October 8, 2024

Mr. Neil Esho
Secretary General
Basel Committee on Banking Supervision
Bank for International Settlements
Centralbahnplatz 2
4051 Basel, Switzerland

Subject: AWS response to the Basel Committee on Banking Supervision (BCBS) consultative document: Principles for the sound management of third-party risk

Dear Mr. Esho:

Amazon Web Services (AWS) is grateful for the opportunity to comment on the Basel Committee on Banking Supervision (BCBS, or "Committee") consultative document: *Principles for the sound management of third-party risk* ("Principles").[1] We welcome the Committee's efforts to strengthen third-party risk management in the banking sector and to promote alignment and coordination on an international scale.

Technologies such as cloud computing enable digital transformation and rapid innovation. As financial institutions (FIs) continue to adopt these technologies, principles-based, proportionate, and outcomes-focused regulatory frameworks can help foster innovation, security, and resilience. Given the global importance of financial services and technology, coordination among the public and private sectors and ensuring regulatory harmonization are essential for a thriving financial sector. To this end, the work of international bodies such as BCBS is critical to ensuring effective risk management in an evolving technology landscape. With rapid technological innovation in financial services, we strongly believe the enumerated Principles should remain adequately flexible. We appreciate the Committee's focus on remaining technology-agnostic, promoting international engagement, and reducing regulatory fragmentation.

AWS is committed to working with the financial services community to enhance operational resiliency and security. We believe enhancing the document in some key areas will assist FIs to interpret and apply the Principles effectively. In particular:

(i) We commend the Committee's efforts to ensure the concepts of *criticality* and *proportionality* apply to all the Principles and the full lifecycle of third-party risk management. There is further scope for the requirements set out in the document to be applied proportionately as it is currently unclear which requirements apply to critical versus non-critical third-party service provider arrangements. In the absence of this clarity, the requirements may impose undue burden upon FIs and third parties.

(ii) Concerns about concentration in the provision of technology services should be addressed through proven risk management approaches: define, identify, manage, mitigate, and transfer. Until we have a definition of concentration within technology services, it will be difficult to determine where the risk appears and how it should be addressed.

[1] Basel Committee on Banking Supervision, Consultative Document: Principles for the sound management of third-party risk, July 2024. https://www.bis.org/bcbs/publ/d577.pdf

Please find our detailed feedback below.

1. Definitions

AWS is supportive of the Committee's view on aligning definitions with those previously defined by the Committee and other international standard-setting bodies, and to ensuring a common understanding of key terms. For purposes of global alignment and defragmentation, any definitions should rely on existing global standards. Delivering a lexicon for common terms and definitions around third-party risk management and outsourcing is an important step to enhancing coordination. We would advocate for further clarity on the Committee's definition of certain terms:

Critical TPSP arrangement: The definition of critical third-party service provider (TPSP) arrangement could benefit from further clarity as the inclusion of TPSP arrangements which "support(s) or impact(s)" critical services, is unclear and overly broad. This could lead to a disproportionate number of TPSP arrangements being considered "critical". We recommend amending the definition to ensure it aligns with the Committee's intention for its principles to be applied on a proportionate basis. Specifically, we recommend critical TPSP arrangement be defined as "a TPSP arrangement which materially supports the provision of one or more critical services provided to a bank, where a defect or failure in its performance would materially impair their financial performance, the soundness or continuity of their banking and payment services and activities, or their continuing compliance with their regulatory obligations."

Critical TPSP: We are concerned that having separate definitions for "critical TPSP arrangement" and "critical TPSP" may create the potential for conflicting definitions. Identifying "critical TPSP arrangements" in the context of their own operations is sufficient for FIs to effectively manage third-party risk and optimize resilience. We recommend removing the category of "critical TPSP" entirely to avoid confusion and unnecessary additional burden.

Supply chains, nth party, and key nth party: While an nth party's ability to access sensitive or confidential bank information is an important consideration from a data protection and cybersecurity perspective, it is not an accurate proxy for access to information that could interfere with a bank's critical or material operations. Moreover, the definitions of and guidance for nth parties and supply chains do not provide for a criticality threshold of a service. The Committee should make it clear that third-party risk management need not flow down to nth providers that are not critical to the provision of a service.

Concentration risk: Concentration risk has no uniform definition. As defined by the Committee, concentration risk *can* result from a number of different situations and circumstances, at the bank level and at the systemic level, however it can be mitigated through banks appropriately architecting their environments and cloud services providers (CSPs) providing relevant tools.

- At the bank level, the Committee's definition refers to "risk arising from a dependency of a bank on one or more services provided by a single TPSP (directly or indirectly through nth parties) or a limited number of TPSPs…". Choosing a single service provider is not indicative of concentration risk and it can reduce complexity and reduce attack vectors. Concentration is not a new concept and is common in the financial services industry, especially in the securities and capital markets sector where some settlement and custodial services may only be offered by one entity. It is important to note that choosing a single service provider is not necessarily inherently risky and not indicative of concentration risk. Concerns that cloud services are concentrated at a sector, geographic, or service level perspective are unfounded as robust architecture by cloud users and

locational diversity by CSPs can manage and mitigate this risk.[2] While the Principles focus on identifying, measuring and monitoring concentration risk, our view is efforts are better focused on ensuring FIs establish robust operational resilience plans to handle potential disruptions in critical operations and that third-party providers are similarly focused on resilience.

From an operational risk perspective, CSPs offer access to necessary skills and expertise, which may reduce an entity's cyber risk, particularly for smaller entities with limited resources. CSPs typically have substantially more secure and resilient IT infrastructure than alternatives, such as smaller-scale infrastructure owned and managed by FIs. CSPs are also able to make investments in security and resilience that exceed that which individual entities or even industry sectors may be able to make. CSPs proactively mitigate potential concentration risks by offering services via physically separate locations and logically segregated IT systems. Even if multiple FIs exclusively use the same CSP, this would not create a problematic concentration risk so long as that CSP's infrastructure and services are offered via physically separate locations and are designed to be highly secure and resilient. The US Treasury observes, "the potential for increased resilience to physical and cyber incidents, with the use of multiple data centers or regions from the same CSP and broader use of encryption and zero trust models" as one of the primary drivers of cloud adoption in financial services.[3] The Financial Stability Board also notes, "financial institutions may choose to increase their use of a given service provider for various reasons…These attributes can strengthen financial institutions' resilience and improve the efficiency and flexibility of their operations."[4]

If the purported concentration risk pertains to concentration of services or geographic concentration risk, both can be mitigated through FIs appropriately architecting their environments. Service providers are incentivized to support interoperability. If a service provider cannot reasonably interoperate with these third-party solutions, customers will either stay with their current provider or choose an alternative that supports interoperability. AWS provides services and features that aid customers migrating workloads both to and from AWS, including AWS Application Migration Service and AWS Database Migration Service.

As noted also by the US Treasury in its report on the adoption of cloud by financial services, "the mere presence of large CSPs is not necessarily an issue for the financial sector's operational resilience. Evaluating the operational risks that could arise from concentration in cloud services depends on how firms use and design these services."[5] In the case of cloud services, diversification by way of additional providers often increases operational complexity while providing limited practical benefits in terms of resilience.

- At the systemic level, while the potential exists for a technology failure to affect multiple FIs, particularly where the FIs are using the same provider, there are limited examples of such incidents occurring. As noted by the Program on International Financial Systems

[2] There is substantial evidence that the cloud services sector is not concentrated. Since 2006, many providers around the world have begun offering IT services on-demand over a network. Google Cloud (launched in 2008), Microsoft Azure (2010), Rackspace (2010), Dell (2011), IBM (2011), OVHcloud (2011), DigitalOcean (2012), Hewlett Packard Enterprise (2012), Oracle (2016), Cloudflare (2018), Flexential (2019), and others have entered and continue to expand. AWS also vigorously competes with on-premises IT components, which capture the large majority of IT spend.

[3] US Department of the Treasury, The Financial Services Sector's Adoption of Cloud Services, Feb. 2023, https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

[4] Financial Stability Board, Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities, Dec. 2023. https://www.fsb.org/uploads/P041223-1.pdf

[5] US Department of the Treasury, The Financial Services Sector's Adoption of Cloud Services, Feb. 2023, https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

(PIFS) in its whitepaper Cloud Adoption in the Financial Sector and Concentration Risk "the financial system has proven operationally resilient: disruptions resulting from the failure of a technology service provider can occur, even at great financial cost, without triggering a systemic crisis."[6] The discussion around the use of CSPs in financial services has tended to highlight the reliance by FIs on a handful of major providers. The total number of CSPs is only one data point on which to base the discussion of systemic concentration risk. As noted by PIFS, "cloud adoption in the financial sector is varied and, for many FIs, still in its early stages… critical operations—those involved in processing transactions, updating accounts, and reconciling ledgers—are still largely conducted using legacy IT systems…For "core" workloads—defined as workloads related to core systems, such as back-end process and systems that manage customer interactions throughout the bank—the percentage of workloads that had been migrated to the cloud…stood at a paltry three percent."[7]

The locational diversity of AWS's infrastructure can greatly reduce geographic concentration risk. To avoid single points of failure, AWS minimizes interconnectedness within our global infrastructure, reducing geographic concentration risk, by doing the following: (i) Regions are designed to be independent and are isolated from each other, meaning that a disruption in one Region does not result in contagion in other Regions; (ii) Availability Zones within each Region are physically separated and independent from each other, built with highly redundant networking to withstand disruptions; and (iii) compared to on-premises environments, the locational diversity of AWS's infrastructure greatly reduces geographic concentration risk.

The identification of important TPSPs to FIs is in its infancy in many jurisdictions. As this identification progresses it will be important to review and assess the data on the impact of additional measures imposed on such TPSPs.

We recommend the Committee's approach to concentration risk can be strengthened by acknowledging that choosing a single provider is not indicative of concentration risk and will often lead to an overall lower net risk position than pursuing a multi-provider strategy[8]; explicitly stating that running workloads in an active-active configuration across two different service providers is extremely technically complex; confirming that the intent is for FIs to be aware of the level of concentration among their service providers, and to only take mitigating actions where the FI considers it necessary in a way that will not increase its overall net risk position.

2. Principles

Governance, risk management and strategy: Principles 1 and 2

---

[6] Program on International Financial Systems (PIFS), "Cloud Adoption in the Financial Sector and Concentration Risk", April 2023. https://www.pifsinternational.org/cloud-adoption-in-the-financial-sector-and-concentration-risk/ (page 11)

[7] Program on International Financial Systems (PIFS), "Cloud Adoption in the Financial Sector and Concentration Risk", April 2023. https://www.pifsinternational.org/cloud-adoption-in-the-financial-sector-and-concentration-risk/ (page 8)

[8] For example, the Treasury noted in its February 2023 white paper: "…[w]hile many financial institutions can increase resilience by operating in multiple regions of the same CSP, few experts believe that complex use cases can be developed to support seamless failover from one CSP environment to a different CSP environment. Reasons include the inherent differences among service offerings, the associated complexity of designing across multiple cloud environments, and the need to hire multiple staff familiar with various environments." US Department of the Treasury, The Financial Services Sector's Adoption of Cloud Services, Feb. 2023. https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

The guidelines around governance, risk management, and strategy should clearly reflect the concepts of *criticality* and *proportionality.* As the Committee states, critical services typically warrant a greater level of risk management consideration. The oversight and approval responsibilities of the board and senior management should be aligned with the Committee's corporate governance principles and should be proportionate to the criticality of the TPSP arrangement.[9] For example, the board's approval should be limited to oversight of the strategic framework governing critical TPSP arrangements, rather than individual arrangements.

With regards to risk management, while we recognize the importance of banks assessing bank-level concentration risk during the due diligence phase, we caution against over-indexing on concentration as a risk. FIs should focus instead on optimizing their resilience posture to respond to potential disruptions. For reasons described in detail above, we caution against advising multiple service providers as a mitigation against perceived concentration risk, given this may result in greater technical complexity and weaken a bank's resilience and security postures.

Risk assessment: Principle 3

The proposed definition of a critical service takes a risk-based and outcome-focused approach, based on the impact of failure or disruption: "a service provided to a bank, the failure or disruption of which could significantly impair a bank's viability, critical operations, or ability to meet legal and regulatory compliance obligations." However, Paragraph 28 suggests an alternate approach, outlining factors to be considered to determine "criticality" of potential services provided by an arrangement with a TPSP. To avoid confusion, we recommend the Committee to remain consistent with the proposed definition.

Due diligence: Principle 4

Appropriate due diligence should follow the principles of criticality and proportionality, to avoid overburdening banks and TPSPs. The Committee should also clarify that banks may rely on third-party certifications for effective due diligence. AWS encourages reliance on established, widely adopted standards, frameworks, and guidelines. Permitting coordinated, standardized solutions for audit, testing, and assessments ensures high-quality, consistent and efficient evaluation while reducing the potential for operational disruption. Most TPSPs are not financial services firms and TPSPs should adopt the policies, procedures, and leading practices appropriate for its sector. FIs and supervisors should accept sector-appropriate materials, including those validations, certifications, and assessments that demonstrate compliance.

The following are examples of documentation or processes AWS has developed, which customers across multiples sectors can use when conducting onboarding due diligence and ongoing monitoring:

- AWS Well-Architected Framework, which describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud and helps customers build secure, resilient, and efficient infrastructure for a variety of applications and workloads;
- AWS Compliance Program, which helps customers to understand the robust controls in place at AWS to maintain security and compliance of the cloud;
- AWS FedRAMP compliance, which provides details on AWS' compliance with the Federal Risk and Authorization Management Program (FedRAMP), a US government-

[9] Basel Committee on Banking Supervision, "Guidelines for Corporate Governance Principles for Banks," July 2015. https://www.bis.org/bcbs/publ/d328.pdf

wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP uses NIST 800-53 as a baseline for its security requirements, and adds additional controls for cloud services.

- Dashboards about events that might affect AWS services and resources and assurance offerings, providing up-to-the-minute information on service availability. Customers can review the current status information of services at any time or can subscribe to an RSS feed to be notified of any interruptions to each individual service;
- Information on Amazon financials, insurance, and other information available to the public on the Amazon Investor Relations website; and
- Ongoing direct engagement with customers including monthly and quarterly business reviews.

Paragraph 38 requires banks to consider their "ability (including cost, timing, contractual restrictions) to exit the TPSP arrangement and either transition to another TPSP or bring the activity back in-house". Changing or shifting among IT providers has always required time, effort and money, but cloud computing has made that process easier than ever before. AWS does not place contractual restrictions in cases where a customer may decide to cease using AWS services. This means that if a customer decides to move, they can do so without unreasonable difficulty. Whereas customers using on-premises IT solutions have been and continue to be largely "locked-in" to costly infrastructure legacy hardware, as well as software that only runs on specific hardware and costly licensing fees, the introduction of cloud computing has greatly increased customers' ability to move to another vendor. AWS provides many services and features that can aid customers migrating workloads both to and from AWS, including services such that customers will not even need AWS' assistance to retrieve their assets, nor even to migrate off of AWS. AWS was the first on-demand IT provider to offer pay-as-you-go pricing, creating an immediate reduction in the cost and burden of switching providers and solutions. With AWS, customers have full control, ownership, and portability of their data.

We recommend avoiding an over-prescriptive approach to managing TPSP exits and suggest the Committee amend this provision to refer to "the bank's ability to exit the TPSP arrangement without undue disruption" which would allow more flexibility to FIs.

Contracting: Principle 5

With respect to contracting, the Committee notes a number of potential contractual provisions that FIs might consider including in their contracts and provides that 'the nature and details of these contracts should be appropriate to the banks and the criticality of the services provided by the TPSPs…' While this is the case, banks should also consider the nature of the service provided and whether particular contractual terms are required for particular relationships. As FIs are best placed to manage their contractual requirements with the CSP, depending on business plan, workloads, and materiality, we caution against imposing prescriptive requirements related to contractual details.

With respect to the proposed requirement for banks' contracts governing TPSP arrangements to include "rights of banks to access (including premises), audit and obtain relevant information from the TPSPs", we would re-emphasize the importance of leveraging existing certification standards, third-party attestations and reports. In addition to being more efficient and effective for individual FIs, leveraging existing reporting will enhance the consistency of critical third-party due diligence across FIs. In the case of AWS, we provide our customers with an overview of IT standards we comply with by certifications and attestations; laws, regulations and privacy; and alignments and frameworks. Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. AWS customers remain responsible for complying

with applicable compliance laws, regulations and privacy programs. Compliance alignments and frameworks include published security or compliance requirements for a specific purpose, such as a specific industry or function.

Customers can also benefit from efficient assurance measures such as audit symposiums, that are offered digitally, and pooled audits. Permitting coordinated, standardized solutions for audit, testing, and assessments ensures high-quality, consistent and efficient evaluation while reducing the potential for operational disruption. There is growing global recognition by international authorities (e.g., 2023 BIS, 2023 US Treasury, 2021 MAS) of the value of pooled audits, reliance on independent third-party audit reports, and other audit efficiencies for third-party assessments.[10] AWS agrees with these authorities and encourages entities to rely on consolidated or pooled testing and audit, third-party audit reports. In its February 2023 white paper, the Treasury acknowledged that "intensive in-person audits are challenging to accommodate at scale while maintaining the security of the multi-tenant environment," and noted its support for "alternative approaches to one-to-one audits like pooled audits, certifications, or real-time updates to customers" and "efforts that could yield efficiency gains for both CSPs and FIs without compromising outcomes."

Moreover, we would caution against requirements that include knowledge of a specific industry or firm-level operations as this can negatively impact efforts by third parties to develop clear and consistent documentation about their services. In AWS's case, the tools we provide to customers to facilitate due diligence are generally industry agnostic. The safety and security of AWS's services are paramount and our approach remains the same irrespective of the industries in which our customers operate.

Paragraphs 41-42 also set out impracticable requirements related to business continuity and disaster recovery. In particular, we recommend amending as follows the bullet on "obligations and responsibilities relating to business continuity and disaster recovery for the services provided ~~and to support banks' BCP and DRP testing as appropriate~~". As we note in further detail below under Principle 8, requiring CSPs to support banks' BCP and DRP testing is not appropriate for how CSPs provision services. It is fundamentally a bank's responsibility to build its own BCP and DRP and it will be unique to every FI. FIs need to ensure that their cloud workloads are architected, operated, and tested to meet the workload's specific requirements for business continuity and disaster recovery. AWS provides FIs with the capability to implement their own robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple AWS regions as well as across multiple AWS Availability Zones within each AWS region, but the resiliency of our FIs' workloads ultimately depends on how they have architected those workloads using our services. CSPs have limited capacity to influence these elements as the banks are responsible for architecting their own environments.

Additionally, joint testing would involve the disclosure of the provider's own business contingency plan to the FI. This would involve the disclosure of confidential security information, which could create a risk to the security of the multi-tenant environment. This would affect both FI's data and all other FI data, significantly reducing resiliency and not achieving the goal of reducing risks associated with TPSPs in the banking sector.

---

[10] Juan Carlos Crisanto, Jefferson Umebara Pelegrini And Jermy Prenio, Financial Stability Institute, Bank Of International Settlements, FSI Insights On Policy Implementation No. 50, (2023); US Department of the Treasury, The Financial Services Sector's Adoption of Cloud Services, Feb. 2023. https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf; Letter from Tommy Tan, Director & Head (Division I), Monetary Authority of Singapore to Chief Executive Officers of All Financial Institutions (June 1, 2021), https://www.mas.gov.sg//media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/RiskManagement/Cloud-Advisory.pdf

In regards to "obligations and responsibilities for BCPs and DRPs should include minimum service uptime and/or maximum service downtime commitments, recovery time objectives (RTOs) and recovery point objectives (RPOs)", requirements for "minimum service uptime and/or maximum service downtime commitments" also do not align with how CSPs provision services. These will all be within the FI's control in regards to how they architect their environment and based upon their unique business needs. While we do include information about service uptime in our service level agreements (SLAs), it's not feasible or reasonable to expect a contract to include such information as it is highly dependent upon how a FI builds their environment.

Onboarding and ongoing monitoring: Principles 6 and 7

We advise the Committee to explicitly apply the principles of criticality and proportionality to the guidelines provided for ongoing monitoring of TPSP arrangements. For example, the triggers for review of TPSP arrangements listed under Paragraph 48 are extensive and may lead to excessive and unnecessary review processes regardless of whether the changes impact the TPSP's provision of services to the bank. Such reviews should only be triggered when events directly impact the TPSP's ability to provide their services to the bank.

Business continuity management: Principle 8

Paragraph 58 suggests "using multiple TPSPs" as a possible recovery strategy or compensating control. In the context of cloud computing, we caution against advising banks to follow a multi-cloud strategy. Many global authorities note that multi-vendor, multicloud failover entails significant cost and complexity that can be detrimental to overall efforts to improve uptime, reduce risks, and improve security and resiliency. For example, the US Treasury noted in its February 2023 white paper: "…[w]hile many financial institutions can increase resilience by operating in multiple regions of the same CSP, few experts believe that complex use cases can be developed to support seamless failover from one CSP environment to a different CSP environment. Reasons include the inherent differences among service offerings, the associated complexity of designing across multiple cloud environments, and the need to hire multiple staff familiar with various environments." The Monetary Authority of Singapore has made similar observations about multicloud saying, "FIs should be cognizant of the added complexity of operating in a multi-cloud environment, such as having adequate resources and appropriate expertise in securing and managing the use of different public cloud services and ensuring the consistent enforcement of policies."[11] In the UK the discussion paper on operational resilience (DP 3/22) highlights: "Although substitutability could be an important factor in assessing the potential impact of the failure or disruption of a third party's services, the supervisory authorities do not require firms and FMIs to adopt a multi-vendor strategy".[12]

AWS agrees with the importance of robust BCPs. In the context of cloud services, business continuity is a shared responsibility between an FI and their CSP(s). FIs need to ensure that their cloud workloads are architected, operated, and tested to meet the workload's specific requirements for business continuity and disaster recovery. FIs also need to understand how the cloud services and underlying infrastructure they rely on contribute to the resilience of their cloud workloads. AWS can provide services that meet certain SLAs, but the resiliency of our customers' workloads ultimately depends on how they have architected those workloads

[11] Letter from Tommy Tan, Director & Head (Division I), Monetary Authority of Singapore to Chief Executive Officers of All Financial Institutions (June 1, 2021), https://www.mas.gov.sg//media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/RiskManagement/Cloud-Advisory.pdf

[12] Joint UK Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) Discussion Paper 3/22 – Operational resilience: Critical third parties to the UK financial sector (paragraph 4.33)

using our services. To ensure a flexible, proportionate and risk-based approach, we would not suggest adding more detail regarding what should be included in a BCP given these plans can be very FI and workload specific.

As part of AWS's Well-Architected Framework, we work with our customers to communicate our approach to disaster recovery including the development of BCPs. Doing so supports AWS's shared responsibility model and helps customers' make informed decisions with regards to their approaches to resilience and recovery. In addition, AWS's business continuity measures are assessed as part of Systems and Organization Controls (SOC) 211 Reports adhering to internationally recognized standards.

Paragraph 60 advises banks to "consider joint design and testing of BCPs with TPSPs, or utilise independent parties to do the same". Business Continuity Management plans are sensitive and requiring TPSPs to share these has the potential to jeopardize the multi-tenant environment and is not operational for companies that operate on a 1-to-many model. Testing should not further exacerbate or create new vulnerabilities. Moreover, conducting joint tests is not scalable and is unnecessary given the wide availability of third-party certifications. Reliance upon disaster recovery certifications or third-party certifications is a scalable and widely acceptable proxy for FIs as part of comprehensive ICT risk management. For AWS, for example, the disaster recovery tests are a technical program where failure scenarios are simulated on a center's critical infrastructure, which includes electrical, mechanical, controls and ancillary systems inclusive of life safety. It is also possible to conduct failure simulations, as well as simulate power failure of an availability zone. Given the one-to-many model, AWS is able to test a plethora of situations that would be difficult or expensive for a financial entity to test on its own. 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 widely recognized 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. In addition, 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. For AWS, such certifications are carried out independent of AWS and other CSPs to internationally recognized standards. Compelling financial entities to engage in individual testing would be costly and less effective than relying on third-party certifications, which can enable the testing of multiple scenarios in ways a single firm may not be able to achieve.

Role of supervisors: Principles 10 and 11

We agree with the Committee's efforts to analyze available information to identify potential systemic risks. Most third-party providers, including CSPs, do not pose an inherent systemic concentration risk. As discussed above, while the potential exists for a technology failure to affect multiple FIs, particularly where the FIs are using the same provider, there are limited examples of such incidents occurring. The discussion around the use of CSPs in financial services has tended to highlight the reliance by FIs on a handful of major providers. However, it is important to acknowledge that concentration in a single or small number of service providers is not the only relevant consideration for resilience. The total number of CSPs is only one data point on which to base the discussion of systemic concentration risk.

The identification of important third-party service providers to financial entities is in its infancy in many jurisdictions. To assess effectively the potential for systemic third-party risk will require specific information on how third-party providers and their services are used on a firm-by-firm level. As stated by the US Treasury "the key issue for policymakers and financial authorities is in understanding the potential aggregate impacts on financial institutions' functions and the services that financial institutions provide to consumers and

businesses."[13]

Establishing mechanisms for cross-sectoral and cross-border coordination and dialogue is critical to facilitate a better understanding of third-party service operations in the financial services space. This includes regulator-to-regulator coordination and avoiding potential regulatory fragmentation as a result of a multiplicity of requirements across jurisdictions, which in some cases could lead to conflict of laws and would have a detrimental effect on the resiliency and security of the global financial system. The Bank of England (BoE)'s Cross-Market Operational Resilience Group (CMORG), the Euro Cyber Resilience Board (ECRB), Asia Pacific Financial Sector Cloud Resilience Forum (FSCRF), and the U.S. Financial Services Sector Coordinating Council (FSSCC) provide good examples of private-public partnerships that could serve as a basis for a voluntary mechanism at the international level to facilitate the above. These groups provide the opportunity for sector-wide collective action on operational resilience, as well as discussion and consultation on operational resilience matters among industry participants.

* * *

Thank you for the opportunity to contribute to this important consultation. We would welcome the opportunity to expand on our submission in a discussion with BCBS and we remain available to provide any further information. Please reach out to Anum Malkani (anmalkan@amazon.com).

Sincerely,

Anum Malkani
Financial Services Public Policy Lead, Asia-Pacific & Japan
Amazon Web Services

[13] US Department of the Treasury, The Financial Services Sector's Adoption of Cloud Services, Feb. 2023. https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf;