450 W 33rd Street
New York, NY 10001
United States

+1 212 931 4900 Phone
+1 212 221 9860 Fax
ihsmarkit.com

Ms. Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Mr. James P. Sheesley
Assistant Executive Secretary
Attention: Comments-RIN 3064-ZA26
Legal ESS
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW
Suite 3E-218
Washington, DC 20219

Submitted electronically via federalregister.gov

September 17, 2021

Re: Proposed Interagency Guidance and Request for Comment, RIN 3064-ZA26, 86 FR 38182 (July 19, 2021)[1]

IHS Markit (NYSE: INFO) is a world leader in critical information, analytics and solutions for the major industries and markets that drive economies worldwide. The company delivers next-generation information, analytics and solutions to customers in business, finance and government, improving their operational efficiency and providing deep insights that lead to well-informed, confident decisions.

,

IHS Markit came together with 16 leading financial services organizations and two of the "Big 4" consulting firms to design, build and launch a solution to drive improved TPRM risk management practices across the industry. Know Your Third Party ("KY3P") is focused on standardizing best practices for managing third-party risk and optimizing the processes by which financial institutions, including, in particular, banking organizations, assess and monitor inherent risk in engaging suppliers and entering into third-party relationships. KY3P is therefore a leading example of what the Proposed Guidance contemplates when it speaks of utilities and collaborative arrangements.

[1] Available at https://www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third-party-relationships-risk-management.

IHS Markit KY3P is pleased to have the opportunity to comment on the Proposed Interagency Guidance and Request for Comment ("Proposed Guidance") from the Board of Governors of the Federal Reserve System ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of the Comptroller of the Currency ("OCC") (collectively "the Agencies"). In particular, we welcome the Proposed Guidance's recognition that banking organizations can collaborate with one another to facilitate due diligence of particular third-party relationships by sharing expertise and resources. Moreover, the Proposed Guidance acknowledges that "[t]hird-party assessment service companies have been formed to help banking organizations with third-party risk management, including due diligence."[2]

I. Executive Summary

We agree with the Agencies that KY3P and other collaborative arrangements can "improve risk management and lower the costs among such banking organizations."[3] It is from our perspective as a collaborative platform launched in partnership with leading Financial Services organizations with the express purpose of driving greater standardization, reducing risks and lowering the costs associated with third-party risk management.

Firms can have a huge number of suppliers and outsourcing relationships, often spanning many jurisdictions. Identifying, managing and mitigating the risks relating to these third-party relationships is a daunting and potentially onerous task, particularly as these entities often have their own multi-jurisdictional third party and outsourcing arrangements. Such arrangements can lead to difficult to identify risks, including concentration risk if these third parties rely on a limited number of providers (particularly with IT and cloud providers). Manually trying to track and monitor outsourcing risk is virtually impossible given the complicated nature of many suppliers' own third-party relationships, the inconsistency of any manual inputs from firms and the need to effectively track changing situations. It is, therefore, important that firms set aside sufficient resources and adopt appropriate technology to make the process of identifying and managing such risks as effective and efficient as possible.

As has been shown by the success of the KY3P consortiums, the use of utilities accelerates standardization, improves risk management outcomes and reduces the overall cost of compliance for the banking industry. We welcome acknowledgement from the Agencies as we build the functionality and enhance the capabilities of KY3P to mutualize the cost of compliance across the industry.

The eradication of unnecessarily divergent approaches between banking organizations for third party risk management will also reduce the overall cost of regulation. Agencies and their staff will be able to focus on the implementation and configuration of standard platforms rather than having to understand processes from the ground up. We have seen gradual alignment of common practices across banking organizations but this

[2] Proposed Guidance at 38,186.
[3] Id.

needs to accelerate to improve efficiency and effectiveness for the industry.

Several features of KY3P and other utilities, consortiums and shared assessments support this reduction in the cost of compliance. These include, inter alia, the development of agreed approaches, common risk categories, standardized monitoring and common protocols.

IHS Markit KY3P believes that it is important for regulators to have a systemic view of outsourcing risks and, through KY3P, would also like to offer to support initiatives to create centralized repositories or registers of outsourcing arrangements. This could include sharing the lessons we have learned through our own solution's design and development as well as exploring the potential to enable organizations to use KY3P as one of the portals to up-load data into a central repository.

II. Request for Comment Questions

1. ***To what extent does the guidance provide sufficient utility, relevance, comprehensiveness, and clarity for banking organizations with different risk profiles and organizational structures? In what areas should the level of detail be increased or reduced? In particular, to what extent is the level of detail in the guidance's examples helpful for banking organizations as they design and evaluate their third-party risk-management practices?***

The Proposed Guidance provides a broadly comprehensive overview of the various facets of a "fit for purpose" third party risk management process. We outline below several areas where we feel that the level of detail could be increased. We would also support the inclusion of a more standardized control framework and expectations within that to support banking organizations in implementing a proportionate approach. Smaller organizations can struggle to identify what is proportionate and acceptable to regulators as they have reduced access to resources and subject matter expertise. The KY3P standard control framework has been designed in partnership with our banking and consulting design partners and is already being used broadly across the industry to drive standardization.

2. ***What other aspects of third-party relationships, if any, should the guidance consider?***

Banking organizations can improve their ability to respond, recover and learn from operational disruption through a program of testing and exercising. We believe that this is particularly important in relation to testing and exercising the services provided by third parties. The guidance should include reference to the benefits of an independent organization / industry utility like KY3P implementing a testing and exercising regime to support the individual banking organizations and the wider financial system where third party provided services could either fail or become significantly disrupted.

3. ***In what ways, if any, could the proposed description of third-party relationships be clearer?***

To help banking organizations better identify and define their third party populations, the Proposed Guidance could be more specific in the following ways:

- A third-party relationship should involve the receipt of goods for services by the banking organization. Recommend incorporating this concept into the definition.
- The use of 'or otherwise' should be removed from the definition. This could be open ended and make it difficult for originations to precisely define their vendor population
- The Proposed Guidance could clarify on what is meant by "on-going relationship." Does this exclude one-time engagements with a third party?

4. ***To what extent does the discussion of "business arrangement" in the proposed guidance provide sufficient clarity to permit banking organizations to identify those arrangements for which the guidance is appropriate? What change or additional clarification, if any, would be helpful?***

The Proposed Guidance seems to suggest that a business arrangement is any interaction with a third party other than with a customer. It would be helpful if this was clarified, and any other exceptions confirmed, e.g., how would charities, speakers, directors be treated?

5. ***What changes or additional clarification, if any, would be helpful regarding the risks associated with engaging with foreign based third parties?***

Third-party providers, like the financial firms they service, often operate across many jurisdictions and competing, duplicative or incompatible standards between jurisdictions can be particularly problematic. Third-party providers, such as IHS Markit, are committed to help their clients meet their regulatory requirements and to work with their regulators and auditors. However, the Agencies should be cognizant that differing standards and the need to provide constant access to premises and systems for all clients, their regulators and their auditors would be completely impracticable and unworkable. This would quickly overwhelm providers.

The Agencies should be promoting a focus on consistency and proportionality in approaches, particularly to access and assurance. Working with our design partners and consortium members, KY3P has created and implemented a standardized control framework for the assessment of third parties. This KY3P framework incorporates regulatory requirements from multiple agencies and jurisdictions allowing organizations to assess third parties in a consistent way across multiple geographical locations.

Given that utilities can help to drive consistency across geographical locations, , pooled audits and other assurance processes should be used wherever possible. This would help manage the burden of these process, which we agree are necessary (and is something many regulated firms are already doing) and avoid passing increased

costs on to regulated entities or making services uneconomical for some jurisdictions.

6. ***How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?***

It is our experience that one of the biggest challenges banking organizations face when scaling their TPRM practices are associated with resourcing and expertise. Agencies could help by recognizing that industry solutions such and KY3P can play and part in addressing these constraints.

As per pervious answers, the KY3P standard control framework has been designed in partnership with our banking and consulting design partners and is already being used broadly across the industry to drive standardization. The use of common and consistent frameworks enables banking organizations to scale TPRM practices by improving efficiency, reducing process burden and delivering better risk management results. This is especially relevant to small and medium sized banking organizations that can access due-diligence reports and data through utilities that they would find challenging using their own in-house resources.
It is also important to note that industry solutions like KY3P are equally beneficial to the vendors that providing goods and services to the financial service industry.

7. ***In what ways, if any, could the proposed guidance be revised to better address challenges a banking organization may face in negotiating some third-party contracts?***

In our experience there remain challenges for banking organizations both in successfully including right to audit clauses in contracts and in exercising those rights in practice. The Agencies should continue to reinforce their expectation that these must be included in all contracts, and that in order for a firm to provide goods or services to a banking organization, these clauses are mandatory. For example, the phrase "the contract often establishes the…...right to audit, monitor performance…" could be strengthened, e.g., by making the expectation a requirement, subject to enumerated exceptions, e.g., when the risk of the third party is minimal.

The Proposed Guidance could also reflect the importance of the third party in enabling the banking organization to identify and manage the risk inherent in the use of material "fourth parties" by the third party. Contracts should include provisions for the third party to acknowledge its role and responsibility for the management of overall risk in the supply chain and the wider global financial system.

We would support the acknowledgement in the guidance of the utility and shared assessment approaches and their inclusion in the guidance on rights to audit. The guidance could clarify that right to audit provisions could be drafted to incorporate shared assessments or pooled audits.

8. ***In what ways could the proposed description of critical activities be***

clarified or improved?

Critical activities could be linked to the definitions of activities within other regulations such as the operational resilience sound practices. This would reduce the amount of time that banking organizations need to individually map requirements and develop their own views of what may or may not be critical.

In practice banking organizations do not have third party relationships that neatly fall on either side of a line that is deemed "critical". The guidance should include more information on how banking organizations might risk assess the various third parties and the services that they provide and enable the development of a tiering of third parties not just critical/non-critical. Further clarity is needed around the term 'Significant', which could be interpreted differently by banking organization. This would then support a range of treatments that extend from the highest levels of due diligence through a series of levels to the lightest touch monitoring for low risk third parties.

9. ***What additional information, if any, could the proposed guidance provide for banking organizations to consider when managing risks related to different types of business arrangements with third parties?***

The guidance should include reference to the consideration of Environmental, Social and Governance "ESG" factors that could be relevant to banking organizations' assessment and management of risk. Various studies have shown that a significant proportion of the ESG impact to a firm is brought by its supply chain. This is particularly true as it relates to carbon and greenhouse gas emissions, as quantified in scope 2 and 3 emissions metrics.[4]

In a similar way to how a banking organization would monitor the financial risk of third parties in its due diligence and ongoing monitoring the use of ratings, indicators and other information for the various components of ESG will improve the ability of the firm to manage third party risk.

The guidance should also include reference to the country/location risk brought to the banking organization through the physical location of third-party suppliers. The location of the facilities that provide services to the third party is an important risk factor that should be considered in monitoring and due diligence. Recent experience in the rapid changes in economic and market risk in certain countries has meant that banking organizations have needed to quickly understand the extent to which aspects of their and their clients' supply chain is delivered from that country either through their third or fourth parties.

10. ***What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?***

Our experience is that one of the most challenging aspects of third party risk

[4] See e.g., EPA Center for Corporate Climate Leadership, Scope 1 and Scope 2 Inventory Guidance https://www.epa.gov/climateleadership/scope-1-and-scope-2-inventory-guidance.

management for firms is related to cloud computing. It would be helpful to increase the level of granularity of the guidance by breaking down the nature of the cloud service e.g., Platform As a Service, Software As a Service. Additional guidance or clarification in this area would be helpful.

11. ***What additional information, if any, could the proposed guidance provide to banking organizations in managing the risk associated with third-party platforms that directly engage with end customers?***

    [no comments]

12. ***What risk management practices do banking organizations find most effective in managing business arrangements in which a third party engages in activities for which there are regulatory compliance requirements? How could the guidance further assist banking organizations in appropriately managing the compliance risks of these business arrangements?***

    [no comments]

13. ***In what ways, if any, could the discussion of shared due diligence in the proposed guidance provide better clarity to banking organizations regarding third-party due diligence activities?***

As covered in the introduction section of this response, IHS Markit came together with 16 leading financial services organizations and 2 of the big 4 consulting firms to design, build and launch a solution to drive improved TPRM risk management practices across the industry. Know Your Third Party (KY3P) and other industry solutions are focused on standardizing best practices for managing third-party risk and optimizing the processes by which financial institutions, including, in particular, banking organizations, assess and monitor inherent risk in engaging suppliers and entering into third-party relationships. KY3P is therefore a leading example of what the Proposed Guidance contemplates when it speaks of utilities and collaborative arrangements.

The Proposed Guidance, and FAQ No.12, acknowledge the existence of industry utilities such as KY3P and the consortiums that utilize the KY3P platform. To enable industry solutions such KY3P and consortiums to grow, the guidance could be more specific in acknowledging these are appropriate to use in support a firm's third party risk management process in addition stating that the use of pooled assessments the use of does not abrogate management responsibility it would be informative to clarify and confirm.

.

The use of common standards, such as those developed and used within KY3P helps reduce the cost of compliance for firms and the cost of regulatory oversight by regulators. Rather than understanding multiple different yet conceptually similar

approaches, common standards and utilities enable regulators to focus on understanding generic platforms and can focus efforts on their configuration and implementation, in a similar way to how financial accounting has evolved.

FAQ No. 14 could also acknowledge the concept of utility provided shared assessments in addition to the other forms noted.

14. ***In what ways, if any, could the proposed guidance further address due diligence options, including those that may be more cost effective? In what ways, if any, could the proposed guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations?***

As per the response to question 13, the use of industry utilities can help banking organizations improve efficiency of their TPRM programs through reduced duplication of effort, driving increased standardization and accelerating the execution of assessments.

It is also important to note that the cost of completing the due diligence process required by banking organizations can be greatly reduced for the Financial Services supply chain. These costs can represent a significant barrier to entry into the Financial Service industry for small / medium size firms, including those that are diverse.

We believe the increased use of industry solutions like KY3P can reduce the cost of compliance across the Financial Services industry and associated regulatory agencies and supply chain. Therefore, the guidance should be more specific in acknowledging these are appropriate to use in support a firm's third party risk management process.

15. ***How could the proposed guidance be enhanced to provide more clarity on conducting due diligence for subcontractor relationships? To what extent would changing the terms used in explaining matters involving subcontractors (for example, fourth parties) enhance the understandability and effectiveness of this proposed guidance? What other practices or principles regarding subcontractors should be addressed in the proposed guidance?***

In our experience working with banking organizations, fourth parties is one of the most challenging areas for due diligence and monitoring. We see firms unsure about how far to go in the chain and how to interpret criticality. Additional guidance would be helpful, including examples of situations where due diligence and monitoring of fourth parties would be expected.

16. ***What factors should a banking organization consider in determining the types of subcontracting it is comfortable accepting in a third-party relationship? What additional factors are relevant when the relationship involves a critical activity?***

We believe that the most important factor in the management of fourth parties is the

ability of a banking organization to be able to identify and risk assess the most critical fourth parties. This is made more challenging where there is limited cooperation from the relevant third or fourth party. It would be helpful for the guidance to acknowledge the role that third parties are expected to play in enhancing the visibility of risk from fourth parties.

17. ***What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?***

[no comments]

18. ***To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?***

We support the inclusion of the FAQs within the Proposed Guidance.

* *** *

Please do not hesitate to contact me at richard.blore@ihsmarkit.com if you have any questions. We would welcome the opportunity to assist the Agencies as they consider finalizing the Proposed Guidance.

Sincerely,

[redacted]

Richard Blore
Chief Executive Officer
KY3P