "enabling technology", as mentioned in page 6 of the discussion paper. Indeed, we believe that cloud enables innovation and digital transformation by lowering the cost of experimentation while providing a safe environment to do so. Our customers, regardless of size, also inherit the same high bar for security because we constructed the AWS cloud for the most security intensive organizations in the world. Specifically, AWS enables firms of all sizes to adopt state-of-the-art security services and capabilities such as fine-grained control of identity and access management, cryptography, managed Distributed Denial of Service (DDoS) protection, and threat detection.

Modern technology such as cloud services can be used to overcome traditional challenges associated with cost overruns and technology failure. Financial entities can leverage globally distributed infrastructure to build redundancy in all components of the ecosystem and modernize, standardize and automate antiquated, manual disaster recovery processes. The same technologies can also be used to prevent and detect fraud or misuse of the services. There will always be a potential for misuse of any technology, but that should not deter financial entities from adopting new technologies that may improve service delivery while enhancing resiliency and security.

We fully appreciate the importance of business continuity and disaster recovery in the context of operational resilience. As demonstrated by our response to the COVID-19 pandemic, by proactively preparing for potential disruptions, we have been able to scale servers and network capacity in order to respond to additional load resulting from changing work patterns, while protecting our customers from short-term supply disruptions. By doing this, our financial services customers, and also our non-financial services customers, have been able to scale up as needed, so they can continue to leverage AWS as normal. Further, AWS maintains diversity in our supply chain from multiple locations around the world, as well as significant buffer capacity, which allows us to work around disruptions in our supply chain as we continue to grow capacity, add new instance types, and expand in our regions[1]. Our Business Continuity Policy lays out the guidelines used to implement procedures to respond to a serious incident or degradation of AWS services, including the recovery model and its implications on the business continuity plan. This is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement. AWS' comprehensive approach to business continuity planning is designed to mitigate risks to people, facilities, equipment, and technology. These efforts are intended to protect the safety and well-being of our employees and maintain continuity of our business operations.

[1] AWS Regions are physical locations around the world where we cluster data centers. We call each group of logical data centers an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area. Unlike other cloud providers, who often define a region as a single data center, the multiple AZ design of every AWS Region offers advantages for customers. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple AZ's to achieve even greater fault-tolerance. AWS infrastructure Regions meet the highest levels of security, compliance, and data protection.

In addition, while we appreciate questions from regulators about how we and our customers minimize the potential for concentration risk, we strongly believe financial institutions (FIs) can decrease their operational risk by running well-architected applications on the AWS cloud. Indeed, the cloud helps FIs 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.

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. Further, 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. In this sense, AWS can be conceptualized as a set of building blocks that can be combined in infinitely different ways. 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. CSPs like AWS make it easier for FIs to manage operational resilience than legacy IT systems. Indeed, FIs benefit from an infrastructure that is 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 77 availability zones (AZs) in 24 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, meaning that a disruption in one Region does not result in contagion in other Regions. Compared to global FIs' 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. AWS becomes aware of incidents or degradations in service based on continuous monitoring through metrics and alarms, high-severity tickets, customer reports, and the 24x7x365 service and technical support hotlines. The AWS core infrastructure also provides FIs with the ability to monitor their resources 24/7 to help ensure the confidentiality, integrity, and availability of their customer data.

AWS believes that FIs should ensure that they—and the critical economic functions they perform—are resilient to disruption and failure, whatever the cause. By leveraging the cloud, FIs have the ability to architect and build workloads that are able to withstand outages and security threats. AWS provides tools that enable FIs to deliver secure and resilient services that also comply with regulatory requirements. In the design, building, and testing of their applications on AWS, customers are able to achieve their objectives for operational resilience. For example, AWS customers can take advantage of the redundancy within AWS regions (e.g. Elastic Load Balancing) and managed Distributed Denial of Services (DDoS) protection (AWS Shield Advanced). Furthermore, customers can use the AWS Well-Architected Framework build secure, high-performing, resilient, and efficient infrastructure for their applications. Automating security tasks on AWS enables FIs to be more secure, by reducing human configuration errors and giving them more time to focus on other work critical to their business.

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

Additionally, FIs get access to AWS' third party certifications proving their compliance with international security standards. AWS operates thousands of controls that meet the highest standards of operational resilience in the industry. To understand these controls and how we operate them, FIs can access security standards and compliance certifications issued by third parties. For example, our System and Organization Control (SOC) 2 Type II report, reflecting examination by our independent third-party auditor, provides an overview of the AWS Resiliency Program. Additionally, AWS aligns with the ISO 27001, the ISO 27017 guidance on information security in the cloud and ISO 27018 code of practice on protection of personal data in the cloud and other standards.

Lastly, FIs are not "locked in" to our contracts with them and can generally terminate them at any time. FIs can choose to deploy any of AWS' services in a manner that suits their business needs. For example, AWS offers many licensing options where FIs can bring their own license, or use license-integrated services (e.g., Windows licenses) or take advantage of available open source licenses when using the services. Customers can switch between these options as necessary for their operational needs. Further, AWS can support FIs in planning their reversibility/exit strategies, which would help FIs to migrate the workloads successfully and promptly onto a new IT environment – either to an on-premises solution or to a different CSP. Such reversibility/exit planning helps ensure effective operational resiliency of FIs.

2. What are possible ways to address these challenges and mitigate related risks? Are there any concerns with potential approaches that might increase risks, complexity or costs?

We welcome and fully concur with the statement in page 3 related to the multiple benefits outsourcing and other third-party relationships can bring to FIs. As mentioned above, particularly in relation to the topic of systemic risk, cloud allows enhanced operational resilience at the firm level, which translates into a net reducing effect of operational risk across the financial system.

At the firm level, to most effectively manage operational risks (including technology risk), AWS encourages FIs 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 FIs to meet their desired business outcomes. This comprehensive approach enables FIs 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 FI from achieving its business objectives (e.g., governance, financial, human resources, reputational, operational, technology).

Further, technology risks should not be viewed in a silo, as this has historically created a disconnection wherein specific risks were viewed as an "IT problem" rather than an organization-wide business problem. By integrating all risks, including ORM risks, into an overarching ERM program, FIs will be able to establish a holistic, enterprise understanding of their risks. Once these risks are defined, mapped, understood, and tracked across the institution, FIs can perform due diligence and traceability to provide confidence that all of their material risks are addressed and their business objectives can be achieved.

In relation to alternative approaches, we stress that the location of data should generally have no bearing on data security or the ability for a regulator to oversee the institution that owns or controls the data. Indeed, we strongly believe that allowing cross-border data flows and avoiding data residency restrictions enable financial institutions to fully realize the full benefits of cloud, including resiliency and security.

Requiring a "locally stored back-up of relevant data" introduces inherent complexity and security risk, depending on the specific implementation, while increasing costs. It is worth noting that regulated entities that are CSP customers own and control their data and as such, can promptly retrieve relevant data regardless of where it is stored. A regulated entity can furthermore provision access to a designated third party, other than its cloud service provider, that would be responsible for responding to regulators' requests in case the regulated entity does not.

Additionally, any measures which, deliberately or not, restrict the ability of financial entities to select their provider strictly on the basis of a risk assessment and preferred service offerings, including mandatory multi-cloud requirements, would be counterproductive to the aim of enhancing the resiliency and security of the financial system. In particular, requirements related to the adoption of a multi-cloud environment would increase operational complexity and risks, as well as costs. 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. For clarity, by multi-cloud we refer to the idea of building workloads that can run/are interoperable across any cloud provider or a customer's own data centers. 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.

3. What are possible ways in which financial institutions, third-party service providers and supervisory authorities could collaborate to address these challenges on a cross-border basis?

AWS fundamentally believes in the value of globally resonant and actionable financial regulatory principles. Given the global and interconnected nature of financial services, a common set of principles will serve to further the development of a pragmatic, principles-based approach to strengthening operational resilience. Over time, we believe in the need for an effective cross-border regulatory framework for technology providers that provide the same set of services globally, such as AWS. The FSB would play an important role in achieving this, taking a leadership role in enabling cross-border regulatory cooperation.

As a starting point, given the rapidly evolving regulatory agenda on cloud, we believe the FSB could provide a useful forum for the development of globally consistent definitions and terminology related to outsourcing and cloud. For example, the FSB could consider the definition of outsourcing found in the US Federal Financial Institutions Examination Council's IT Handbook. The FFIEC defines outsourcing as, "the practice of contracting through a formal agreement with a third-party/ies to perform services, functions, or support that might otherwise be conducted in-house."[1] Additionally, we urge the FSB proposes the use of a definition for "operational resilience" consistent with the definition used by the Basel Committee on Banking Supervision: "… the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adopt to, as well as recover and learn from disruptive events in order to minimize their impact on the delivery of critical operational through disruption." The adoption of a globally consistent set of definitions and terminally would facilitate cross-border supervisory discussions, but could also allow for cross-border resilience simulations and exercises.

Additionally, building on the ongoing work already happening in the EU in the context, we urge the FSB and its members to consider the development of a global taxonomy for incident reporting, which would facilitate cross-border cooperation amongst regulatory authorities. A common understanding of major IT-

related incident with significant impact on financial entities would benefit the financial sector as a whole. A shared set of definitions (or taxonomy) and cooperation amongst authorities will also enhance the ability of national regulators to detect potential sources of financial risk by providing them with a comprehensive picture of incidents occurring in other jurisdictions.

Further, we urge the FSB and its members to collaborate to achieve a harmonized set of regulatory and supervisory requirements that:

- Leverages existing global standards where possible and recommend these be used as the foundation on which financial institutions develop their cloud risk management frameworks;
- Harmonizes as much as possible with other jurisdictions to avoid confusion and potential conflicting requirements; and
- Develops mechanisms to enable an on-going and bilateral dialogue with its regulated entities wherein financial institutions can raise questions and provide feedback, and regulators can provide additional guidance on how to interpret principles-based guidance in a constantly evolving digital context (e.g., with respect to location of records requirements).

We also note that, in most cloud service models, providing meaningful data to the regulator requires the involvement of regulated entities. Customers using cloud services maintain control over their data. AWS recommends that customers implement additional security measures over their data on cloud (e.g., to encrypt data and to own and manage the encryption keys). A CSP, such as AWS , has no visibility or control over the customer data, and will not be able to either decrypt the data or separate specific data under investigation from other data of other entities in the same corporate group that are not under investigation. Therefore, in order to get access to readable and specific data sets, the best course of action for a regulator to take is to directly request information from its regulated entities.

4. What lessons have been learned from the COVID-19 pandemic regarding managing and mitigating risks relating to outsourcing and third-party relationships, including risks arising in sub-contractors and the broader supply chain?

AWS has helped banks and other financial services organizations quickly scale their technology infrastructure to help maintain business continuity during these unprecedented times. For example, we recently worked with a global bank to expand its high-performance computing grid to scale in response to unprecedented market volumes and volatility. We have continued to work with a range of customers to refine their Disaster Recovery strategies and to ensure business continuity even during the most adverse circumstances.

By proactively preparing for potential disruptions, we have been able to continue servicing our customers and attend to specific needs resulting from the pandemic, such as the increase in working from home arrangements. For data center operations, we have segmented our data center staff in each region into sub-teams to assure that we can both protect our employees and our ability to support our data centers. Regarding capacity, we have proactively scaled both servers and network capacity in order to be able to respond to any additional load that we see as a result of changing work patterns or protect our customers from short-term supply disruptions. We also have diversity in our supply chain from multiple locations

around the world, as well as significant buffer capacity, and were able to work around disruptions in our supply chain as we continue to grow capacity, add new instance types, and expand to new regions.

Similarly, in relation to our network capacity, the AWS's global network is regularly tested and scaled well ahead of demand. This has allowed us to respond to emergent needs that have arisen as part of COVID-19 changes. Further, just as we have with our data center staff, we have similarly segmented our support staff into sub-teams to assure that we have sufficient support bandwidth available to help deal with any potential customer questions or issues that may arise.

Based on feedback from our financial services customers, we have enhanced the ability of our customers to respond to COVID-19 by:

- Providing additional capacity to meet the changing computing and storage needs of customers, including the rapid shift to work from home and increased reliance on video conferencing and collaboration tools.
- Providing strong security controls and monitoring of the cloud.
- Providing the ability to enhance resiliency through geographic diversity and high availability of service.