MICROSOFT’S RESPONSE TO THE BASEL COMMITTEE ON BANKING SUPERVISION CONSULTATIVE DOCUMENT PRINCIPLES FOR OPERATIONAL RESILIENCY

6 November 2020

1. **Introduction**

Microsoft welcomes the Basel Committee on Banking Supervision's ("Committee") consultation on the Principles for Operational Resilience. We support the Committee's pragmatic and flexible approach to operational resiliency as this will help banks withstand, adapt and recover from potential hazards that can emerge across different parts of the organization.

2. **An evolving operational risk landscape**

As a starting point, we agree that, foundationally, the Operational Resilience Principles contained in the consultation paper provide for an outcomes based approach that is both flexible and adaptable to that institutions should follow in managing risk, including for use of third-party outsourcing.

We appreciate the Committee's perspective that the pandemic has "exacerbated these operational risks and increased economic and business uncertainty." At the same time, we have also experience that the pandemic has shown that banks who relied on innovative technology found themselves in a better position to address these abrupt global changes, thereby efficiently and effectively addressing operational risks. In other words, use of technologies like cloud computing actually enhanced operational resilience, as opposed to diminishing it. This illustrates that modern technology, in particular technologies such as cloud computing that offer a high level of elasticity, may increase a bank's ability to be agile and flexible when responding to operational risks and unanticipated external factors, enabling institutions to manage such risks effectively, if not better, than traditional legacy environments.

With this in mind, we recommend that the Committee account for in its principles that institutions may manage operational risks and resiliency by design. Legacy technology solutions may have inherent design weaknesses that prevent them to adapt quickly to changing circumstances following from operational risks such as infrastructure failures, pandemics, cyber-incidents and other external factors. Operational design elements in addressing risk may include the following:

- First, technology used for banking operations should be updated on a continuous basis to avoid end-of-support and end-of-life issues, or known security vulnerabilities, that increase operational risk.

- Secondly, implementation of solutions should leverage distributed deployments across multiple physical locations or fault domains, eliminating single points of failure, balancing loads across multiple systems and by ensuring there is sufficient spare capacity or elasticity in the environment to deal with abrupt increases in usage. On this last point we have seen during the pandemic that the elasticity offered by cloud providers has allowed financial firms to quickly adapt and respond to abrupt changes in demand without a need for setting up on premise spare capacity. This presents a clear benefit of cloud computing in addressing operational risks.

3. Principle 5: third-party dependency management

Under paragraph 34 concerning business continuity and exit planning, we recommend that, for clarity, that exit strategies requiring planning and testing, but are a measure of last resort, and do not require immediate action in the event of downtime but are more for transition and migration should an institution for whatever reason choose to switch to a different platform.

4.0 Principle 7: ICT including cyber security

As a matter of good hygiene and practical application of address cybersecurity risks, we recommend that the Committee consider including the cyber security principle of assume breach, which is intended to include ensuring that necessary mechanisms are put in place to timely detect threats, such as performing regular penetration testing against the environment and ensuring threat monitoring capabilities are both in place and working effectively.

In addition, the elements under paragraph 41 should not be limited to remote connection but should apply broadly to all systems used by the financial institution.

5. **Questions on the proposed principles**

We limit our responses only to those questions not previously addressed above.

Q3. Are there any specific lessons resulting from the Covid-19 pandemic, including relevant containment measures, that the proposed principles for operational resilience should reflect?

We believe the Covid-19 pandemic has demonstrated that technology has helped banks address and manage operational resiliency, including with remote working and remote connections to customers.

Q4. Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience?

We believe it is important that there is global alignment on the principles on operational resiliency across bank supervisors and overseers. Therefore, we do welcome these proposed principles by the Basel Committee and are generally very supportive of this consultation.