THIRD PARTY RISK ASSOCIATION

P.O. Box 824
Ankeny, IA 50021
julie@tprassociation.org
www.tprassociation.org

October 11, 2021

Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System
Attention: Comment Processing, Docket No. OP-1752
Federal Reserve System
20th Street and Constitution Ave, NW
Washington, DC 20551

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, Docket ID OCC-2021-0011
Office of the Comptroller of the Currency
400 7th Street, SW., Suite 3E-218
Washington, DC 20219

VIA ELECTRONIC SUBMISSION: Federal eRulemaking Portal - http://www.regulations.gov

Re: Proposed Interagency Guidance on Third-Party Relationships: Risk Management
[Guidance: https://www.fdic.gov/news/press-releases/2021/pr21061a.pdf]

Dear Ann E. Misback, James P. Sheesley, and Chief Counsel's Office:

On behalf of the Third Party Risk Association (TPRA), its Members (to include those belonging to Financial Institutions) would like to submit the following comments for consideration on the "Proposed Interagency Guidance on Third-Party Relationships: Risk Management".

The TPRA is a 501c(6) not-for-profit professional organization that was created out of a necessity to build a community of like-minded third party risk professionals to allow for the sharing of best practices, exchanging of ideas, and influencing of an industry. Established in October of 2018, the organization has over 200 Practitioner & TPRM Service Provider members and a LinkedIn following of over 1,000 subscribers.

Activities in support of this purpose include, but are not limited to:

- Promoting the value that third party risk professionals and practitioners add to their organizations;
- Providing comprehensive professional, educational, and development opportunities, as well as standards and other professional practice guidance;
- Researching, disseminating, and promoting to practitioners and stakeholders knowledge concerning third party risk and its appropriate role in control, risk management, and governance;
- Educating practitioners and other relevant audiences on best practices in third party risk; and
- Bringing together third party risk professionals and practitioners from all countries to share information, experiences, tools, and techniques.

The comments are broken down into two sections:

I. Request for Comment – TPRA Member responses to questions posed by the Agencies.
II. Text of Proposed Guidance on Third-Party Relationships – TPRA Member comments and/or proposed edits to the proposed guidance.

If there are any questions regarding the following comments and/or proposed edits, please feel free to email Julie Gaiaschi, CEO of the TPRA at Julie@tprassociation.org.

Thank you for your time and attention. We very much appreciate the opportunity to review and comment on the interagency guidance.

Julie Gaiaschi, CISA, CISM
CEO of Third Party Risk Association

TPRA Member Comments

I. Request for Comment
   A. **General**:
      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?
         - **Member Comment:** Appreciate the regulators are issuing guidance across the agencies for consistency purposes. This will ensure consistency with the implementation and assessment process.
         - **Member Comment:** What are the minimum guidelines you are looking for banks to meet? From an evidence standpoint, what are we required to obtain at a minimum? Are there examples? While I appreciate that the guidance isn't too prescriptive, I want to make sure we can meet regulatory review requirements.

2. What other aspects of third-party relationships, if any, should the guidance consider?
    - **Member Comment**: Would like to better understand what organizations fall under the rigor of the scope of this guidance. Agree Financial Institutions are included but how about the non-financial institutions that are providing similar, financial services? Ex. Affiliated organizations – Should they need to meet these guidelines?

B. **Scope**:

3. In what ways, if any, could the proposed description of third-party relationships be clearer? **NO COMMENT.**
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?
    - **Member Comment**: I appreciate the notation of a "business arrangement" as there is risk with these arrangements; yet, some organizations scope these out of their program assessments. One example of a business arrangement could be a relationship with a university where you provide them with confidential data for research purposes and in return, your organization receives reports from the research. There may or may not be a contract in place and there may or may not be payments made. Yet, this type of relationship causes risk, especially if the university does not have strong information security controls in place. Therefore, they should still be evaluated. Another example may be a professional association where members of the organization is purchasing conference registrations. It may be beneficial to add some examples of what would constitute a "business arrangement". Agree that leaving the scope up to the banks for business arrangements is beneficial as long as regulators agree that if a bank thinks through business arrangements and documents why one may be out of scope, then that would pass an assessment.
5. What changes or additional clarification, if any, would be helpful regarding the risks associated with engaging with foreign-based third parties? **NO COMMENT.**

C. **Tailored Approach to Third-Party Risk Management**:

6. How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?
    - **Member comment:** I do not see mention of the "risk appetite" of the bank being taken into consideration. Some banks may require stronger controls to be put in place commensurate with the bank's risk appetite (i.e., the risk the bank is/is not willing to accept). In addition, a risk-based approach would also consider the inherent and residual risk of a third party. They would first be evaluated based on inherent risk. The continuous monitoring activities of a third party would then be based on the residual risk of a third party.

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?
    - **Member Comment:** Would be beneficial to note certain aspects of the inherent risk rating activities should be taken into considerations when negotiating the contract (e.g., if there is an increased risk due to the level of data they will have access to, then a separate clause around the minimum information security requirements should be added). Another example is if the third party will not provide a certain level of information, then additional penalty clauses should be put in place should an incident or other negative activity impacting the organization be realized.
8. In what ways could the proposed description of critical activities be clarified or improved? **NO COMMENT.**

D. **Third-Party Relationships**:

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?
    - **Member Comment**: Appreciate that the guidance isn't too specific on what constitutes a third party relationship as it allows for the flexibility for banks to determine the scope for their TPRM programs.
    - **Member Comment**: For organizations that will not provide information or evidence to complete assessments efficiently, it would be helpful to have guidance around next steps and/or additional contracting efforts needed.
10. What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?
    - **Member Comment**: For the smaller banks (not sure who would fit in that category), it would be beneficial to mention continuous maturity activities to ensure if a bank cannot comply with certain aspects of the guidance, that they at least have a plan in place the regulators recognize.
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?
    - **Member Comment**: Would like clarity around what organizations you are referencing. Would it include organizations that provide mailing and/or billing services where banks send customer data to them for processing?
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?
    - **Member Comment**: They could ask if the third party has regulatory requirements they need to adhere to and if so, do they have a regulatory compliance program in place.

E. **Due Diligence and Collaborative Arrangements**:

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?
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?
    - **Member Comment:** What are the minimum guidelines you are looking for banks to meet? From an evidence standpoint, what are we required to obtain at a minimum? Are there examples? While I appreciate that the guidance isn't too prescriptive, I want to make sure we can meet regulatory review requirements.
    - **Member Comment:** Could we obtain additional information on what's required from an accuracy standpoint? Would you like to see information on the source of the data and how accuracy was validated? Is there a time period for the evidence? E.g., information was collected in 2019, is it still valid for 2021? This is specifically important when you use a risk-based approach that takes into account the residual risk of a vendor and maybe you don't look at a vendor every year due to a low or moderate residual risk.

F. Subcontractors:

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?
    - **Member Comment:** For the Reliance on Subcontractors section, request you to add this guidance for "material" subcontractors and then define "material". A material subcontractor could be any fourth party that participates in and/or supports a substantial part of the product/service being provided to the bank. If banks evaluate the volume of all subcontracted activities, then that may end up being the entire third party portfolio for that vendor organization.
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? **NO COMMENT.**

G. **Information Security:**

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 COMMENT.**

H. OCC's 2020 FAQs

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?
    - **Member Comment**: An FAQ would add value to the document as it clarifies broader statements made within the guidance and also provides examples. Feel you could either keep the FAQ as an amendment at the end of the guidance or incorporate the FAQs after each pertinent section it relates to.

I. Paperwork Reduction Act

19. The agencies request comment on the conclusion that the proposed guidance does not create a new or revise an existing information collections.
    - **Member Comment**: Cannot confirm this statement as it would require review of all new or revised and existing information collections. Will look to the agencies to make this determination.

II. Text of Proposed Guidance on Third-Party Relationships

A. Summary
    - **Member Comment**: Request you to input the definition of a "Business Arrangement" in the first paragraph of the summary as you jump from third-party relationship to business arrangement without noting the nuance between the two.
    - **Member Comment**: Request you to provide clarity around the noted statement within the second paragraph of the *Summary* section. "A banking organization's use of third parties does not diminish the respective responsibilities of its board of directors to provide oversight of senior management to perform the activity in a safe and sound manner and in compliance with applicable laws and regulations, including those related to consumer protection." What activities are you noting that senior management performs? Is this in relation to third party risk management?

B. Background
    - **Member Comment**: Request you to consider the edits in red for the noted statement. "It is therefore important for a banking organization to identify, assess, monitor, and ~~control~~ address the risks associated with the use of third parties and the criticality of services being provided." It is unfair to ask for banks to "control risks associated with the use of a third party".

C. Risk Management

- **Member Comment**: Request you to insert a sentence regarding the "inherent risk" of a third party. Banking organizations don't just engage in more comprehensive and rigorous oversight and management of relationships that support "critical activities", but also perform more rigorous oversight for those relationships with high inherent risk. Yes critical activities could be related to those third parties with high inherent risk, but there are also third parties that have a substantial amount of confidential data that do not support a bank's critical activities.

1. Planning – **NO COMMENT.**
2. Due Diligence and Third-Party Selection
    - **Member Comment:** Sections within the *Due Diligence and Third Party Selection* chapter seems to be very prescriptive. Are these suggested due diligence activities or will you be evaluating banks on the implementation of these activities? E.g., "Consider reviewing the third party's service philosophies, quality initiatives, efficiency improvements, and employment policies and practices". While it may be clear how organizations review efficiency improvements and employment policies and practices, it is not clear how they assess service philosophies or quality initiatives. Suggest you to add less definitive wording such as "suggest reviewing" instead of "review". Or, if it is the intent that banks implement all of the guidance, suggest you to add examples of how you will evaluate each section when performing an assessment to ensure the bank is operating in compliance with these guidelines.
    - **Member Comment:** Some guidance noted seems to not have an actionable event tied to it should the third party fail. E.g., Within the *Legal and Regulatory Compliance* section, there is a statement that notes "Determine whether the third party has the necessary licenses to operate…". If a TPRM assessment shows the third party does not have a necessary license operate, what next? Should it be on the banks to report the organization? What if they accept the risk?
    - **Member Comment:** Some of the due diligence requirements within the Planning chapter may not be applicable for the level of inherent risk a third party poses to the organization. Suggest you to add language that discusses due diligence should be completed based on inherent risk during the pre-contract phase and residual risk during the post contract phase. It should not be the expectation that the banks evaluate "Business Experience" for each organization (such as window washers).
    - **Member Comment:** I appreciate the inclusion of assessing the "results of vulnerability and penetration tests" within the *Information Security* section as third parties often refuse to provide such evidence as they note it is not "industry standard" when in fact, it is regularly requested.

- **Member Comment:** Within the *Operational Resilience* section, it notes "disruption from any hazard" within the first sentence and also has a foot note. Unfortunately, the foot note does not line up with the language in the sentence as it notes "disruptive event". Suggest you to change "disruption from any hazard" to "disruptive event" to ensure consistency.
- **Member Comment:** Request you to add an additional form of review to the *Operational Resilience* section in the form of a datacenter walkthrough. This will ensure third parties understand that datacenter walkthroughs are industry best practice and an expectation.
- **Member Comment:** For the Reliance on Subcontractors section, request you to add this guidance for "material" subcontractors and then define "material". A material subcontractor could be any fourth party that participates in and/or supports a substantial part of the product/service being provided to the bank. If banks evaluate the volume of all subcontracted activities, then that may end up being the entire third party portfolio for that vendor organization.

3. Contract Negotiation
    - **Member Comment**: Please consider adding/removing language in red to the following sentence: "While third parties may initially offer a standard contract, banks may seek to request additional contract provisions or addendums ~~upon request~~ to address specific third party risk."
    - **Member Comment**: In response to the pandemic, please consider adding a bullet under *Responsibilities for Providing, Receiving, and Retaining Information* that suggests enhancing the Force Majeure clause to include more specific language such as "Pandemic/epidemic, Government order, law, or actions, National or regional disaster or emergency, and Material or Equipment shortages" in lieu of general language such as "act of God" or "other events beyond the reasonable control of a party".
    - **Member Comment**: Please consider adding a bullet under *Responsibilities for Providing, Receiving, and Retaining Information* that suggests adding a contract clause related to responding to questionnaires, surveys, and assessments to ensure the third party is meeting TPRM program requirements. This should be separate from the "Right to Audit" clause as it is not a formal audit and should be attainable multiple times throughout the year (not just once).
    - **Member Comment**: Consider adding a bullet for a clause related to the transfer of data across international borders and to ensure in compliance with local laws and regulations regarding the transfer and protection of said data.

4. Oversight and Accountability
    - **Member Comment**: Consider noting either in Board or Management responsibilities the acceptance of risk process to ensure high risks are accepted by an executive of the organization with oversight of the board to ensure transparency and agreement of the accepted risk. Also note risks should not be accepted for an indefinite period of time.
5. Ongoing Monitoring – **NO COMMENT.**
6. Termination
    - **Member Comment**: Request you to add to the list of termination reasons "the degradation of service and/or controls".
    - **Member Comment**: Request you to add a sentence regarding the creation of an exit plan during the pre-contract process for critical activities to ensure continuation of services should a disruption occur that results in the termination of the relationship.

D. Supervisory Review of Third Parties
    - **Member Comment**: The bullets related to what examiners typically consider when reviewing third party risk management is too broad. Suggest you to add how an examiner would approach an assessment related to this specific guidance and what evidence would be required to satisfy the examination.