Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

October 15, 2021

Via Electronic Mail

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

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

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

Re: Proposed Interagency Guidance on Third Party Relationships: Risk Management

Microsoft welcomes the decision of the Office of the Comptroller of the Currency ("OCC"), Board of Governors of the Federal Reserve System ("Board"), and the Federal Deposit Insurance Corporation ("FDIC") (together, the "Agencies") to consult on the *Proposed Interagency Guidance on Third Party Relationships: Risk Management* (the "Proposed Guidance").[1]

As the financial services industry continues to evolve and modernize, Microsoft considers it particularly important that regulation and supervision is responsive and adaptive to innovation. With this in mind, Microsoft supports the Agencies' approach to a risk-based framework for third-party risk management that reflects the principle of proportionality, where risk management expectations are commensurate with the level of risk and complexity of a third-party relationship. Microsoft also supports the Agencies' decision to maintain the technology-neutral approach of the existing supervisory guidance so that products, services, and processes can evolve and support innovation regardless of the changes in technology that enables them.

It is important such a framework provides for the flexibility and adaptability required to address rapidly changing innovation in this highly dynamic marketplace – allowing financial institutions to innovate responsibly, enhance the competitive fabric, and operate in a safe and sound manner.

[1] *Proposed Interagency Guidance on Third Party Relationships: Risk Management*, 86 Fed. Reg. 38,182 (July 19, 2021) (Docket No. OCC-2021-0011; OP-1752; RIN 3064-ZA26).

In the sections below, Microsoft offers substantive input on five key concepts in the Proposed Guidance: (I) Critical Activities; (II) Subcontractors; (III) Third Party Reports and Certifications; (IV) Contractual Provisions; and (V) Consistency and Harmonization.

I. Critical Activities

In Question 8, the Agencies requested comments on ways to clarify or improve the proposed description of "critical activities."

Microsoft agrees with the use of the concept of "critical activities" to help banking organizations scale their risk management practices, so that third-party relationships that support critical activities are subject to more comprehensive and rigorous oversight and management than those that support non-critical activities. Approaching risk management of "critical activities" in this way is consistent with the foundational principle that risk management practices should be commensurate with the level of risk and complexity of their third-party relationships and the risk and complexity of the banking organization's operations.

Microsoft generally supports the inclusion of the concepts discussed in OCC's 2020 Frequently Asked Questions ("OCC 2020 FAQs") in the finalized Guidance, but recommends minor revisions to the language in FAQs 1, 5, and 8 to better align the FAQ answers to how the concept of "critical activity" is used in the body of the Proposed Guidance.

Microsoft agrees with the statement in FAQ Number 8 that "[m]ere involvement in a critical activity does not necessarily make a third party a critical third party." If a banking organization determines that an activity is a "critical activity," it does not necessarily follow that all third parties that support that activity are "critical third parties" that should be subject to enhanced risk management and oversight.

To enhance the clarity of the description of "critical activities" in the finalized Guidance, Microsoft encourages the Agencies to replace references to "critical third party" and "critical third party service provider" in FAQs 1, 5, and 8 (where not being used to illustrate the differences noted above) with the phrase "third party that supports a critical activity" (or similar).

II. Subcontractors

In Question 15, the Agencies requested comments on ways the Proposed Guidance could be enhanced to provide more clarity on conducting due diligence for subcontractor relationships.

Microsoft considers it of importance that the finalized Guidance should not operate in such a way as to render subcontracting impractical. Banking organizations cannot be reasonably expected to oversee the entire supply chain for all outsourced activities, nor should that be necessary from a risk management perspective. A substantial part of subcontracting can be considered non-essential or low risk to the services that are being provided by the third party to the banking organization, and imposing compliance requirements that are not proportionate to the level of contribution can lead to unnecessary administrative burden.

To provide more clarity on conducting due diligence for subcontractor relationships, Microsoft recommends the finalized Guidance expressly differentiate between subcontractors that support "critical activities" and subcontractors that support non-critical activities. Enhanced risk management

expectations should apply by default only where there is "subcontracting of a critical activity, or a material part thereof," with the parties free to impose similar requirements for other arrangements by contract (e.g., if they determine that subcontracting would increase risks materially). This standard is intended to provide a clear yet flexible limiting principle for the application of risk management obligations to subcontractors to ensure that all supervisory expectations are respected and, where necessary, audit rights are granted.

As discussed in more detail below, Microsoft encourages the Agencies to harmonize supervisory expectations for third-party risk management in the United States with standards in Europe and elsewhere, and this proposed standard for subcontracting aligns to the standard used by the European Banking Authority.[2]

III. Third-Party Reports and Certifications

In Question 16, the Agencies requested comments on ways the Proposed Guidance could provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations.

FAQs 14, 24, and 25 of the OCC's 2020 FAQs suggest a number of ways to increase the efficiency of risk management through reliance on reports of compliance with service-level agreements, reports of independent reviewers, certificates of compliance with International Organization for Standardization (ISO) standards, service organization control (SOC) reports, and third-party assessment services (sometimes referred to as third-party utilities).

Microsoft agrees that use of these due diligence options may be more cost effective for banking organization, and further supports these options due to their potential to reduce the compliance burden on third parties if their adoption allows banking organizations to reduce the number of duplicative due diligence requests. Microsoft believes that quality, integrity, and fitness-for-purpose are what matter, rather than the identity of the party that conducts them, and believes banking organizations should be permitted greater latitude to rely on third party diligence options so long as they provide adequate information for the banking organization to properly assess its risks.

Microsoft recognizes that a risk-based approach to third-party risk management may necessitate individualized due diligence and audits in some instances, but a one-to-one audit relationship for all banking organization-to-third party combinations in all circumstances is not scalable, nor is it necessary if reliable alternative or standardized approaches are available. Permitting banking organizations to make use of these alternatives to direct one-on-one audits according to a risk-based principle of proportionality would be more consistent with the approach taken in other sections of the Proposed Guidance.

To provide better clarity to banking organizations conducting due diligence, Microsoft encourages the Agencies to revise the language of FAQs 14, 24, and 25 to be more specific about the level of reliance banking organizations may place on each due diligence option discussed therein. For example, as currently written, the plain text of the answer to FAQ 14 expressly permits banking organizations to

[2] *See* European Banking Authority, *Final Report on EBA Guidelines on Outsourcing Arrangements*, Section 10.1 (Feb. 25, 2019). A summary of the EBA standard can be found on page 112 of the Final Report.

actually "rely" on "pooled audit reports," (audits paid for by a group of banks that use the same company for similar services) and disclosures made by financial market utilities. By contrast, the text of the answer to FAQ 24 does not expressly permit a banking organization to "rely" on a third party's SOC reports, an omission made more confusing given the fact that the text of the question itself asks whether a bank may "rely" on such reports.

Microsoft encourages the Agencies to remove this ambiguity by expressly confirming that banking organizations may "rely" on the third-party reports, certifications, and assessment services discussed in FAQs 14, 25, and 25. These changes are particularly significant to cloud services providers, which offer standardized services at hyperscale and would benefit from the scalability of cloud SOC reports, third-party assessments (e.g., TruSight[3]), and other standardized approaches.

To the extent the Agencies have concerns that permitting reliance in all circumstances could undermine the efficacy of risk management activities in some instances, Microsoft suggests the Agencies make reliance conditional on a determination that reliance is reasonable under the circumstances, and if necessary, articulate principles in the finalized Guidance or FAQs to guide banking organizations on how to determine whether reliance is reasonable.

Microsoft believes these changes would be more consistent with a principles-based approach and would strike a balance that would enable banking organizations and third-party service providers alike to benefit from the efficiency associated with use of third-party certifications, reports, and assessment services.

IV. Contractual Provisions

In Question 7, the Agencies requested comments on ways the Proposed Guidance could be revised to better address challenges a banking organization may face in negotiating some third-party contracts.

Banking organizations are sophisticated organizations. Microsoft believes the list of contractual provisions typically considered in contract negotiations provides helpful guidance that will be relevant to a wide range of third-party relationships. Microsoft supports the use of tailored contractual provisions to manage risks presented by a service or activity (e.g., cloud computing), but notes that tailoring contractual provisions to every counterparty banking organization to reflect that organization's unique internal compliance or risk management posture would be impractical, and inconsistent with nature of hyperscale cloud services which are standardized

V. Consistency and Harmonization

Microsoft supports the Agencies' efforts to promote consistency in third-party risk management guidance by applying the guidance to all banking organizations supervised by the Agencies and encourages other U.S. federal and state financial regulators to take comparable action. We understand

[3] https://trusightsolutions.com/

that the Financial Industry Regulatory Authority ("FINRA") is monitoring the Agencies' Proposed Guidance,[4] and Microsoft encourages other regulators to do the same.

Microsoft also encourages the Agencies to consider ways to promote clarity as to how the Agencies' third-party risk management expectations complement or overlap with the regulatory and supervisory frameworks for cybersecurity and data protection. These overlapping frameworks reflect many of the same principles as the Proposed Guidance, and processes and controls often support compliance with more than one framework.

Finally, Microsoft encourages the Agencies to coordinate with comparable non-U.S. financial regulators such as the UK's Prudential Regulation Authority, the European Banking Authority, and Monetary Authority of Singapore, as well as other influential bodies such as the International Organization of Securities Commissions ("IOSCO"), the Financial Stability Board, and the Basel Committee on Banking Supervision, to promote greater consistency in third-party risk management expectations across jurisdictions in an increasingly global industry.

We appreciate the effort by the FFIEC to modernize its approach in light of the fast-paced nature of innovation occurring in the banking segment, including the rapid adoption of cloud computing for banking functions. We hope these comments will help further clarify some key points consistent with these overarching principles of managing risk and enabling innovation for the benefit of the financial ecosystem as a whole.

Sincerely,

David J. Dadoun

Managing Director, Global Regulatory Compliance
Worldwide Financial Services
Microsoft Corporation

[4] *See* FINRA Regulatory Notice 21-29, *FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors* (Aug. 13, 2021).