Microsoft Comments on the Basel Committee on Banking Supervision's Proposed Principles for the Sound Management of Third-Party Risk

9 October 2024

Microsoft appreciates the opportunity to provide comments on the Basel Committee on Banking Supervision's ("***Committee***") proposed *Principles for the Sound Management of Third-Party Risk* in the banking sector (the "***Principles***").

As an overarching objective, Microsoft supports the goal of the Principles to "achieve a balance in improving practices related to the management of third parties and providing a common baseline for banks and supervisors, while maintaining sufficient flexibility given the evolution of practices in this area."[1]

The Committee's Principles can and should be referenced as a foundation for national regulators to develop their own third-party risk management guidance and regulations, which can further facilitate regulatory interoperability across jurisdictions. Financial institutions[2] and their service providers can also use the Principles as a foundation for their own third-party risk management frameworks, using the Principles as a guide to ensure that they satisfy baseline regulatory requirements within jurisdiction-specific requirements, yet remain flexible with a principles-based approach.

Based on Microsoft's experience in supporting financial institutions to meet their regulatory requirements across jurisdictions, we share perspectives on key elements concerning these Principles in addressing these areas at a global scale.

* * * * *

Introduction: A holistic, principles-based, technology-agnostic approach to third-party risk management.

> *"The Principles focus on third-party risk management holistically and are technology-agnostic to keep pace with technological developments. They*

[1] *Principles*, Paragraph 3.

[2] The Committee stated in the preamble that the Principles are designed provide guidance to "banks," but also recognized and intended that financial institutions other than banks may find the Principles beneficial. Microsoft is a third-party service provider to both banks and other financial institution types, and our comments are intended to apply to both banks and other financial institutions unless expressly indicated otherwise in the text.

> *aim to promote international engagement, greater collaboration, and consistency, with a view to reducing regulatory fragmentation and strengthening the overall operational resilience of the global banking system."*[3]

Consistent with other regulatory frameworks, such as DORA,[4] reaffirming a technology-agnostic approach to third-party risk management will support regulatory frameworks that permit and enable innovation without exposing financial institutions to unnecessary risk. By remaining technology-agnostic, the Principles allow for the incorporation of cutting-edge solutions without being constrained by more prescriptive approaches that are tied to specific technologies, ensuring that financial institutions can adopt the latest advancements while maintaining robust risk management practices.

Further, by promoting international consistency, the Principles can help ensure that financial institutions and their service providers manage risks effectively across evolving technologies and regulatory landscapes, without facing the operational challenges that regulatory fragmentation might cause. This promotes smoother operations, reduces compliance complexity, and ensures a consistent framework for managing third-party risks globally. It can also enhance overall risk management practices that are more centralized in a consistent way for businesses operating across multiple jurisdictions.

Definitions: Expectations for "nth parties" versus "key nth parties"

> *"Banks should have appropriate risk management processes to identify and manage the supply chain risks, proportionate to the criticality of the services being provided. Banks' risk assessment, due diligence, contracting and onboarding and ongoing monitoring processes should evaluate the TPSP's ability to manage its nth parties[5] and meet equivalent contractual obligations (e.g., level of service, risk management, compliance, operational resilience standards). Further, contracts should reflect the right of banks to obtain information (including incident notifications) about key nth parties[6] on an ongoing basis."*[7]

---

[3] *Principles*, Paragraph 4.

[4] Digital Operations Resilience Act (DORA), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022).

[5] *See Principles*, Paragraph 11 (defining "nth party" as "a service provider that is part of a TPSP's supply chain and supports the ultimate delivery of services to one or more banks. This term includes, but is not limited to, subcontractors of the TPSP").

[6] *See Principles*, Paragraph 11 (defining "key nth party" as "a service provider that is part of a TPSP's supply chain and supports the ultimate delivery of a critical service by a TPSP to a bank or that has the ability to access sensitive or confidential bank information (e.g., consumer data)").

[7] *Principles*, Paragraph 6.

We broadly support the Principles' stated expectation that "[b]anks should have appropriate risk management processes to identify and manage the supply chain risks, *proportionate to the criticality of the services being provided*" (emphasis added).[8] However, we believe the Principles could be improved by more clearly distinguishing the expectations for oversight of "nth parties" from those of "key nth parties."

As currently defined in the Principles, the term "nth party" captures any service provider that is part of a TPSP's supply chain and supports the ultimate delivery of services to a bank, even in circumstances where (i) the service being delivered by the TPSP to the bank through the TPSP's use of the nth party is not critical to the bank, and/or (ii) the service being provided by the nth party to the TPSP is not critical or material to the TPSP's delivery of the service (which service may or may not be critical to the bank).

We believe the Principles should be modified to recognize that supply chain risk management throughout the entire supply chain — not just for banks themselves, but also their TPSPs — should be proportionate to the criticality of the services being provided. We believe this adjustment is necessary to prevent banks and TPSPs from expending limited resources attempting to closely oversee all nth parties that have *any* role at all in the TPSP's provision of a service, even if the nth party's contribution is immaterial and would not disrupt the provision of the TPSP's critical service to the bank. Thus, we recommend this is narrowed to only those "key nth parties" for purposes of establishing oversight and risk assessments, given that otherwise it is unmanageable and not proportionate or risk-based in approach.

Principle 5: "TPSP arrangements should be governed by legally binding written contracts that clearly describe rights and obligations, responsibilities, and expectations of all parties in the arrangement."

Paragraph 42 of the Principles lists contractual provisions to be included in banks' contracts with critical TPSPs. We wish to provide our views on three specific provisions listed in Paragraph 42 and our suggestions for minor adjustments that can be made to better tailor the provisions to their policy aims.

First, the Principles state that banks' contracts governing critical TPSP arrangements should address "TPSPs' obligation to take out insurance against insurable risks."[9] We believe there should not be a regulatory requirement or expectation for the TPSP to take out insurance as a blanket rule. Insurance is one aspect of commercial risk that banks and TPSPs should consider. A TPSP's commercial decision to obtain insurance coverage (or have self-insurance if appropriate), is one aspect of assessing risk of that provider that a financial institution should consider, including obtaining its own insurance coverage when outsourcing to a third-party. This commercial aspect should be left between the parties as part of an overall risk assessment when considering a TSPS.

---

[8] *Principles*, Paragraph 15.

[9] *Principles*, Paragraph 42.

Second, the Principles state that banks' contracts governing critical TPSP arrangements should address "obligations and responsibilities for BCPs and DRPs [and] should include minimum service uptime and/or maximum service downtime commitments, recovery time objectives ("RTOs") and recovery point objectives ("RPOs")." In the context of "Infrastructure as a Service" ("IaaS"), we agree that RTOs and RPOs can be important metrics for defining resilience and recovery expectations in case of data loss service interruptions, or failures, but this fails to account for criticality of workloads or the shared responsibility model associated with cloud computing. Indeed, as drafted this language implies that the burden is primarily or exclusively on the TPSP, which is inconsistent with a "shared responsibility" model. Within the shared responsibility model, IaaS providers (e.g., cloud providers) secure and maintain the IaaS physical infrastructure, but the bank customers are accountable for implementing RTO and RPO through their own configurations, backups, and recovery practices to meet their specific business continuity needs. Thus, this should be re-drafted to account for the shared responsibility model, including implementation and configuration requirements for critical workloads running on IaaS, which remain the responsibility of the financial institution, not the TPSP, to address.

Third, the Principles state that banks' contracts governing critical TPSP arrangements should address the "rights of banks to access, audit, and obtain relevant information from key nth parties." As the definition of "key nth party" makes clear, banks do not have direct relationships with the key nth parties; the relationships are through the TPSPs. We recommend that this language be clarified to reflect that the right to access, audit, and obtain relevant information from key nth parties must necessarily involve the TPSP given there is not privity between the financial institution and downstream key nth parties. Provided that the contract confers audit rights between the TSTP and the financial institution, and that the TSTP enables audit rights through to the key nth party, this should satisfy expectations on audit and assurance through the supply chain of key nth parties.

Principle 7: "Banks should, on an ongoing basis, assess and monitor the performance and changes in the risks and criticality of TPSP arrangements and report accordingly to board and senior management. Banks should respond to issues as appropriate."

In support of all Principles, but Principle 7 in particular, the Committee states that there are various types of audits and multiple sources of assurance that banks can use in their due diligence and onboarding and ongoing monitoring of TPSPs:[10]

> *Audits include those by independent parties engaged by either a single bank, a collection of banks working collaboratively (e.g., pooled audits), or the TPSPs themselves (to be provided to and critically reviewed by banks). Additional sources of assurance may include industry-recognized certifications or standards (e.g., ISO*

[10] *Principles*, Paragraph 15.

certification). These certifications and standards can help provide a comparable, baseline level of assurance about TPSPs' controls, but they may not, by themselves, provide all the assurance banks need regarding the resilience of critical services. These certifications and standards should therefore not be seen as eliminating the need for audits and other forms of assurance where appropriate.

We agree with the Committee that the level and depth of assurance should be proportionate to the level of criticality of the service and the risks it poses to the bank. It follows that regulators cannot and should not prescribe a "one-size-fits-all" approach to assurance.

We believe that the use of several different assurance approaches, either alone or in combination, can help mitigate unnecessary costs and burden while achieving a level of assurance that is proportionate to the criticality of the service and the risks presented to the bank.

For non-critical services provided by TPSPs we agree that financial institutions should be able to rely on third-party audits and certifications, such as SOC 2, ISO 27001, and ISO 22301. These certifications involve rigorous, independent evaluations conducted by certified auditors. These approaches can provide banks with confidence that their TPSPs are managing risk effectively while avoiding the need for each bank to perform that assessment itself, thereby eliminating the burden on the TPSP of redundant assessments. If the level of risk warrants a greater level of assurance than can be provided through a certification alone, banks should be able to use pooled audits, which can often be a cost-effective way of obtaining the additional information needed.

Advances in technology and automation are also introducing new approaches that can be leveraged by banks to fulfill their third-party risk management responsibilities. Automated assurance relies on real-time data collection and monitoring from the TPSP's systems to provide early alerts on potential risks, helping banks identify potential issues more promptly and efficiently than could be accomplished through a more traditional periodic audit. Self-serve evidence portals can allow banks to access up-to-date compliance and risk metrics directly from the TPSP, reducing the need for ad-hoc data requests.

We believe the approaches discussed above provide efficient, effective, and logistically feasible ways for banks to monitor TPSP's risk management practices and reflect the principles of criticality and proportionality. These solutions promote consistency, ensure high-quality assessments, and reduce duplicative efforts. By tailoring their assurance approaches to be proportionate to the criticality of TPSP services, banks can maintain a balanced, effective risk management framework while reducing compliance burden on both their TPSPs and themselves.

Principle 8: "Banks should maintain robust business continuity management to ensure their ability to operate in case of a TPSP service disruption."

The Proposal states that a bank's business continuity management (BCM) governing critical TPSP arrangements should include "assurance testing (e.g., walkthroughs, tabletops and simulations) [to ensure that] that the TPSP's BCP methodologies are robust."[11] It also states that banks should consider "joint design and testing of BCPs with TPSPs or utilize independent parties to do the same."[12]

Joint testing, if performed on a one-to-one basis between each bank and the TPSP, effectively requires banks to engage in redundant assurance testing. This results in unnecessary operational burdens for banks and TPSPs, without any measurable increase in the efficacy of risk management.

To alleviate these logistical and practical burdens while still promoting the overall policy aims of these expectations, we propose that banks and TPSPs be allowed to rely on third-party testing reports for business continuity management. These provide an appropriate level of assurance needed and can be done at scale without duplication for standardized services.

Principle 10: "Supervisors should consider third-party risk management as an integral part of ongoing assessment of banks."

In support of Principle 10, the Committee states that "[a]s certain TPSP arrangements require highly technical skills, supervisors should periodically evaluate the knowledge and skills of supervisory staff."[13] Microsoft has for several years worked to have a dialogue with and educate regulators about cloud services to help upskill examiners to enable them to perform their supervisory duties. We would encourage and welcome the opportunity to continue to hold examiner workshops, tailored for the audience, and would equally support a program for BIS in this regard (and have done such workshops for BIS in various areas such as on Responsible AI).

Principle 12: "Supervisors should promote coordination and dialogue across sectors and borders to monitor systemic risks posed by critical TPSPs that provide services to banks."

In support of Principle 12, the Committee states that "[b]ank supervisors should promote coordination and dialogue among themselves, supervisors of other sectors and relevant stakeholders to monitor systemic risk" and explains that such collaboration "may

[11] *Principles*, Paragraph 59.

[12] *Principles*, Paragraph 60.

[13] *Principles*, Paragraph 69.

include a variety of efforts to support the resiliency of critical infrastructure (e.g., industry- and/or supervisory-led business continuity exercises)."[14]

Microsoft supports regulatory coordination and dialogue and believes there remain opportunities for greater collaboration in areas beyond the policy area, including: (i) sectoral tabletop exercises on key issues, (ii) coordination amongst regulators on cyber risks, (iii) assess concentration risks at a macro level, and (iv) greater coordination when it comes to regulatory oversight of third-party service providers through implementation of memorandums of understanding (MOUs).

By way of example, when supervisory authorities in multiple jurisdictions coordinate their oversight through MOUs, it alleviates the need for multiple, overlapping examinations that often take place concurrently across different jurisdictions. It also helps drive synergies for regulators, avoiding duplicative efforts, and saving both costs and resources. Thus, in the same manner that financial institutions can conduct pooled audits, regulators could, through MOUs, conduct joint examinations, avoiding duplicative processes. Such joint examinations already exist to some degree today by and between US bank regulators, certain European regulators, the European Central Bank, and are also contemplated as the process under DORA. There is an opportunity to enhance joint examination teams across jurisdictions going forward.

In addition, regular tabletop exercises and coordinated response and recovery exercises between supervisory bodies and TPSPs would facilitate best practices for learnings on cross-border resilience. This proactive approach would enhance the ability to respond to and recover from cyberattacks, outages, or other systemic disruptions in a coordinated manner, reducing the potential impact on global financial stability.

In each of these areas, greater synergies, learnings, and information sharing can facilitate a more coordinated and systemic approach that will enhance regulatory oversight of global technology providers supporting critical infrastructure. Commonality of issues by such providers, operating across jurisdictions, remains constant, and thus a more coordinated approach amongst regulators can help mitigate regulatory fragmentation and inefficiencies.

In summary, the use of MOUs and cross-border collaboration mechanisms is not only beneficial for reducing regulatory fragmentation but also enhances regulatory oversight and strengthens resilience of the financial ecosystem.

* * * * *

Microsoft appreciates the Committee's leadership in developing the *Principles for the Sound Management of Third-Party Risk*. As a provider of innovative technology services to financial institutions of all sizes in dozens of jurisdictions around the world, Microsoft supports the use of the Principles as a baseline set of expectations to create a globally

[14] *Principles*, Paragraph 71.

consistent regulatory framework for management of third-party risks in the banking sector. We look forward to continued collaboration with regulators, financial institutions, and other stakeholders on these efforts.