TruSight™

The New Industry Standard For Third-Party Risk

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

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

Chief Counsel's Office
Attention: Comment Processing
Docket ID OCC-2021-0011
Office of the Comptroller of the Currency
400 7th Street, SW
Suite 3E-218
Washington, DC 20219

October 6, 2021

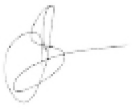
Dear colleagues:

As a partner to many financial institutions and their third parties, TruSight Solutions aims to bring the industry together under a common and transparent risk assessment framework. We are pleased to see the federal regulators also come together with this proposed common regulatory guidance. We believe this consistency will support shared expectations and reduce confusion.

In the attached document, we have responded to questions that are applicable to our industry-led utility. We are providing feedback based on our unique position, which unites many financial institutions and their third parties under one model. We believe clear regulatory guidance will allow institutions and third parties to manage risk in an effective yet efficient manner.

We appreciate your consideration and welcome continued dialogue.

Sincerely,



Jonathan Pressman

CEO
TruSight Solutions, LLC

Q1 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?

A1 We believe this guidance is a positive step towards unifying institutions and third parties. In support of that goal, we would like to see continued emphasis in the guidance and exam procedures on the level of validation required to validate third party controls. Some institutions rely heavily on questionnaires, or on SOC reports with limited scope. We would like to see greater clarity as to the appropriate evidence a third party should share to demonstrate the appropriate design and operation of their control environment. We believe industry-led utilities like TruSight support more consistent control validation without creating undue burden for smaller institutions. With regulatory support for models like TruSight, all institutions get access to more thorough assessments that meets the rigorous regulatory obligations Tier 1 Banks must comply with and third parties only need to complete one comprehensive assessment. However, in its current state, it may be unclear to institutions that validation of controls beyond just questionnaires and SOC reports is both prudent and available to all Banks using a consortium model.

Q7 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?

A7 The 2020 FAQ included in the proposed guidance highlights the value of utilities and alternative risk assessment models. However, many institutions have not considered such models in their contracts, and as such, struggle to take advantage of these types of options. We recommend that the regulators expand their guidance on contract terms for right to audit, specific to the incorporation/usage of a utility model, such that Institutions can take advantage of options best suited for the execution of their third-party risk management program.

Q8 In what ways could the proposed description of critical activities be clarified or improved?

A8 As referenced in our response to question 1, we have seen significant variations from Bank to Bank in the levels of due diligence performed. We believe the detail provided on critical activities will be very helpful in creating more consistency. However, the guidance should make it clear that while a smaller institution may have fewer critical activity providers, the rigor that institution places on its oversight of critical third parties should be commensurate with the critical risk posed. While the scale of the TPRM program will be significantly different from a small institution to a large institution, the evaluations of its most critical providers should be consistent as they pose a critical risk to the Bank.

Q13 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?

A13 The level of due diligence performed from institution to institution varies significantly. We believe all industry participants, regardless of their size should have access to a consistent level of the highest quality, validated data given the interconnectivity between financial institutions and their suppliers. Providing examples of the tests an institution might perform on its vendors or other guidance on validation methods will support greater consistency. The benefit of the utility / TruSight is that we perform the most comprehensive diligence on all suppliers and then allow the bank to curate the data applicable to their internal TPRM program. This flexibility reduces the need for third-party service providers to respond to multiple variations of assessments. We believe the industry needs one golden source of information that is available in a format easily consumable regardless of the size of the financial organization requesting access.

Additionally, TruSight continues to see varying levels of assessment depth with regards to applications, even within the G-SIFI organizations. Many organizations review applications individually while others review them as a group under the related System Development Life Cycle program. In group settings, when asked why each institution reviews to the level they do, the response is generally "based on regulatory feedback". This inconsistency has trickled down to non-G-SIFI institutions leading to vastly different assessment models and frustrations from third parties. We believe clarity around application assessment depth would continue to help unify the industry, provide due diligence clarification, and provide efficiency to the third-party community.

Q14 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?

Q14 The guidance correctly summarizes the general benefits of utility and consortium models. However, as there continues to be an increase in technology-backed utilities, there is a greater risk that Banks rely on a utility model that doesn't meet regulatory expectations. Most notably, we believe utilities may provide due diligence without the rigor expected by the guidance. The regulators should provide guidance as to how a Bank might evaluate the capabilities of utility service providers to facilitate due diligence, including the involvement of institutions in the utility, the degree to which the utility validates the third party's control environment, the qualifications of the utility to perform this due diligence, and the consistency of the due diligence from one third party to another. We believe the TruSight methodology is the most thorough assessment process addressing the regulatory obligations of all financial industry participants from small institutions to Tier 1 Banks. Our methodology ensures that a third party only needs to go through one comprehensive assessment.

Q18 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?

A18 We believe that the concepts in the FAQ should be incorporated into the guidance, as it materially clarifies the guidance itself.

However, we believe the regulators should consider FAQ 24:

"24. Can a bank rely on a third party's Service Organization Control (SOC) report, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 18 (SSAE 18)? (originally FAQ No. 14 from OCC Bulletin 2017-21)."

The FAQ cites the SSAE-18 or SOC1, which, per the AICPA website[1], is intended primarily to support financial reporting. The SOC2, by comparison, is listed as supporting controls over its system relevant to security, availability, processing integrity, confidentiality, or privacy. In our evaluations, the SOC2 is more commonly aligned to the controls requiring validation by our clients.

It is also worth noting that organizations may over rely on a service organization's SOC report without confirming which controls are validated in the report itself. We believe the guidance should encourage institutions to consider which controls are not covered in the SOC report for independent validation using another mechanism.

[1] https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html