1
October 18, 2021

Via Federal eRulemaking Portal – https://regulations.gov

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

Mr. James P. Sheesley , Assistant Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429

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

RE: Proposed Interagency Guidance on Third-Party Relationships: Risk Management; Docket No. OP-1752 (Board), FDIC RIN 3064-ZA026 (FDIC), Docket ID OCC-2021-0011 (OCC)

Ladies and Gentlemen:

Shared Assessments is pleased to respond to the July 13, 2021, request for comment on the third party relationships 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).

Shared Assessments is a global membership organization dedicated to developing the best practices, education, and tools to drive third party risk assurance. We are creators of the industry standard third party risk toolkit, used by over 15,000 organizations worldwide. Although founded in the banking industry, Shared Assessments now represents a variety of voices from a wide coss section of industries. All of our members believe in the foundational principle of third party Risk management (TPRM): that an organization can outsource activities, but it can never outsource the accountability for the services it provides.

Shared Assessments applauds the agencies on their decision to collaborate on updated, unified guidance for managing third party relationships. Consolidated guidance for the U.S. financial sector is long overdue, and the agencies' consolidation of regulation will be of great benefit to the industry. We further appreciate the opportunity to share our members' perspectives on specific issues that are important to consider before finalizing the interagency guidance.

The Current State of the Industry

Shared Assessments believes that key elements underlying existing federal third party risk management guidance continue to be appropriate:

- An emphasis on risk management practices throughout all phases of the third party relationship lifecycle;
- A recognition of heightened due diligence responsibilities when an organization outsources critical activities; and
- A strong focus on board and management oversight responsibilities in third party risk management.

In fact, sound regulatory guidance has contributed to an environment in which many financial institutions (FIs) have well-developed policies, procedures and programs for effectively managing third party risk. Five cycles of Shared Assessments research on the maturity of third party risk management practices across all industries suggests an environment in which about 40% of third party risk management programs are at or above full maturity; 32% of programs have either no or only ad hoc TPRM activities; and 28% have programs that are defined and operating, but typically are incomplete. Financial institutions are in the middle of the maturity pack in the most recent survey but led other sectors at the time of the first survey in 2014.

Today's third party operating environment is changing radically. Financial services companies, both big and small, operate as "extended enterprises" where lines easily blur between outsourcers and the increasingly complex outsourcing chains that supply and support them. The past few years have seen an acceleration of this trend, helped along by the pandemic, which has sped mass digitization to minimize person-to-person contact.

Mass digitization has changed third party risk management, with far more information being delivered to outsourcers in real time (or near real time) in digital formats that FIs must integrate with their existing work streams. Another important trend is the substitution of virtual (or remote) assessments for some on-site third party due diligence. Virtual assessments are not new, but the pandemic has increased outsource adoption rates. The combination of significantly improved economic efficiency and superior due diligence capabilities will likely lead to continued remote assessment growth.

At the same time that the scope of business relationships between FIs and their third parties has expanded, FIs—and larger banks in particular—have expanded their global reach. Many third parties with whom FIs have contracted have global operations. Both FIs and their suppliers operate in more jurisdictions than ever before, a trend that shows few signs of slowing and sometimes complicates regulatory compliance.

Indeed, banks' use of third parties, the third party risk environment and the tools FIs have at their disposal to better manage third party risks have changed significantly since the current guidance language was drafted in 2013. The recommendations below are made in the context of those changes and the feedback from Shared Assessments program members.

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?**

Bank regulators in the United States have issued principles-based third party risk management guidance, and in the past that guidance has sufficed both within and beyond U.S. borders. Third party risk management guidance from regulators abroad has evolved, however, and today is often far more prescriptive than in the U.S. Examples can be found in recent third party guidance from the Bank of England's Prudential Regulatory Authority (PRA), the European Banking Authority (EBA), and the Monetary Authority of Singapore (MAS). All three of these regulators have promulgated robust guidelines on outsourcing arrangements for FIs operating under their jurisdiction.

That same trend of increasingly prescriptive regulations has emerged in other areas that are central to third party risk management. Privacy regulations such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) are examples of how regulations have become ever more scrupulous, especially compared to anything financial services companies might have imagined when the OCC 2013 TPRM guidance was fashioned. Proposed regulations such as the EU's Digital Operational Resilience Act (DORA) will intersect with third party risk management guidance in many places. Indeed, no matter where a bank is located, it is increasingly subjected to regulations that are not of local origin.

Increasingly large regulatory guidance gaps between principle-based regimes and those that are building more precise structures cannot be ignored, and regulators should take more aggressive steps to close them.

In certain areas, guidance that at one time was reasonably clear no longer fits today's risk and risk management environment. Terms such as "ongoing monitoring" are not sufficiently precise at a time when near real-time monitoring has become critical (see question 2 for more detail on this point).

The structure of the United States' banking system is unlike any other. With about 4,500 FDIC-insured institutions (as of 2019—down from more than 8,000 in the year 2000) and more than 6,000 credit unions (up slightly in recent years), the size and complexity of individual FI operations is anything but uniform, certainly eschewing any "one size fits all approach" to regulation. Tremendous variations in the size and complexity of FIs have made it difficult for regulators to issue even high-level, principle-based, third party risk management guidance that conforms with the realities on the ground.

Overarching, basic minimum third party risk management requirements should be part of any revised guidance, as they are, largely, today. However, guidance could be more specific in certain areas to be truly useful and relevant, as this letter will show.

Key elements of TPRM governance, such as board oversight and approval requirements, are relevant no matter the institutional size. Expectations such as regular board-sponsored, arm's-length assessments of third party risk management programs effectively set the oversight tone.

Although the proposed guidance does not specifically reference Environmental, Social, and Governance (ESG) considerations, Shared Assessments believes that ESG should become a priority for the agencies. FIs, already under pressure from investment firms to escalate their ESG commitments, are also finding

themselves under attack from those who question the sincerity of their commitments. ESG, especially in relation to climate, is emerging as a regulatory focus point in the United States and is well established elsewhere.

Of particular interest is the reality that third party ESG due diligence is likely to be especially challenging, even for larger firms. Emerging evidence suggests that collaboration will be especially important to achieving truly useful ESG third party due diligence. As such, this area should receive more regulatory attention. Regulators should make clear that FIs will be faced with ESG compliance responsibilities in the future (from financial services regulators and others), and that they should begin examining their ESG risk frameworks now. Finally, the guidance should address the impact of scope 3 emissions[i], that is, emissions that are the result of activities from sources not owned or controlled by the outsourcer, but still result from its supply chain.

Summary of Recommendations:

- Updated guidance and regulations should take more aggressive steps to close TPRM deltas across international jurisdictions, especially in the area of principles-based guidance in the United States versus more prescriptive language more common elsewhere (see also questions 2, 17).
- Updated guidance should focus on sharpening language to better fit the realities of today's third party risk management environment and better reflect today's due diligence approaches (see question 2).
- Revised guidance should specifically address ESG-related issues. One particularly important example is scope 3 emissions reporting, where industry could benefit from a better understanding of due diligence expectations in complex third party outsourcing chains.

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

An approach that more explicitly tailors third party guidance to general categories of operational complexity may have merit. For example, small retail FIs that completely outsource their banking platforms do not have fewer third party risk obligations, but guidance specifically honed for those environments may be more effective. Indeed, more specific guidance in certain areas might make regulatory perspectives more useful and relevant. New regulations should consider referring more explicitly to other current regulatory output that is clearly relevant to third party risk management; for example, the recently released FFIEC Information Technology Examination Handbook "Architecture, Infrastructure, and Operations" (June 2021). Much of that material constitutes de facto guidance.

Different monitoring intervals are appropriate when dealing with an increasingly divergent set of third party risks. As the cybersecurity environment has evolved, regulatory use of the term "ongoing monitoring" has become less meaningful. Some regulators, such as the New York State Department of Financial Services, have used the term "continuous monitoring" when discussing internet-specific due diligence requirements. The term "continuous," whether or not it is defined precisely, conveys the need for near real-time (or at least extremely frequent) monitoring of controls when third parties touch sensitive customer and FI information.

Regulators should consider the benefits of more descriptive monitoring intervals when discussing due diligence techniques most useful for mitigating specific types of risks common in third party environments (for example: financial viability, cyber hygiene, and concentration risk).

The risks in today's world are intermingled and expanding at an alarming rate. Not only have the quantity of risks that organizations must monitor increased greatly, but also the *types* of risks that organizations face have evolved quickly.

New guidance should stress the importance of improved horizon scanning (a stepwise process that should be coordinated with the analysis and response to information gained through observation) and other foresight methods. During the past eighteen months FI's have seen a parade of casdcading risks, a succession of risks in which the impact of one exposure may magnify the impact of other, often considered independent, hazards. Few organizations were prepared for the type of cascading risks that have emerged from simultaneous calamitous events, such as the COVID-19 pandemic, wildfires, and a range of other environmental crises. It is important that FIs and regulators alike understand and address the potential impact of such events and their effects on FIs and outsourcing chains.

Updated guidance would benefit from an increased focus on mitigating risks from a geographically-dispersed set of third party providers supporting a single service. Specifically, there are two types of this geographic dispersion on which to focus:

1. Dispersion of contractors geographically, especially outside of the United States; and
2. Dispersion of workforces (remote working employees/work from anywhere). An organization's ability to assure a secure dispersed workforce varies significantly by geography, and especially in countries with emerging economies. Regulators should stress the importance of understanding underlying infrastructure (electrical, water, transportation, etc.) when outsourcing outside of the United States.

Regulators around the world have focused on concentration risk not just within FIs but within the financial services sector more generally. That focus has resulted in sharply increased third party inventory (register) requirements (EBA, MAS, and PRA). The PRA's most recent guidance (March 2021) stated the agency's intent to explore the creation of an online portal to track, in real time, FI third party inventories across the financial services sector.

Two factors in particular have heightened concentration risk concerns:

1. The rapid expansion of cloud services, an industry dominated by a few large companies.
2. The rapid evolution of complex outsourcing chains, which sometimes make it difficult for FIs to be aware of what organizations are providing services on their behalf.

U.S. regulators should pay careful attention to rapidly changing concentration risk in any new guidance, and, in particular, the frequency with which regulators might require a near real time understanding of sector-wide concentration risk.

In addition, although third parties have an obligation to understand what compliance requirements their FI customers must meet, SA member experience suggests that many third parties have not communicated that understanding throughout their organizations. Rather, members have often

reported pushback from third parties for actions FIs have taken while fulfilling their regulatory compliance obligations.

Regulators have an obligation to help financial institutions better inform third parties about required compliance documentation. Shared Assessments believes that regulator outreach, including written materials that might be shared internally within third parties, could be extremely helpful.

Summary of Recommendations:

- Regulators should consider the benefits of more descriptive monitoring intervals.
- New guidance should stress the importance of improved horizon scanning and other foresight methods.
- Updated guidance would benefit from an increased focus on mitigating risks from a geographically-dispersed set of third party providers supporting a single service.
- U.S. regulators should pay careful attention to rapidly changing concentration risk (both at a firm and sector level) in any new guidance.
- Regulators have an obligation to help financial institutions better inform third parties about required compliance documentation.

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

The proposed guidance defines a third party relationship as "any business arrangement between a banking organization and another entity, by contract or otherwise." Further,

> *A third party relationship may exist despite a lack of a contract or remuneration. Third party relationships can include relationships with entities such as vendors, financial technology (fintech), companies, affiliates, and the banking organization's holding company. While a determination of whether a banking organization's relationship constitutes a business arrangement may vary depending on the facts and circumstances, third party business arrangements generally exclude a bank's customer relationships.*[ii]

OCC Bulletin 2013-29 has a substantially similar definition and adds further clarification that "[n]either a written contract nor a monetary exchange is necessary to establish a business arrangement; all that is necessary is an agreement between the bank and the third party."[iii] In other words, when in doubt, FIs should normally assume a business relationship exists with a third party.

Shared Assessments believes any definition of a third party relationship must be sufficiently expansive to encompass any third party that may create a more-than-incidental risk to an FI, and Shared Assessments believes that the proposed guidance is sufficient in this regard.

In addition, beyond merely defining these relationships, there should also be more discussion on the types of risks associated with various types of third parties. Specifically, there could be more focus on:

- Risks related to contracting with third parties outside of the United States;
- Risks of regulated vs. unregulated parties due to country of origin; and
- Logistical challenges for on-site control assessments and general third party oversight could be addressed, especially in the context of COVID and the additional logistical challenges it has brought.

Summary of Recommendations:

- Shared Assessments believes that language in the current guidance describing third party relationships is sufficient.
- Updated guidance could also focus on the types of risks associated with various categories of third parties.

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?

As noted above, the proposed guidance defines a third party relationship as "any business arrangement between a banking organization and another entity, by contract or otherwise." Current guidance clearly stipulates that no contract is required for a business arrangement to be classified as a third party relationship.

The guidance also defines the types of entities that are considered third parties for the purposes of regulation:

> *Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where a banking organization has an ongoing relationship or may have responsibility for the associated records. Affiliate relationships are also subject to sections 23A and 23B of the Federal Reserve Act (12 U.S.C. 371c and 12 U.S.C. 371c-1) as implemented in Regulation W (12 CFR Part 223).*[iv]

The language states plainly that "third parties" includes all affiliates and subsidiaries of a financial institution.[v]

Summary of Recommendations:

- The current guidance is sufficient to provide clarity to financial institutions to enable them to identify the arrangements for which the guidance is appropriate.
- Provide additional nuanced guidance on outsourcing to wholly-owned entities such as a bank services company supporting all affiliates.

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

The proposed guidance, along with OCC Bulletin 2002-16 on *Bank Use of Foreign-Based Third party Service Providers: Risk Management Guidance*, provides robust guidance on this topic. However, international regulations, both explicitly TPRM focused and not, are changing rapidly. Shared Assessments believes that additional guidance may be prudent on the level of legal and regulatory compliance requirements in a foreign jurisdiction where new and specific requirements have emerged. Many of those jurisdictions have increasingly stringent legal obligations for companies operating within

their borders, and U.S.-based companies may also be liable for meeting certain obligations by simply contracting with a foreign-based third party. The guidance should consider these and associated risks.

Conversely, additional guidance should be provided on foreign-based third parties operating in jurisdictions with weaker laws and regulations than in the United States. Operating in environments where lax laws have led to behaviors that would not be tolerated in the United States creates a clear need for incremental due diligence. In Bulletin 2002-16, the OCC has already noted the importance of compliance with all applicable U.S. laws and regulations along with those laws' intersection with foreign data privacy laws or regulatory requirements, and "how any possible conflicts can be managed."[vi]

Banks must be particularly mindful of regulations from the U.S. Treasury's Office of Foreign Assets Control (OFAC) and obligations under the Foreign Corrupt Practices Act (FCPA). These types of laws and regulations represent the kinds of compliance liability of which U.S. FIs must be aware when dealing in foreign jurisdictions with higher risk environments. Incremental due diligence may be necessary to ensure that FIs are operating in compliance with U.S. law within these jurisdictions.

Summary of Recommendations:

- Shared Assessments believes that additional guidance may be prudent on the risks of outsourcing to foreign jurisdictions where new restrictions have emerged.
- Guidance should identify where U.S.-based companies may be liable for meeting certain obligations by simply contracting to send personal identification to a foreign-based third party.
- Guidance and regulations should continue to highlight increased risks when banks operate in jurisdictions with relatively lax regulatory schemes.

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

With the right executive management support there are several keys to successfully scaling third party risk management programs. Organizations should seek tools and processes that accomplish two goals simultaneously: (1) improve TPRM efficiencies, freeing dollars for more effective and expanded third party risk management scope; and (2) increase the effectiveness of third party risk management through the use of new tools, automating previously manual internal processes, effectively utilizing continuous monitoring services, and harnessing the collective knowledge and experience of peer institutions through cooperative structures such as Shared Assessments.

Five cycles of Shared Assessments' third party risk management benchmark studies have shown a clear relationship between board involvement and understanding of third party security issues and third party risk management maturity (see chart below[vii]). The importance of strong support from the Board of Directors and the C-level team cannot be overstated, nor can it be overstated in regulatory guidance.

Some of that support has come as a function of the The Dodd-Frank Act, which required the creation of board level risk committees at larger banks to oversee risk management practices on an enterprise-wide basis. Those committees have proved their value; they allow for more focused board discussion and education and – perhaps most importantly – the time to address deeper operational risk issues that would not be

available with a less focused committee agenda.

Degree of board engagement with and understanding of vendor-related cybersecurity issues	High engagement and level of understanding by the board	Medium engagement and level of understanding by the board	Low engagement and level of understanding by the board
Fully functional and advanced VRM programs (Levels 4 and 5)	57%	37%	25%
Transitional VRM programs (Level 3)	25%	30%	24%
Programs with ad hoc or no VRM activities (Levels 0, 1 and 2)	18%	33%	51%

Board and senior executive support is critical to enable appropriately resourced TPRM infrastructure. For example, properly implemented Governance, Risk and Compliance (GRC) systems help standardize escalation and other third party risk management processes, provide a single source of organizational truth for everything from third party inventories to compliance records, and over time generate significant economies that come from automating previously manual processes and efficient process standardization. For all but the smallest FIs, scaling TPRM programs without the right set of tools is almost impossible.

Virtually all organizations would benefit from using collaborative third party risk assessments and other collaborative tools. Revised guidance should touch more on the use of such tools, their benefits, risks, and other considerations when using them.

Summary of Recommendations

- Updated guidance should highlight board of directors' oversight responsibilities and stress the importance of appropriately funding third party risk management staff, tools, and training.
- Restated guidance should focus on the utility of Governance, Risk, and Compliance (GRC) systems, without which scaling TPRM programs may not be possible.
- Revised guidance should discuss in greater detail the use of collaborative third party risk assessments and collaborative tools. Guidance should discuss the benefits, risks, and other considerations when using such tools.

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?

Many Shared Assessments members across all sectors report significant difficulties negotiating contracts with certain suppliers, such as Cloud Service Providers (CSPs). And smaller FIs, who often outsource their

technology infrastructure, often report difficulty when negotiating contracts with a wide range of suppliers.

Perhaps all but the largest FIs have faced significant pushback when seeking CSP due diligence contract rights, such as the right to onsite due diligence and a right to audit in certain instances, even though these items would be routine in most third party agreements. International regulators are increasingly addressing this issue (e.g., EBA, PRA) and have recognized that certain suppliers (including CSPs) have unique operating challenges that might prohibit inclusion of otherwise common due diligence rights. A workable solution in other jurisdictions has been for supervisors to mandate specific language and then recognize that in practice certain rights would be exercised only in extreme circumstances.

Some regulators have been very hesitant to eliminate onsite due diligence requirements from contracts. The EBA, for example, in its 2017 guidelines on outsourcing to CSPs, underscored the importance of an outsourcer's access and audit rights for its third parties, since the outsourcer retains the ultimate accountability for its outsourced functions.[viii]

Similarly, the PRA has also underscored the importance of retaining audit rights for CSPs in its March 2021 PS7/21 *Policy Statement on Outsourcing and Third Party Risk Management*, while also acknowledging the potential risk that certain types of onsite audits may create for a cloud service provider. However, the PRA nonetheless recommends that, even where an outsourcer and service provider could agree on an alternate method of achieving the risk assurance offered by onsite audits, any such alternative *must* ensure an equivalent level of assurance. In other words, the level of risk assurance offered by onsite audits remains vitally important today, and the rights to such audits must be contractually protected.

Shared Assessments believes that regulators should provide clear guidance on this matter and believes the approach the PRA and EBA have taken is workable in practice.

Summary of Recommendations:

- Revised guidance should stress the necessity for on-site due diligence language in virtually all outsourcer agreements. The level of risk assurance offered by onsite audits remains vitally important today, and the rights to such audits must be contractually protected.
- Recent PRA guidance and policy statements (*Supervisory Statement | SS2/21* and *Policy Statement | PS7/21*) strike the right balance between protecting sometimes sensitive third party process and the need to preserve outsourcer due diligence rights. U.S. regulators should carefully consider creating language that strikes that balance.

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

Defining critical services accurately is one of the most important prerequisites to an effective third party risk management process. The task has become more difficult with increasingly complex outsourcing chains and the concentration of risks in certain areas such as cloud services.

As noted in our response to question eight above, OCC Bulletin 2013-29 defines critical activities as those which:

- *could cause a banking organization to face significant risk if the third party fails to meet expectations*
- *could have significant customer impacts*
- *require significant investment in resources to implement the third party relationship and manage the risk*
- *could have a major impact on bank operations if the bank has to find an alternative third party or if the outsourced activity has to be brought in-house.*[ix]

Shared Assessments believes that the existing definition continues to be appropriate because it strikes the right balance between specificity and language that enables management at different FIs to apply custom interpretations that best fit a specific book of business and operating environment.

Revised guidance would benefit from more discussion about critical activities, with examples depicting how certain activities might be rated at different FIs, especially at smaller and mid-size institutions.

Summary of Recommendations:

- Shared Assessments believes that the existing definition of critical activities continues to be appropriate.
- Revised guidance would benefit from more discussion about critical activities in the context of small- and medium-sized institutions.

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?

Updated guidance might emphasize the importance of categorizing the types of services in a financial intuition's inventory of third parties. Broad categories of services, such as call centers, and other workforce outsourcing, legal/accounting, technology outsourcing, etc. allow outsourcers to develop a set of focused contractual and due diligence control templates which can be enhanced to fit specific third party relationships.

The New York State Department of Financial Services has categorized financial institutions, segregating them based on size, activities and how institutions are structured. Due diligence requirements are then tailored to those categorizations. This approach could be a better way of categorizing, rather than just focusing strictly on the size of an FI. Thus, guidance can potentially focus on the types of activities outsourced and the risk posed to the organization, to better determine and align the due diligence required.

In the guidance generally, and here too, regulators should recognize the category of small banks that outsource their technology infrastructure. Institutions that outsource their banking platform infrastructure could benefit from guidance specific to that situation. For example, the New York State Department of Financial Services' Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500) requires each covered entity to designate a chief information security officer to oversee and implement the organization's cybersecurity policy. Many smaller organizations may not have the resources to maintain a CISO full time internally, and thus must outsource the responsibility (specifically anticipated and allowed by NYS guidance)—an action that exposes the organization to potential conflict-

of-interest situations when the CISO is outsourced from the platform provider, whose technology may be the source of the risk.

Summary of Recommendations:

- Updated guidance should emphasize the importance of categorizing the types of services in a financial intuition's inventory of third parties, such as call centers, and other workforce outsourcing, legal and accounting, technology outsourcing, etc. Such categories allow outsourcers to develop a set of focused contractual and due diligence control templates which can be enhanced to fit specific third party relationships.
- New guidance should recognize the category of small banks that outsource their technology infrastructure and the set of unique challenges they often face.

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

Risks associated with rapidly evolving technologies is another area where revised guidance may be appropriate. The use of machine learning and artificial intelligence algorithms has mushroomed with sometimes headline-making consequences. FIs—in common with others—have been hit by Distributed Denial of Service (DDOS) attacks fueled by improperly secured IoT devices (at both FIs and third parties), and distributed ledger (blockchain) variants have been deployed at dizzying speed. Ransomware attacks on supply chains are in the headlines regularly. Worldwide attention to the NIST Post Quantum Cryptography (PQC) program is an indicator that, although not immediate, quantum computing, with its associated benefits and risks, is not far off.

Yet, it is not always clear how quickly FIs should be adopting new technologies and what new precautions need to be taken because of new technologies. Third party risk managers must understand where new technologies are being used in their supply chains and must do appropriate due diligence to know that the use of new technology does not create incremental risks for outsourcers. In addition, due diligence is becoming more and more difficult as outsourcing chain complexity has increased to the point where some FIs might not be aware of all the subcontractors working on their behalf.

Rather than guidance focusing on specific technologies, revised guidance should focus on steps FIs can take when evaluating technology use at third parties. Some involve asking simple questions. For example, does a third party have a complete inventory of its IoT devices (Shared Assessments research has shown that most organizations haven't catalogued even half their IoT devices)? Other steps include continuous monitoring of third party cyber hygiene and understanding how third parties monitor the cyber hygiene of entities to which they have outsourced activities. These ideas could be addressed broadly and perhaps with additional detail on certain specific technologies as issues emerge. Along these lines, the guidelines should address the inevitability that new technologies will continue to emerge and FIs must evolve their due diligence techniques so that they are effective as they do.

To protect the outsourcer, a third party risk manager must take certain steps regarding emerging technologies. Specifically, they must:

- Understand emerging technologies, how they operate, and how they will be used by the organization;

- Understand risks associated with their implementation and potential future uses;
- Understand which controls may be necessary to mitigate risk associated with the technological use and implementation; and
- Conduct proper due diligence to ensure that the use of the technology will not be detrimental to the outsourcer.

The outsourcer must ensure—on an ongoing basis—that its third party risk management staff is appropriately trained and supported to conduct due diligence given an increasingly sophisticated and rapidly evolving technology landscape.

The emergence of fintechs has been valuable in the development and delivery of new technologies, but it has become apparent that fintech startups have themselves created additional risks for the FIs they often seek to serve. Because these firms may be relatively new, they may not understand the regulatory environment in which FIs operate and the specific obligations FIs carry.

The OCC has already taken an important and commendable step towards addressing emerging technology risks with the establishment of its Office of Innovation. The OCC has made strides in fostering a risk management culture at the agency that can adapt to and embrace an evolving technological landscape as well as improving the agency's ability to provide appropriate guidance when FIs or third party fintechs approach it.

If federal regulatory agencies seek to deepen their involvement at the interface between new technology and the banking sector to the benefit of all, the agencies should consider the implementation of a regulatory sandbox which will yield significant benefits for FIs and technology companies alike. Most importantly, firms will have a test bed overseen by regulators who can provide valuable feedback on new services and products. Other regulators internationally have already adopted regulatory sandbox programs, and these efforts have allowed FIs under their jurisdiction to accelerate technological innovation while simultaneously minimizing the potential risks associated with putting new technologies in the field. In the U.K., the FCA's regulatory sandbox transitioned to an "always open" operating model in August, and in September, announced a new sustainability cohort designed to "provide support to innovators looking to develop and validate solutions in the area of ESG data and disclosure."

Regulators should strongly consider implementing a regulatory sandbox program in the U.S.

Summary of Recommendations:

- Revised guidance should focus on steps FIs can take when evaluating technology use at third parties.
- The guidelines should address the inevitability that new technologies will continue to emerge and FIs must evolve their due diligence techniques to remain effective.
- Updated guidance should discuss the importance of management efforts to ensure its third party risk program staff is appropriately trained and supported in an increasingly sophisticated technology landscape.
- Regulators should strongly consider implementing a regulatory sandbox program in the U.S.

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?

Whether a banking organization provides access to and use of their system to a third party, or a third party uses its own platform to obtain data on behalf of a customer, the guidance must speak to the technical, regulatory and governance aspects of direct customer interaction and use of associated data collected. Since the third party in certain of these scenarios acts as an agent of the banking organization, the same compliance requirements need to be extended to the third party engaged in the business arrangement. Compliance requirements may include, but are not limited to:

- Authentication and authorization
- Consumer protection
- Affiliation transparency
- Data collection and use
- Complaint and dispute handling
- Data breach reporting and disclosure

Aggregators are among the most common third party entities that directly engage with customers. Aggregators, with appropriate permissions, compile financial data from multiple sources to assemble a holistic view of an individual's financial status. Through automation and/or through individual analyses performed by trained agents, clients benefit from the holistic understanding that aggregated financial data can provide.

Screen scaping was once almost universally deployed by data aggregators. In essence, screen scraping enables third parties to operate as customers and to collect data with no action (and knowledge) on the part of the financial institution. Although the process has been slow, aggregators are reaching agreements to utilize Application Programming Interfaces (APIs), and, when they are used, FIs may have an obligation to ensure that customer data is managed in compliance with its own standards. Any proposed guidance should discourage the use of screen scraping in data aggregation and should encourage the use of APIs.

Guidance from the FFIEC *Information Technology Handbook—Architecture, Infrastructure, and Operations Booklet* should also be included (or referenced) in the proposed guidance, specifically the following section:

> *Management should monitor third party service providers as part of the entity's third party risk management program.* ***Reports from third party service providers should include effectiveness of security controls, performance metrics, resolved versus outstanding issues, and root causes of problems****. Management should monitor the third party service provider's ability to meet defined SLAs, compliance with identified action plans when they are not met, and remuneration of penalty fees when appropriate.* [emphasis added]

In addition, the next iteration of the proposed guidance should stress the use of monitoring techniques as outlined in the FFIEC IT Handbook AIO booklet, specifically Section VI.D.1 Monitoring and Reporting. Specifically, organizations should implement monitoring processes that demonstrate the effectiveness of established controls to senior management, with whom engagement is critical. Senior management

should provide input for the types of reports and metrics produced, and the reports "should be understandable and useful to them."[x] Senior management should also periodically meet with operations management to "assess the value of the monitoring and reporting and to identify any changes" that may be warranted.[xi]

Summary of Recommendations.

- Revised guidance should recommend the use of APIs to replace screen scraping in data aggregation.
- Revised guidance should incorporate or reference due diligence language from the June 2021 Information Technology Handbook (cited above).
- Revised guidance should note that senior management should periodically meet with operations management to assess the value of the current monitoring and reporting program and identify any warranted changes.

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?

Although third parties have an obligation to understand what compliance requirements their FI customers must meet, SA member experience suggests that many third parties have not diffused that understanding throughout their organizations. Members often report pushback from third parties for actions FIs have taken while fulfilling their regulatory compliance obligations. There is a necessity for educating third parties about required compliance documentation. Shared Assessments believes that regulator outreach, perhaps in the form of written materials that might be shared internally at third parties, could be extremely helpful.

The last two years have tested FI enterprise risk management (ERM) processes and systems, of which third party risk management is an essential part. Although ERM effectiveness is improving, third party risk management teams are often peripheral to existing ERM structures, with unfortunate consequences. Refreshed regulatory guidance should stress the importance of fully integrating third party risk management programs within ERM programs.

Summary of Recommendations:

- Enhance regulatory outreach to third parties to socialize outsourcer regulatory compliance and documentation obligations. Update outreach as required.
- Stress the importance of fully integrating third party risk management programs with Enterprise Risk Management (ERM) programs.

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?

Shared due diligence brings with it the promise of significant economies as multiple organizations leverage the discovery efforts conducted by a single firm or consortium. Fifteen plus years of Shared Assessments efforts has proven the utility of an approach where superior due diligence techniques are created by bringing together expert resources from a number of organizations and then sharing the output from assessments conducted based on those enhanced tool sets.

Shared due diligence can be an efficient and effective means of lowering TPRM costs and better utilizing scarce resources, while maintaining or improving the quality of due diligence. Shared due diligence may provide valuable data to FIs seeking to evaluate third parties, but utilizing shared due diligence (and associated external processes) does not relieve FIs of the responsibility of evaluating due diligence information, no matter the source. Discussion of collaboration should have a focus on the continuing responsibilities of the outsourcer, including what liability it may have should any collaborative reports prove inaccurate. Regulators should highlight the fact that collaborative activities do not decrease the level of due diligence required of the outsourcer.

Summary of Recommendations:

- Updated guidance should stress that shared due diligence can provide significant economies as multiple organizations leverage the discovery efforts conducted by a single firm or consortium.
- Updated guidance should note that shared due diligence tools can be superior to those created by a single organization because multiple entities, each with complementary experience, come together to fashion due diligence tools.
- Revised guidance should highlight that shared due diligence (and associated external processes) does not relieve FIs of the responsibility of evaluating the adequacy of due diligence information, no matter the source.

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 previously discussed, organizations can find benefits, such as enhanced efficiency and leveraging better and more timely due diligence data from using collaborative risk assessments, TPRM exchanges, and other collaborative tools. As such, guidance could elaborate on the utility of these techniques, their benefits, risks, and other considerations when using them.

Today's third party risk management environment is notable for an ever-expanding set of rich due diligence data from a growing array of sources. However, some organizations lack the ability to fully evaluate and integrate that new, often time sensitive, data into existing work streams. Updated guidance should stress management's responsibility to: (1) understand when such circumstances are present, and (2) take appropriate action to address those situations.

Often, outsourcers may find that additional TPRM skill sets are required in-house. Revised guidance should better speak to the need for outsourcers to regularly evaluate the competencies of existing third party risk management staff and should explicitly enourage management to ensure ongoing training of existing staff in a resource constrained environment. For example, third party risk management

certificate and certification programs, at Shared Assessments and elsewhere, are readily available to practitioners at different skill levels and can be an important aid to organizations seeking to build leverageable core competencies.

Revised guidance could better assist organizations in determining their responsibility to fill in the gaps when information from a utility, consortium, or other organization is not adequate to meet the outsourcer's due diligence requirements. As more and more information becomes available from sources outside of an outsourcer's own due diligence efforts, more attention should be placed on the outsourcer's ability to utilize that data effectively to yield a more complete picture of the risks a third party presents at any stage in the third party risk management lifecycle. Utilization may require investment in new technologies, and indeed ML and AI applications are being utilized to streamline efforts that might not have been possible without internal technology investment.

Revised guidance should also encourage the FI community generally to engage with standard setting organizations dedicated to advancing the practice of third party risk management. FI-centric organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Financial Services Sector Coordinating Council (FSISCC), and the Financial and Banking Information Infrastructure Committee (FBIIC) have played important roles - with robust industry input - in strengthening industry security.

Guidance could touch on whether there are different responsibilities for an FI receiving data from a monitoring technology as opposed to an FI that uncovers the information itself through its own assessments.

Summary of Recommendations:

- Revised guidance could better assist organizations in determining their responsibility to fill in the gaps when information from a utility, consortium, or other organization is not adequate to meet the outsourcer's due diligence requirements.
- Revised guidance should stress outsourcer responsibility to regularly evaluate the competencies of existing third party risk management staff and training programs.
- Revised guidance should speak to the consequences that result from an outsourcer's inability to integrate rich, often time sensitive, due diligence data into existing work streams and the steps managaement should take to address those situations.
- Revised guidance should encourage the FI community to engage with standard setting and risk management organizations dedicated to advancing the practice of third party risk management.

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?**

The terms used to describe subcontractors matter far less than providing enhanced guidance about the increasing complexity of supply chains. A November 2020 report issued by the Financial Stability Board

identified outsourcing chains with as many as 20 providers.[xii] That example is why banks and others are increasingly using the term "Nth party" to describe outsourcing chains which exceed 4th parties. Supply chains are becoming increasingly complex as more financial institutions and third parties outsource functions. An unfortunate characteristic of complex outsourcing chains is that it has become harder for banks to document the parties' controls when relationships go much beyond a 4th party. Revised guidance should recognize this reality.

Along with a rapid increase in the number of complex outsourcing chains comes divergence in due diligence guidance among international regulators. The Bank of England's Prudential Regulation Authority stated in its March 2021 Policy statement that it "does not expect firms to directly monitor fourth parties in all circumstances."[xiii] This statement is out of step with not only the positions taken by peer regulators around the world, but also some other of the PRA's own statements. The guidance also seems counterintuitive, since there are more techniques outsourcers can deploy, such as continuous monitoring, to meet the challenge. The proposed guidance should provide clarity on this issue and Federal regulators should work quickly to achieve cross-jurisdictional harmonization.

Any new guidance should address questions surrounding the level of controls an outsourcer is required to maintain over the outsourcing chain in its entirety. Outsourcers must be aware of what is happening in their supply chains, but the Financial Stability Board, in its *Regulatory and Supervisory Issues Relating to Outsourcing and Third party Relationships Discussion paper*, noted that:

> *…the longer and more complex a chain of service providers is, the more challenging it becomes for FIs and supervisory authorities to manage the relevant risks or even to identify all the different providers involved.*[xiv]

The paper then provides recommendations for helping FIs manage these risks, including contractually ensuring that they:

- have the right to limit, approve, or object to some forms of sub-contracting;
- be notified of material changes to sub-contractors; and
- have the opportunity to terminate arrangements in certain circumstances.[xv]

Furthermore, these contractual rights should "remain throughout the supply chain."

Updated guidance should also consider questions of how and when a supply chain's complexity creates too burdensome a risk for the FI to manage, and what other steps FIs can take to minimize risk for particularly complex supply chains.

Summary of Recommendations:

- Revised guidance should speak to the rapid evolution of complex outsourcing chains and the increased risk that comes with them.
- Updated guidance should provide clarity on the level of due diligence an outsourcer is required to maintain over the outsourcing chain in its entirety.
- Regulators should recognize that conflicting international guidance about 4th and Nth party due diligence has developed, and U.S. regulators should work quickly to achieve cross-jurisdictional harmonization.

Updated guidance should also consider questions of how and when a supply chain's complexity creates too burdensome a risk for an FI to manage, and what steps FIs can take to minimize risk for particularly complex supply chains.

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?

Subcontracting has become common today and will continue to grow especially in technology services. Banking organizations should focus on assurance and their ability to perform while maintaining the contractual right to exit contracts if a proposed subcontractor does not meet the outsourcer's requirements. Developing and implementing multi-layered assurance protocols to review the complete third party business arrangement, including subcontractors, is key to ascertain adequate operational and technical controls by all parties.

As mentioned in our response to question 15, any outsourcing organization must be aware of all subcontracting being used across its supply chain. Regulators should address questions and techniques for addressing visibility issues in complex supply chains. If an outsourcer cannot see (to conduct due diligence) the entirety of an outsourcing chain, is any associated risk sufficiently managed if the outsourcer has, theoretically, contractually assured sufficient security hygiene all the way down the chain? At what point does that situation create an unacceptable level of risk?

Guidance should continue to stress the importance of outsourcers having the ability to stipulate that a specific level of controls be in place as well as the option to terminate a contract if a vendor is not doing its job properly from a security hygiene perspective.

Cloud services is playing a more important subcontracting role in today's outsourcing environment. FIs should consider a "short list" of acceptable CSPs and should document and periodically reevaluate the criteria necessary for a provider to make the list.

When critical activities are outsourced, it is more important for banks to evaluate the resilience of the supply chain in its entirety. Future guidance could benefit from more discussion of critical services in the context of complex outsourcing chains. Guidance could address risks when a specific threshold on critical services is exceeded, and how an FI's size and resources relate to the risk calculation for these relationships.

As noted in our response to question 8, OCC Bulletin 2013-29 defines critical activities as those which:

- *could cause a banking organization to face significant risk if the third party fails to meet expectations.*
- *could have significant customer impacts.*
- *require significant investment in resources to implement the third party relationship and manage the risk.*
- *could have a major impact on bank operations if the bank has to find an alternative third party or if the outsourced activity has to be brought in-house.*[xvi]

As noted previously, Shared Assessments believes the definition of "critical" in a third party risk context strikes the right balance between specificity and language that enables management at different FIs to apply custom interpretations that best fit a specific book of business and operating environment.

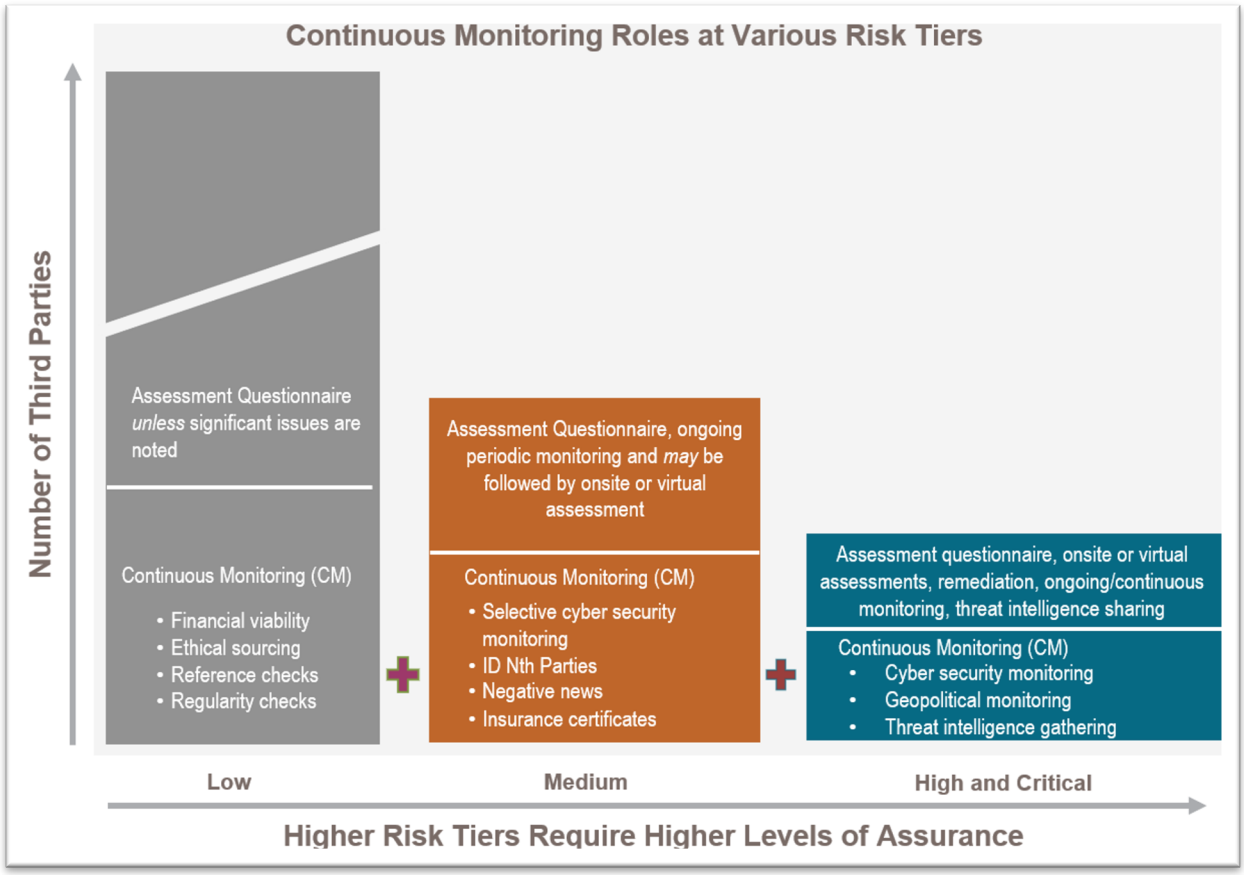
Finally, as discussed previously, U.S. regulators should pay careful attention to rapidly changing concentration risk in any new guidance, and in particular, the frequency with which regulators might require a near real time understanding of sector-wide concentration risk.

Summary of Recommendations:

- Updated guidance should better speak to questions and techniques for addressing vendor visibility issues in complex supply chains.
- Guidance should continue to stress the importance of outsourcers having the ability to stipulate that a specific level of 4th (or Nth) party controls be in place and the option to terminate a contract if a vendor is not meeting its obligations.
- U.S. regulators should pay careful attention to rapidly changing concentration risk in any new guidance, and in particular, the frequency with which regulators might require a near real time understanding of sector-wide concentration risk.

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?

Revised guidance should better reflect current practice. Risk assessment of third parties should begin during the RFP process. Outsourcers should request specific documentation (e.g., SOC reports) as part of an initial review and may utilize standardized questionnaires, such as the Shared Assessments SIG or an equivalent format, to gain an initial understanding of a third party's risk control hygiene. When outsourcing critical activities, outsourcers should consider conducting on site or remote (virtual) assessments and engage in continuous monitoring to review the security hygiene of RFP finalists. In fact, some form of continuous monitoring is often appropriate even when inherent risk levels are lower (see chart below).



Third party due diligence today has moved beyond point-in-time due diligence—the last ten years have seen the emergence of entire business sectors seeking to develop and share near real time cyber security data, as well as data reflecting a range of operational risks. Such risks include geolocations (of which there are many), financial, and others. Often this due diligence data goes beyond what almost any individual financial services company could collect and analyze on its own, and therefore brings significantly enhanced value to the third party risk management practice generally. Revised guidance should note the emergence and use of true value added risk management services and perhaps anticipate where more such services will be required, for example, to improve the quality of ESG due diligence.

Virtual (or remote) assessments have come to play a more material due diligence role during the pandemic and will continue to be useful because of their cost effectiveness. Virtual assessments have come to take many forms. Some third parties have structured periodic virtual open houses where firms can inspect internal processes and artifacts in secure environments. Others enable one on one “visits” from individual outsourcers and tailor such sessions to the needs of individual firms. Regulatory guidance should speak to the role of virtual assessments, their perceived limits (if any), and specific circumstances where they have the greatest utility.

Outsourcers can and should leverage collaborative tools when engaging third parties, but always with the understanding that the accountability for assuring the adequacy of the sum of all due diligence efforts is the responsibility of the outsourcing party and no one else. Therefore, outsourcers should always preserve their ability to conduct the level of due diligence appropriate to the engagement and the risks presented, and guidance should reflect that standard.

The FAQs, specifically questions 12, 13, and 15, do an appropriate job of addressing the balancing act between using collaborative due diligence on third parties and maintaining FIs' ownership over their risk responsibilities. Shared Assessments recommends integrating the content from these three FAQs into the final guidance.

Summary of Recommendations:

- Revised guidance should better reflect current practice and the importance of continuous monitoring.
- Guidance should note that some forms of due diligence bring the promise of data that goes beyond what almost any individual financial services company could collect and analyze on its own, and therefore brings significantly enhanced value to the third party risk management practice generally.
- Regulatory guidance should speak to the role of remote (or virtual) assessments, their perceived limits (if any), and specific circumstances where they have the greatest utility.
- Updated guidance should note the importance of preserving individual outsourcer due diligence rights even when an outsourcer participates in a collaborative assessment.
- Shared Assessments recommends integrating the substance of FAQ questions 12, 13, and 15 into updated guidance.

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?

Shared Assessments believes that current FAQs should be integrated with updated guidance. Integration would allow for better clarification of items reviewed in current FAQs and might help identify improvements to the guidance wording once FAQ observations are integrated with current language.

In place of FAQs posted in batches several years apart, regulators could consider a similar FAQ format with items posted online faster, in a rolling fashion. As circumstances warrant, when revised guidance is issued, those rolling FAQs could be integrated into the formal guidance document. A new FAQ format might include the ability for organizations to place comments and questions directly into the FAQ section.

FAQs, or an equivalent that interprets the body of the guidance, are both appropriate and helpful, but they should be specific to the last guidance iteration and should not introduce new measures. In other words, the purpose of additional rolling FAQs should be to provide further clarification on rules and guidance, and not to introduce fundamentally new guidance.

Summary of Recommendations:

- On a periodic basis, integrate FAQs into updated guidance to enhance the current language and context.
- Release new FAQs online on a rolling basis and allow organizations to place comments and questions directly into the FAQ online pages.
- FAQs should not introduce new guidance.

Shared Assessments appreciates this opportunity to share recommendations we believe are important to consider before finalizing any interagency guidance. We are always available to provide clarifications or addess questions about any of our comments

Yours Sincerely,

Catherine A. Allen
Founder, Chairman, and Interim CEO
Shared Assessments

---

[i] EPA Center for Corporate Climate Leadership. *Scope 3 Inventory Guidance.* https://www.epa.gov/climateleadership/scope-3-inventory-guidance

[ii]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). (2021, July 19). *Proposed Interagency Guidance on Third-Party Relationships: Risk Management.* https://www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third party-relationships-risk-management. Page 18.

[iii] OCC Bulletin 2013-29.

[iv] 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). (2021, July 19). *Proposed Interagency Guidance on Third-Party Relationships: Risk Management.* https://www.occ.gov/news-issuances/bulletins/2002/bulletin-2002-16.html.

[v] 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). (2021, July 19). *Proposed Interagency Guidance on Third-Party Relationships: Risk Management.* https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-74a.pdf. Page 18.

[vi] Office of the Comptroller of the Currency (OCC). (2002, May 15). *OCC Bulletin 2002-16 - Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance*. https://www.occ.gov/news-issuances/bulletins/2002/bulletin-2002-16.html.

[vii] Shared Assessments. (2019, April 8). *2019 Vendor Risk Management Benchmark Study: Running Hard to Stay in Place.* https://sharedassessments.org/studies/2019-vendor-risk-management-benchmark-study-running-hard-to-stay-in-place/

[viii]

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
4.3 Access and audit rights – Paragraphs 6 to 14 – Feasibility of full access/audit	A number of respondents considered the full rights to access and audit for outsourcing institutions infeasible in view of highly standardised services and contracts, the limited negotiation power of outsourcing institutions, the risk these rights pose to the cloud environments of other clients and the security risk and operational implications for the cloud service provider as a whole. Respondents also pointed out that the added value of physical facility access can be considered extremely low in modern-day technology environments, where data are physically and geographically dispersed across many systems, data centres and even countries.	The EBA notes the comments with regard to the feasibility of the full rights of access and audit and would like to reiterate that, although these rights should be contractually assured, they can be exercised in a risk-based manner. Since the outsourcing institution retains responsibility for the outsourced functions, it is vital for the institution to have the necessary access and audit rights to fulfil its obligations.	No changes made.

European Banking Authority. (2019, February 25). *EBA Guidelines on outsourcing arrangements*. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf. Page 46.

[ix] U.S. Office of the Comptroller of the Currency. (2013, October 30). *OCC Bulletin 2013-29 | Third party Relationships: Risk Management Guidance.*https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[x] Federal Financial Institutions Examination Council's (FFIEC). (2021, June 30). *FFIEC Information Technology Examination Handbook Architecture, Infrastructure, and Operations*. Page 84.

[xi] *Id.*

[xii] Financial Stability Board. (2020, November 9). *FSB consults on regulatory and supervisory issues relating to outsourcing and third-party relationships.* https://www.fsb.org/2020/11/fsb-consults-on-regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships/

[xiii] Prudential Regulation Authority. (2021, March 31). *Policy Statement | PS7/21 Outsourcing and third party risk management*. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2021/march/ps721.pdf?la=en&hash=6C70BEE48B89D7965D43894DB848FC41CD5EC6C0. Page 4.

[xiv] Financial Stability Board. (2020, November 9). *Regulatory and Supervisory Issues Relating to Outsourcing and Third party Relationships Discussion paper*. https://www.fsb.org/wp-content/uploads/P091120.pdf. Page 24.

[xv] *See Id.*

[xvi] U.S. Office of the Comptroller of the Currency. (2013, October 30). *OCC Bulletin 2013-29 | Third-Party Relationships: Risk Management Guidance.*https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.