Date: 7 January 2021

To: fsb@fsb.org

From: Robin Slade, EVP & COO, The Shared Assessments Program
robin@santa-fe-group.com
(630) 815-4420

RE: Outsourcing and third-party relationships

The Shared Assessments Program appreciates the opportunity to submit comments to the FSB's Discussion Paper: *Regulatory and Supervisory Issues Relating to Outsourcing and Third Party Relationships*. We have provided feedback on all four questions.

For context, the Shared Assessments Program has been setting the standard in third party risk assessments since 2005. Shared Assessments, which is the trusted source in third party risk assurance, is a member-driven, industry-standard body which defines best practices, develops tools, and conducts pacesetting research. Shared Assessments Program members work together to build and disseminate best practices and develop related resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments. More information on Shared Assessments is available at: http://www.sharedassessments.org.

On behalf of the Shared Assessments Program and its members, thank you for your time and consideration.

Sincerely,

Robin Slade
COO & EVP
The Santa Fe Group
Shared Assessments Program

We have two general comments regarding the guidelines as a whole:

1. Ideally, third party risk management guidelines should be jurisdiction-agnostic to match the global nature of outsourcing. This general comment is brought forward throughout our responses.

2. Guidelines with narrow focus on Cloud Service Providers (CSPs) controls and the outsourcer's requirements for monitoring those controls should ensure that outsourcer responsibilities are addressed around security, privacy, change management, continuity, and other configuration controls for which the outsourcer is directly accountable.

FSB Questions	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?
Overview Response	**Challenges:** • Inconsistent cross-jurisdiction regulatory requirements make it difficult to establish due diligence requirements in global enterprises that are workable in different countries. • As referenced in the discussion paper Annex Section 5, there is a significant challenge in obtaining and sharing information with downstream providers, especially when dealing with complex outsourcing chains. Too often there are no contractual requirements that bind downstream providers to comply with an outsourcer's security related contract provisions. • Pandemic related work-from-home requirements and a lack of mature remote environment security policies have significantly exacerbated security concerns. • Talent (skill set) issues pervade all aspects of identifying, managing, and mitigating risks related to outsourcing, especially around cyber-related risks.
Cloud and IT Managed Service Providers outsourcing	**Challenges:** Regarding regulators: • Cloud-related due diligence requirements are increasingly divergent across international jurisdictions, and the more aggressive requirements being brought forward are significantly outpacing current practices. • Regulators have routinely placed little or no emphasis on the outsourcer's responsibilities to monitor their own cloud operations, especially in Infrastructure as a Service (IaaS) environments. Data breaches have been well documented when regulated entities have not provided sufficient real-time oversight of their own operations once those operations have been moved to the cloud. Outsourcers are often not working in harmony with the CSP's. In particular: • Change management is being reported to take place at the outsourcer level without consultation on the impact that has to CSP system integration. This is resulting in system crashes and/or system intrusion. See also overview comments at the beginning of this response document. • While CSP performance can be governed by contract, compliance at the CSP level for data transmission tracking cannot be monitored effectively by the outsourcer. • Overall, key challenges exist in the CSP ecosystem as most CSP arrangements are "one size fits all", including access/audit rights, subcontracting notification and/or approval, and monitoring and performance data reporting. In existing relationships, timely contract changes may not be possible where changes to emerging guidelines have not been contractually bound by the outsourcer with its third party. • The requirements for notification prior to moving to the cloud in some industries is a conservative approach which, from a safety and soundness perspective, could be argued to be appropriate in certain settings. Whether a regulator would be able to reasonably process the volume of applications and understand the materiality in a given organization's unique situation is uncertain.

FSB Questions	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?
Cyber Risk	**Challenge:** • There is a significant challenge in obtaining and sharing information across risk domains when an event occurs with downstream parties. More complex supply chains often result in poorly coordinated and ineffective incident management response mechanics. Where no real-time process and information sharing during an event is available, resources are wasted that are needed to communicate with down-stream parties about the impact of incidents (e.g., recent nation state attacks demonstrate that a fundamental change has occurred in the cyber risk environment to which most outsourcers and third parties alike are currently ill-equipped).
Complex Chain Management – 3rd/4th/Nth Parties	**Challenge:** • Identification of downstream partners in complex outsourcing chains and an inability to assure satisfactory security controls at Nth parties poses a great challenge to all parties in the supply chain.
Cross-border regulations	**Challenge:** • Inconsistent cross-jurisdiction regulatory requirements are an increasingly important issue in third party risk management. • Inconsistent requirements make it more difficult to justify and establish consistent security hygiene and due diligence practices that are workable in different countries for global enterprises. • Areas where requirements are increasingly different are: (1) outsourcer inventory/register requirements; (2) cloud due diligence requirements; and (3) contractual requirements when third parties add their own outsourcing partners.
Concentration Risk	**Challenge:** • Regulators have inconsistent responsibilities for understanding when concentration risk rises to the level where it could compromise the stability of the financial sector performance in a given jurisdiction. • Those inconsistencies are reflected in the level of detail outsourcers are required to maintain and the means by which those details are to be reported when regulators request information. • Also, the ability for both regulators and outsourcers to obtain a complete picture of concentration risk that extends throughout a complex outsourcing chain is limited when outsourcers themselves do not have a full understanding of all the entities that may be working on their behalf.
What Challenges do regulators face?	**Challenge:** • Regulators face challenges due to inconsistencies in rules across jurisdictions. In particular, regulators do not have equivalent data access across international boundaries since requirements differ on a country-by-country or regional basis. • Only regulators have the ability to establish unified nomenclature across jurisdictions.
Data Protection	**Challenge:** • The lack of harmonization across jurisdictions around privacy requirements (e.g., data collection, data storage and transmission, etc.) complicates data management. This issue has been exacerbated by the current Covid-19 remote work environment where an entity's ability to assure compliance in a large work-from-anywhere employee base will vary by location. • It is a concern that regulators, third parties, and outsourcers have not begun to take into account in data protection rules the impact that post-quantum cryptography techniques will have on the ecosystem.
Limitations on Access, Audit and Information Rights	**Challenge:** • Monitoring requirements vary across jurisdictions, especially for cloud. • Small outsourcers may lack the leverage to require a third party to provide access for auditing purposes. Larger companies with more power in the market may be able to dictate contract terms. • Most CSPs will not permit access to secured sites, because they believe that doing so would compromise their security. Given the sensitive nature of the assets that CSPs manage, some form of rationality and process assurance would be needed in contracts to cover evaluation and access rights.

FSB Questions	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?
Overview comments	**Recommendation:** • Ensure more commonly shared standards across regions. • The presence of heightened contractual requirements to ensure good visibility throughout complex chain environments will allow outsourcers to know every level of the supply chain; thereby enabling an improved ability to identify, manage, and mitigate the risks across their ecosystem. Requirements to universally ensure the right for an outsourcer to object to and/or reject any new fourth/nth party would place a burden on the third or Nth party to ensure that its customers have transparency into the supply chain and a degree of control for the outsourcer to mitigate risks. • To improve the skill sets required to effectively identify and meet talent challenges that pervade all aspects of identifying, managing, and mitigating risks related to outsourcing, especially around cyber-related risks, minimum training requirements could be set for both regulators and outsourcers. Those minimum requirements could be built from and expanded upon based on the needs of individual organizations and agencies.
Cloud and IT Managed Service Providers outsourcing	**Recommendation:** • Harmonization of cloud due diligence standards across international jurisdictions is increasingly important. • An outsourcer's aggregate costs should include, at minimum, the resources to conduct the following tasks: (1) *pre-onboarding review* of vendor and services; (2) *contract review* regarding any controls changes needed over time; (3) *ongoing monitoring of criticality* and other impacts to the outsourcer; (4) *service architecture review* for each service migrated to CSP; (5) *ongoing architectural review* where notification or approval of CSP changes cannot be assured. This level of oversight and supervision, at some firms, may require an additional cost burden, because some organizations may need to hire incremental resources. Indeed, these guidelines assume a set of resources and processes for cloud management, including CSP monitoring, that may not be present today. Most firms may have to upskill and use new/adapted tools to govern and monitor CSPs. This would be a considerable additional burden to firms that do not already meet this level of maturity. Mature organizations would not be materially impacted. • Supplemental guidance should focus on monitoring the outsourcer's controls within the CSP's environment. In particular, change management is being reported to take place at the outsourcer level without consultation on the impact that has to CSP system integration. See also the comments in the Overview section of our response to question 1. In Infrastructure as a Service (IaaS) models, there is a shared responsibility for controls, with data, software, runtime, operating systems all being customer managed (i.e., the regulated entity's responsibility). In Platform as a Service (PaaS) models, the customer has responsibility for data and software controls. Guidance should ensure that responsibilities are addressed around security, privacy, change management, continuity, and other configuration controls for which the outsourcer is directly accountable. The outsourcer should be monitoring its own activities in the cloud, including configuration management with continuous monitoring capabilities. Additionally, there is the need to ensure that *appropriate logs* are maintained and reviewed for those CSP-hosted functions, which should be tracked in the same manner as if the application/system/service were hosted internally by the outsourcer.
Cyber Risk	**Recommendation:** • Please see Overview Comments at the beginning of this question 2 in our response.

FSB Questions	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?
Complex Chain Management – 3rd/4th/Nth Parties	**Recommendation:** • Harmonized internal guidelines could follow the European Banking Authority (EBA) and Bank of England Prudential Regulatory Authority (PRA) approach, which requires data on third parties and sub-outsourcers to be collected in a format that is easily accessible (available and in machine readable form from a single source). This allows regulators to assemble and analyze information that would be otherwise be difficult to obtain. • Guidelines should universally protect the outsourcer's right to object to and/or reject any new fourth/Nth party. • Require that enforceable contract clauses that provide the third party with the ability to monitor and manage the risks associated with all subcontractors associated with a complex chain. • The language in regulations or guidelines should provide clear direction suggesting what workable, functional language might increase adherence and active participation by third parties in achieving visibility throughout the outsourcing chain (at the Nth party levels). GDPR serves as an example of provisions that address the shared responsibilities for controllers/processers for the protection of both parties. This type of provision could impose a responsibility that provides leverage for appropriate controls and other contractually agreed upon access rights that would otherwise be absent in the relationship.
Cross-border regulations	**Recommendation:** • Rules harmonization would unify expectations across international jurisdictions to help reduce the deltas between requirements across jurisdictions.
Concentration Risk	**Recommendation:** • Regulators are uniquely positioned to provide visibility into concentration risk in any given jurisdiction, and should assume this responsibility in all geographies. Again, we recommend following the EBA and PRA approach that requires data on third parties and sub-outsourcers to be collected in a format that is easily accessible (available and in machine readable form from a single source), so that regulators can assemble and analyze that information. • To help identify concentration risk, a database needs to: (1) provide concentration data internationally and within individual jurisdictions; and (2) provide industry-specific registries/inventories of service providers. • The requirement for a centralized means of gauging concentration risk where CSPs are used by multiple outsourcer units would help outsourcers to recognize concentration risk. Such a tool would prove valuable for better understanding the tension between cost benefits of multiple licensing arrangements and concentration risk. • Ensure an industry-wide best practice approach is adopted on how to measure concentration risk. • Requirements could be set for parallel contracts to prevent a single point of failure, albeit at added cost to the outsourcer. This would require parallel processes to be in place and viable. In some settings, parallel services are not uncommon. Making this a requirement for all companies in a jurisdiction would level the playing field while raising the bar against concentration risk. • Clear requirements and consistency around the types of data that outsourcer must collect and how that can most effectively be provided to regulators to be better understand where concentration risks exist.
What Challenges do regulators face?	**Recommendation:** • Regulators should establish data exchange capabilities so that risk-related data can be assembled quickly and efficiently across jurisdictions. • Regulators face challenges Fintech financial services development. For instance, the use of regulatory sandbox efforts to encourage technology development in financial services have met with varying success across geographies. Regulators could share peer knowledge about best practices around sandbox processes and evaluation criteria. Process and results data sharing could prove useful in resource development at the regulator level. • Regulators should collaborate across geographies to unify terms related to outsourcing risk management.
Data Protection	**Recommendation:** • Regulators should encourage outsourcers and third parties to begin considering how post-quantum cryptography techniques impact outsourcing risk management once standards are finalized.

FSB Questions	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?
Limitations on Access, Audit and Information Rights	**Recommendation:** • A due diligence model could be developed by regulators collaboratively across jurisdictions, which could be adapted/adopted by regulators for their own jurisdiction and provide harmonized language and intent for rule making. • Rules should mandate that third parties monitor and mirror the same requirements with their fourth and Nth parties that are required under the third party's contract with the outsourcer. • With regard to the challenge of site security among CSPs, regulators could conduct their own due diligence examination and disseminate the results across international jurisdictions to supplement outsourcer analysis relative to their own risk environment. • Wider adoption of current EU CSP-specific guidelines could prod other jurisdictions to follow suit, which would encourage providers to meet this worthwhile requirement globally and help outsourcers to more reliably monitor their cloud service providers.

FSB Questions	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?
Overview comments	**Recommendation:** • Conduct regular, ongoing regulatory forums can be hosted by authorities from multiple jurisdictions that are open to stakeholders (financial institutions, third party providers, and supervisory authorities) to discuss key issues that could generate a broader array of stakeholder feedback to achieve regulatory harmonization to the greatest extent possible. • Begin to address the inconsistent cross-jurisdiction regulatory requirements and agree upon some uniformity for roles and responsibilities, document requirements, and establish rules for cross-jurisdictional sharing. This is critical for organizations that work in these various and highly disparate jurisdictions. • Chain outsourcing requirements and cross-border privacy are two aspects that require examination. Any compendium should cover a broad range of 'common sense' rules. • To foster collaboration and improve hygiene, stakeholders could collaborate to build consistency in processes, outsourcer inventory/register requirements, cloud due diligence requirements, and contractual requirements when third parties add their own outsourcing partners.
Cloud and IT Managed Service Providers outsourcing	• Please see Overview Comments at the beginning of this question 3 section and in the Limitations and Access Recommendations below in this question.
Cyber Risk	**Recommendation:** • Regulators can work with stakeholders to establish require remote access (work-from-home/work-from-anywhere) controls that match the new environment. Requirements for specific controls would substantially reduce risks.
Complex Chain Management – 3rd/4th/Nth Parties	**Recommendation:** • Regulators can work with stakeholders to establish periodic review and validation standards in contracts that require downstream vendors relevant to the scope of work to maintain transparency throughout complex outsourcing chains.
Cross-border regulations	**Recommendation:** • To foster a capacity to respond to regulations, regulators need to come together with stakeholders to establish requirements that establish greater uniformity across jurisdictions.

FSB Questions	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?
Concentration Risk	**Recommendation:** • Regulators should bring stakeholders together to agree upon standardized inventory and requirements and reporting formats and to establish effective data exchange mechanisms to evaluate concentration risk as required.
What Challenges do regulators face?	**Challenges:** • The FSB faces the challenge of whether it can be successfully leveraged to become a focal point in efforts to standardize requirements across geographies. • Regulators may lack sufficient resources to analyze emerging risks and make appropriate remediation recommendations.
Data Protection	**Recommendation:** • Regulators should work with standards organizations and other international organizations who can ensure that regulators are aware of the cyber risk challenges that are likely to emerge over time. • Regulators should collaborate with outsourcers and third parties to better understand real-world risks associated with work-from-anywhere environments and to develop guidance to minimize associated risks.
Limitations on Access, Audit and Information Rights	**Recommendation:** • In particular, cloud service providers and regulators globally urgently need to collaborate to develop a set of due diligence recommendations that apply internationally.

FSB Questions	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?
Overview comments	**Comments:** • The pandemic has demonstrated that force majeure clauses have been inadequate for many organizations across all industries. The insurance industry has faced significant challenges from Covid, as it has from other catastrophic events unfolding worldwide (extreme storms, wildfires, etc.). Some of these issues are still unfolding with severe consequences likely. • Many organizations have found that their risk management policies did not anticipate a wholesale shift to work-from-home environments; and as a result reasonable remedial processes have been, at least temporarily, at odds with documented policies. Organizations have learned to write policies that are inherently more flexible to accommodate extended emergencies. • Work-from-home security infrastructure and at due diligence issues have surfaced that are not adequately resolved as of this writing. • The area of predictive analytics, in some instances fostered by continuous monitoring, has evolved to provide better insight into emerging risks. • Real time analytics must be met with an educated work force capable of interpreting and acting upon sometimes complex data in the right context. Some organizations have faced employee skill set issues that are more difficult to solve in a COVID environment. • The lack of harmony in international regulations has proved to be more of an issue when there are global disruptions, such as the current pandemic.
Cloud and IT Managed Service Providers outsourcing	**Comments:** • COVID has significantly accelerated a pre-existing cloud outsourcing trend. This acceleration has occurred in an environment where forethought and planning that should be present before CSP outsourcing has not always been in place, resulting in the assumption of responsibilities that may have been outside the familiarity of the staff/companies using that technology. • Regulators need to look closely at companies moving into the cloud and the security hygiene being used to monitor risks.

FSB Questions	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?
Cyber Risk	**Comments:** • COVID has materially increased the cyber risk surface (as noted in Cloud/IT section above here in question 4). It is not clear whether regulatory supervision has kept pace with this change.
Complex Chain Management – 3rd/4th/Nth Parties	**Comments:** • There are different definitions of "materiality." A definition that could be applied across international boundaries would be valuable in this effort. Especially during the last two years, alternative definitions of materiality have emerged when considering Environmental, Social, Governance (ESG) related risks, including the terms "double" and "dynamic" materiality. We believe it is appropriate to consider ESG risks when considering materiality definitions. • Materiality is a gating factor in determining inherent risk. Outsourcers utilize the term to influence their third party due diligence protocols and policies to ensure that parties that provide critical business functions/activities have sound business continuity plans in place; and ensure that the business maintains communications with the third parties to mitigate any issues as early as possible. • The FSB can consider if there is any way it can alter the accepted definition of materiality so that key vendors and sub-outsourcers are held to account.
Cross-border regulations	**Comments:** • The FSB can foster harmonization in regulations to enable more agile and consistent responses in the face of disruptions.
Concentration Risk	**Comments:** • The rush to cloud has likely exacerbated concentration risk issues, but organizations may not be aware without a true enterprise-wide risk management structure in place.
What Challenges do regulators face?	**Comments:** • COVID may accelerate an increase in employees moving into positions as independent contractors. With more small contractors entering the field during a time when employee hiring protocols are changing, assuring that individuals are performing to a high standard is an increasing challenge.
Data Protection	**Comments:** • See the comments in Data Protection section in our response to question 1 regarding learnings and challenges around work-from-anywhere environments.
Limitations on Access, Audit and Information Rights	**Comments:** • The pandemic has driven assessment and audit toward virtual methodologies. Organizations may not have policies to adhere to appropriate due diligence in this environment. • There may be room for increased regulatory guidance regarding how to optimize the virtual assessment process. A greater regulatory focus and updated standards more efficient and effective assessments. • Regulators might consult on a set of virtual assessment expectations.