Amazon Web Services (AWS) response to the Financial Stability Board (FSB) consultative document: *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities*

Introduction

Amazon Web Services (AWS) is grateful for the opportunity to respond to the Financial Stability Board (FSB)'s consultative document *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities*.

We welcome the FSB's efforts to advance its work on third-party risk management and oversight on an international scale. Given the global nature of both finance and technology, coordination and interoperability of regulatory approaches across jurisdictions is essential to secure a consistent approach to risk management. The establishment of an internationally consistent, proportionate and risk-based toolkit for financial authorities and financial institutions (FIs) supports the digital transformation of the sector globally.

Given the rapid level of technological innovation in financial services, we strongly believe the framework should remain flexible enough to handle increasingly dynamic complexities in the financial and technology spaces. In addition, we urge the FSB and its members in developing the toolkit to keep in mind its application to the digital world.

By taking into consideration the evolving technology landscape, the aim of such a toolkit would be to consider emerging risks as well as technological advances that can improve the effectiveness by which these risks are mitigated. The toolkit should incorporate the principle of modernization into third-party risk management, which may incent FIs to leverage available resources, including those offered by their third-party service providers, to help them improve their security postures and effectively manage their third-party and outsourcing-related risks

AWS recommendations for the toolkit

- Enhance coordination between financial authorities and, where possible, leverage existing best practices and global standards to limit regulatory fragmentation and redundancies;
- Develop mechanisms to enable an on-going dialogue between financial authorities and their respective regulated entities, which enable FIs to raise questions and provide feedback on third-party risk management guidance, and through which financial authorities can provide additional guidance on how to interpret risk-based, outcomes-focused guidance; and

- Encourage increased understanding by financial authorities of technologies that are supporting regulated FIs through the voluntary provision of information by third-party service providers to relevant financial authorities

Chapter 1 – Common Terms and Definitions

1. Are the definitions in the consultative document sufficiently clear and easily understood? Are there any important terms and definitions that should be included or amended?

AWS is supportive of aligning definitions where possible, as proposed by the FSB. We recognize that complete harmonization of terms is not always possible, but believe attempting to establish consistent terminology across jurisdictions is an important first step to developing interoperable approaches to regulation and supervision of third-party risk.

We would advocate for further clarity on the FSB's definition of certain risk terms. While the FSB notes that common risk terms are not defined in the document, there are certain terms – notably concentration risk – which are not commonly understood in the context of third-party risk management and the provision of technology services. The U.S. Department of Treasury (U.S. Treasury) Cloud Executive Steering Group[1] work on developing a common lexicon and the International Organization for Standards (ISO) work on technical guidance for operational resilience[2] are examples that could be leveraged for this purpose.

Our view is the definition of critical service provider could benefit from further clarity in the context of the proposed toolkit. The concept of critical shared services was established in the 2013 FSB Paper *Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services*.[3] In addition, the Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures (CPMI) defines a critical third party as a *third-party service provider that are essential to an FMI's operations, such as information technology and messaging providers*.[4] We would seek clarity as to how these apply and how the definition of critical services works with these established definitions.

The distinction between FIs and service providers providing services to FIs should be made clearer. The current definition of critical service provider includes the term critical services rather than critical shared services and, in our view, critical shared services, as defined in the 2013 FSB Paper, is more appropriate. The presently proposed definition of critical service lacks

[1] U.S. Treasury press release on the Cloud Executive Steering Group (May 2023)
[2] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1, Subcommittee (SC) 38 and Working Group (WG) 5 – Data in cloud computing and related technologies
[3] https://www.fsb.org/wp-content/uploads/r_130716a.pdf
[4] https://www.bis.org/cpmi/publ/d00b.htm?&selection=194&scope=CPMI&c=a&base=term

acknowledgement of how the services of a provider can be used to support the services or functions provided *by* the FI to its customers. In the case of a service provided by a service provider the service should not be 'critical' unless it is used to support the critical functions of the FI.

While the definition of critical service provider makes clear the 'critical service' must be a service provided by a service provider *to* the FI, the definition of critical service is broader and could be interpreted as including those services provided *by* the FI itself to its customers. We recommend clarifying the definitions to denote the difference between a critical service of the FI, provided to customers of the FI, and a service provided by a service provider, which may support the provision of the FI's operations or functions, the latter being the purpose of this consultation.

Chapter 2 – Scope and General Approaches

2. Are the scope and general approaches of the toolkit appropriate?

The focus on critical services is an appropriate basis for the proposed toolkit. If expanding beyond this scope there should be a clear proportionate and risk-based reason to do so in order to deliver an appropriate approach by both financial institutions and financial authorities.

It will be important that the toolkit evolves in line with digital practices to be effective and efficient as technology evolves, supporting the highest level of security of both providers and financial institutions. In addition, supervisory authorities may consider utilizing new or evolving solutions that do not create security risks for both third-party service providers and their customers when gathering and handling evidence as part of their supervision, for example auditees may provision and secure virtual data rooms for audit evidence and related artifacts to be provided to maintain the files in an immutable format, with access log files, accessible to auditors into the future.

3. Is the toolkit's focus on regulatory interoperability appropriate? Are there existing or potential issues of regulatory fragmentation that should be particularly addressed?

AWS supports the FSB's focus on regulatory interoperability. Similar to established practice within regulated FIs, streamlining compliance obligations and facilitating coordination between authorities enables FIs to focus on their risk management activities rather than on compliance with individual regimes.

When considering regulatory interoperability, we welcome reference to existing, relevant certifications and standards. We would also be supportive of exploring controls that are appropriate for third-party service providers in specific categories that are imperative to the security, resiliency, and operability of regulated FIs.

In particular, our view is the following established and audited controls and certifications could be leveraged: Cybersecurity (e.g., NIST 800 series); Information Security (e.g., ISO 27001 (International: Information Security Management), NIST Cybersecurity Framework and C5 (DE: Cloud Computing Compliance Controls Catalog)); Business Continuity (e.g., ISO 22301 (International: Business Continuity Management)); Privacy (e.g., ISO 27701 (International: Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management). These examples demonstrate how third-party service providers can provide scalable and thorough assurance to customers and, consequently, financial authorities.

4. Is the discussion on proportionality clear?

Proportionality is an important consideration for any toolkit and we appreciate the statement that tools "may be appropriate for large, complex financial institutions but disproportionate or unsuitable for small, less complex financial institutions."[5] It is important that in any application of the toolkit proportionality is properly assessed.

In the context of cloud computing, matters of security, compliance, and resilience, FIs and their cloud service providers (CSPs) have a shared interested in the stability of the financial system. Working in tandem through AWS's shared responsibility model, we help relieve a customer's operational burden and increase its overall security and resiliency posture. This model acknowledges the non-delegable duties established by regulation and emphasizes that responsibility for cybersecurity and operational resilience is shared by a CSP and its customer.

The operating model for cloud services includes components that are managed and controlled by both the CSP and the customer, and controls that are managed by both parties. The CSP operates, manages and controls the components of the host operating system (i.e., the physical security of the facilities in which the services operate). The customer assumes responsibility for and management of the guest operating environment (including backup creation for parallel structure, identity and access management, updates, encryption, etc.) and other associated application software as well as the configuration of the CSP-provided security group firewall. Any standards must incorporate and build on this widely understood concept that delivers a robust and resilient architecture in financial services. Additional requirements should be proportionate and additive to this model, enhancing third-party risk management postures.

[5] https://www.fsb.org/wp-content/uploads/P220623.pdf (page 10)

Chapter 3 – Financial Institutions' third-party risk management

5. Is the focus on critical services and critical service providers appropriate and useful? Does the toolkit provide sufficient tools for financial institutions to identify critical services? Do these tools rightly balance consistency and flexibility?

6. Are there any tools that financial institutions could use in their onboarding and ongoing monitoring of service providers that have not been considered? Are there specific examples of useful practices that should be included in the toolkit?

Please note we have chosen to address questions 5 and 6 together.

AWS supports the focus on critical services and critical service providers. That said, we would emphasize that a service is rarely critical in and of itself – i.e., it is highly dependent on how the service is used by a given FI. We agree that "financial institutions are… usually best placed to assess the criticality of services they receive"[6]

AWS is also supportive of the FSB's efforts to enhance cooperation and regulatory interoperability for the identification of critical services, noting this can promote consistency and comparability of effective third-party risk management efforts. AWS agrees with the FSB's objective to establish consistent approaches, where possible.

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

- AWS Well-Architected Framework[7], 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;
- 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.

[6] https://www.fsb.org/wp-content/uploads/P220623.pdf (page 11)
[7] https://aws.amazon.com/architecture/well-architected/

AWS would also emphasize the importance of leveraging existing certification standards, third-party attestations and reports, where available, for the purposes of conducting due diligence. 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. AWS agrees with these authorities and encourages entities to rely on consolidated or pooled testing and audit, third-party audit reports.

In support of the FSB's desire to promote flexibility in the toolkit, we suggest some changes to the due diligence and contracting considerations noted in the toolkit. For example, in AWS's case, the tools we provide to customers to facilitate due diligence are generally industry agnostic. We would caution against the provision of 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. 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.

With respect to contracting, the toolkit notes a number of potential contractual provisions that FIs might consider including in their contracts and provides that 'the nature and detail of contracts should be appropriate to the financial institution and the criticality of the service.' While this is the case, FIs should also consider the nature of the service provided and whether particular contractual terms are required for particular relationships. For example, the toolkit suggests that an FI may consider a service provider's obligation to take out insurance against certain risks. Existing guidance of the EBA[8], suggests the contract between a provider and its customer determine whether insurance is required and, if applicable, the level of insurance cover required.

[8] EBA Guidelines on outsourcing arrangements (Article 75(k))

7. What are the potential merits, challenges and practical feasibility of greater harmonisation of the data in financial institutions' registers of third-party service relationships?

AWS supports the efforts of the FSB to encourage the harmonization of definitions, where possible, noting that this common understanding of terms improves clarity and consistency, and enhances communication among stakeholders. As noted, the shared responsibility model is one such example of a mechanism through which we communicate and engage with our customers about the safety and security of the services we provide.

AWS supports the identification by financial authorities of global standards for the measurement of third-party risks and controls. It is necessary that the relevant certifications and standards are aligned with minimum resilience standards to ensure consistency across services.

The identification of critical services and their level of criticality is dependent on a number of factors that are often unique to each FI including, but not limited to, how the service is used by a given FI, the FI's internal risk and control environment, as well as the FI's unique risk appetite. While agreed upon terms and definitions may assist with the consistency of data inputs, given the individual firm-level factors that go into measuring risk, it will be challenging to identify a set of harmonized third-party risk data across FIs.

The usefulness of harmonized data is also dependent on what one is trying to measure. As noted in the U.S. Treasury's report *The Financial Services Sector's Adoption of Cloud Services*,[9] "the impact from an operational incident will depend on how individual financial institutions use and manage the cloud service and how critical that service is to the financial institutions' core operations." That many FIs use the same provider or that they have deemed the same provider as critical for their own operations in and of itself may not be a useful piece of data from a risk-management perspective if the FIs are using and managing the services provided by that provider in different ways.

8. Are the tools appropriate and proportionate to manage supply chain risks? Are there any other actionable, effective and proportionate tools based on best practices that financial institutions could leverage? Are there any other challenges not identified in the toolkit?

As noted by the FSB, "for service providers, particularly those that provide services to many different entities, there are similar practical limitations, particularly around cost, resourcing and

[9] https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf (page 7)

time”[10] with respect to monitoring and managing supply chain risks. In light of this, AWS supports the FSB’s proportionate and risk-based approach.

We understand the rationale for focusing on those nth-party service providers that are *essential to the delivery of critical services* but, to understand the role of those nth-party service providers, the materiality of those services is an important consideration. We do not believe there is currently agreement on what ‘essential’ means nor is there a consistent approach adopted by financial authorities to identify such providers across FIs. The extent to which an nth party is essential, may also be dependent how the FI uses the service. AWS recognizes the importance of this issue to financial authorities and our customers in assessing their third-party providers.

9. What do effective business continuity plans for critical services look like? Are there any best practices in the development and testing of these plans that could be included as tools? Are there any additional challenges or barriers not covered in the toolkit?

AWS agrees with the importance of robust business continuity plans (BCPs), as highlighted in the toolkit. In the context of cloud services, business continuity is shared responsibility between an FI and their cloud service provider(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 service level agreements (SLAs), but the resiliency of our customers' workloads ultimately depends on how they have architected those workloads using our services. Given we are proponents of a flexible, proportionate and risk-based toolkit, 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) 2[11] Reports adhering to internationally recognized standards.

10. How can financial institutions effectively identify and manage concentration and related risks at the individual institution level? Are there any additional tools or effective practices that the toolkit could consider?

[10] https://www.fsb.org/wp-content/uploads/P220623.pdf (page 21)
[11] https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

AWS believes the toolkit would benefit from a definition of concentration risk. For the purposes of our response, we have assumed the FSB is referring to concerns resulting from overreliance on a single third party, subcontractor or geography.

The concept of concentration risk is not new to the financial services sector nor is it unique to cloud services. Rather, FIs have consistently made decisions, particularly with respect to IT, to establish relationships with a single service provider for several beneficial reasons including the uniqueness of the product or service offering and the stability arising from a long-term partnership with a single provider. Choosing a single service provider is not necessarily inherently risky from a concentration perspective and may have many benefits for customers. As noted by the U.S. Treasury in its report on the adoption of cloud by financial services, "the mere presence of large [cloud service providers] 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."[12]

Concentration risk can result from a number of different situations and circumstances, most notably at the firm level and the systemic level (see response to question 12 below, for AWS's discussion of systemic concentration risk). At the firm level, concentration risk can be further broken down into two key areas of focus: the perception that a lack of diversification in a given service provider increases the risk to an FI's ongoing operations, particularly in the case of a disruption; and concerns resulting from vendor lock-in, where an FI is forced to rely on a single provider, even in the event of a failure.

With respect to the first issue, while the toolkit is focused 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. In the case of cloud services specifically, but many other third-party providers more broadly, diversification by way of additional providers often increases operational complexity while providing limited practical benefits in terms of resilience. As stated by Gartner in its blog post *Improving cloud resilience through stuff that works,*[13] before considering a multi-provider approach an organization can "first properly resource all the *other* things you could be doing to improve your resilience in the cloud."

Cloud service providers play a vital role in achieving operational resilience. The robustness of AWS cloud services and infrastructure, together with our security services and tools help customers bolster the continuity of their services, facilitating financial stability. AWS global infrastructure is built to avoid single points of failure and minimize the impact of disruptions on customers and the continuity of services. AWS minimizes interconnectedness within our

[12] https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf (page 57)
[13] https://blogs.gartner.com/lydia_leong/2021/10/21/improving-cloud-resilience-through-stuff-that-works/

expanding global infrastructure, which reduces geographic concentration risk, by doing the following:

- Regions are designed to be independent and are fully isolated from each other, meaning that a disruption in one Region should not result in contagion in other Regions.
- Availability Zones within each Region are physically separated and independent from each other, built with highly redundant networking to withstand disruptions.
- Compared to global financial institutions' on-premises environments, the locational diversity of AWS's infrastructure greatly reduces geographic concentration risk.

It is worth noting that the use of terms such as Region and Availability Zone are AWS specific and the meaning of these terms can differ between service providers.

Other risks related to the commercial relationship with a given third party or the potential for externally-imposed restrictions (e.g., regulatory sanctions on the use a type of third-party provider or service) are best addressed by the FI having a clear strategy for critical workloads to meet legal requirements and move if necessary.

With respect to the second issue of vendor lock-in, changing or shifting among IT providers has always required time, effort and money, but cloud computing has made that process easier than ever before. Avoiding lock-in means that if a customer decides to move, it 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, the introduction of cloud computing has greatly increased customers' ability to move to another vendor. 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. They can choose one or more services that meet their particular needs, and mix and match those with hardware and software from other providers, including on-premises providers, to create their overall IT solution. AWS helps make this possible by not requiring up-front payments or long-term contracts, and by building many services on open-source and industry standards that other IT providers also use. This makes it easier for customers to switch among or use multiple IT providers should they choose to do so. Avoiding lock-in does *not* mean there will not be tradeoffs or switching costs. These costs include time, flexibility, functionality as well as financial costs. However, cloud computing substantially reduces these potential costs.

Ultimately, AWS's view is that customers and the financial system more broadly benefit when firms have the freedom to choose what services to use, when to use them, and what steps they want to take to optimize operational resilience.

11. Are there practical issues with financial institutions' third-party risk management that have not been fully considered?

We have addressed this question in our responses to questions 5 to 10.

Chapter 4 – Financial authorities' oversight of third-party risks

12. Is the concept of "systemic third-party dependencies" readily understood? Is the scope of this term appropriate or should it be amended?

Most third-party providers, including CSPs, do not pose an inherent systemic concentration risk. 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 (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."[14]

The discussion around the use of cloud service providers in financial services has tended to highlight the reliance by FIs on a handful of major providers. We welcome the FSB's acknowledgement that concentration in a single or small number of service providers is not the only relevant consideration[15]

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."[16] PIFS further notes that concentration risk is not unique to CSPs stating "…a failure at an FI's managed, on-premises databases can knock out critical systems, like payments and other transactions."[17]

The identification of important third party service providers to financial entities 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 third-party service providers. We think the FSB's discussion of systemic third-party dependencies is warranted but may

[14] https://www.pifsinternational.org/cloud-adoption-in-the-financial-sector-and-concentration-risk/ (page 11)
[15] https://www.fsb.org/2023/06/enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities-consultative-document (page 32)
[16] https://www.pifsinternational.org/cloud-adoption-in-the-financial-sector-and-concentration-risk/ (page 8)
[17] https://www.pifsinternational.org/cloud-adoption-in-the-financial-sector-and-concentration-risk/ (page 13)

benefit from a more in-depth consideration of other factors. In particular, we would note that the FSB's focus on the provision of critical services "by one or a limited number of service providers… to many financial institutions" will not likely provide sufficient data about whether such a situation could give rise to systemic risks. Rather, 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 U.S. 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."[18]

13. How can proportionality be achieved with financial authorities' identification of systemic third-party dependencies?

To ensure the benefits of cloud and digital transformation in the financial sector can be harnessed, keeping proportionality and a risk-based approach in mind will be key. Measures should not pre-emptively restrict firms' choices about the most suitable operating model when it comes to third parties. The toolkit can help deliver a proportionate and a risk-based approach by supporting consistency and examples of best practices, but it should also be emphasized that the toolkit is a flexible instrument that is not intended to be interpreted by financial authorities as providing prescriptive requirements for a third-party regime.

Where possible, efforts should be made to ensure that the toolkit aligns with frameworks from organizations in other industries and reflect that many third-party services are provided agnostic to industry, promoting increased security and resiliency for industries ranging from government to healthcare, and offered across a multi-tenant environment.

14. Are there any thoughts on financial authorities' identification/designation of service providers as critical from a financial stability perspective?

As noted above, to ensure the benefits of digital transformation can be harnessed in the financial sector, the toolkit should focus on proportionate and risk-based service provider management, promote regulatory interoperability, and not pre-emptively restrict firms' choices about the most suitable operating model when it comes to third parties. The services provided by third-parties are often agnostic to industry and offered across a multi-tenant environment.

15. Should direct reporting of incidents by third-party service providers within systemic third-party dependencies to financial authorities be considered? If so, what potential forms could this reporting take?

AWS already invests in delivering transparent and open post-incident communication[19], and we

[18] https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf (page 7)
[19] https://aws.amazon.com/premiumsupport/technology/pes/

are happy to discuss how this can be developed to support the goals of the FSB toolkit. When it comes to direct reporting, FIs are well-placed to receive, react to and manage an incident notification from a third-party service provider, as they understand the impact to the FI and can report to the appropriate financial authority, as applicable and based on their compliance with applicable industry specific regulations.

It is also important to note that financial authorities, in designing any mechanism, should continue to think about the risks posed by sharing certain incident-related information versus the benefits gained. A live list of potential vulnerabilities runs the risk of being out-of-date and could have the unintended consequences, diverting resources from focusing on resolving issues to reporting on them.

16. What are the challenges and barriers to effective cross-border cooperation and information sharing among financial authorities? How do these challenges impact financial institutions or service providers?

We support engagement in international fora to deliver agreed principles and reciprocity to enable cross-border use of third-party services. The international financial system is inherently cross-border with global reach. As such, regulatory obligations that require FIs and third-party service providers to meet industry or country specific requirements may inadvertently divert resources towards burdensome compliance obligations instead of focusing efforts on security and resilience. To deliver an internationally consistent, proportionate and risk-based toolkit for use by third-parties in financial services it is important to consider what risks could result from additional obligations.

Existing international fora with the capacity to enable cross-border cooperation and information sharing include: FSB Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships; CPMI-IOSCO Principles on Outsourcing and Guidance on Cyber Resilience for FMIs; G7 Cyber Experts Group (CEG); and IAIS Operational Resilience Task Force (ORTF). In all of these dialogues, the opportunity for discussions with industry as thinking develops to ensure appropriate and workable initiatives is imperative.

17. Are there any views on (i) cross border information sharing among financial authorities on the areas covered in this toolkit (ii) including [certain third-party service providers] in cross-border resilience testing and exercises, including participation in pooled audits and?

One element of an interoperable regulatory regime for global active market participants is a recognition between authorities on the principles of an effective regime, which bodies such as the FSB can help establish. Reciprocity of trust is a well-established principle in financial services regulation. We support considering better cooperation between financial supervisory authorities, particularly where the jurisdictions are striving for equivalent outcomes.

For any resilience testing regime, it should build on the comprehensive and evolving testing that third-party service providers already carry out. Also, the testing of infrastructure must not endanger the data of FIs, and it must be carried out in a reasonable timeline and risk-based manner to ensure proportionate use of resources for both the third-party provider and the financial authority. This is applicable to cross-border exercises, as well.

18. Are there specific forms of cross-border cooperation that financial authorities should consider to address the challenges faced by financial institutions or service providers?

AWS is supportive of efforts to enhance cooperation and regulatory interoperability between financial authorities, particularly where the jurisdictions are striving for equivalent outcomes.

Cross-border regulatory cooperation is going to be crucial in ensuring that third-party risk management measures continue to support a robust, resilient global financial system. It should have the aim of scoping high-level principles capable of adoption across industries to ensure it recognizes the nature of how third parties are used by customers as well as information sharing among authorities to have a better picture of the global footprint of third-party providers and their functioning. Continued discussions with industry as thinking develops will be an important part of delivering appropriate and workable initiatives, which support transparency while protecting commercially sensitive information of FIs.

In terms of a proposed approach to collaboration, we would welcome exploring various mechanisms to enhance the sharing of information with relevant financial authorities to facilitate a better understanding of third-party service operations in the financial services space. This could also facilitate regulator-to-regulator coordination in the critical providers space avoiding potential regulatory fragmentation as a result of a multiplicity of requirements across jurisdictions, which is 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.

Another model, which could entail a regular cadence of provider specific information exchanges with jurisdictions – for example via the FSB or G7 – is where a specific provider could engage in discussions in relation to specific areas of concerns for financial authorities. It is worth noting that, for providers subject to oversight regimes in one or multiple jurisdictions, this may require explicit consent from their overseers, especially if, for example, there was a wish to share the

results of threat-led penetration testing exercise results. With any of the mechanisms proposed, requirements that are already in the process of being established for incident reporting could be leveraged in order to assess potential systemic risks.