6th November 2020

Mr. Pablo Hernández de Cos, Chairman
Ms. Carolyn Rogers, Secretary General
The Basel Committee on Banking Supervision
Centralbahnplatz 2
4051 Basel
Switzerland

Via Electronic Submission

Dear Mr. Hernández de Cos and Ms. Rogers,

Re: The Basel Committee on Banking Supervision Consultative Document: "Principles for Operational Resilience"

Citi welcomes the opportunity to respond to the Basel Committee on Banking Supervision (BCBS) consultation on "Principles for Operational Resilience".

We agree with the BCBS that "*in light of the critical role that banks play in the operation of the global financial infrastructure, increasing their resilience would provide additional safeguards to the financial system.*" We support the remarks made by The Office of the Superintendent of Financial Institutions (OSFI) Canada that "*operational resilience takes a more outcomes-based approach to a given adverse event. It assumes that operational disruptions will occur and encourages financial institutions to consider ways in which the impact of these events might be reduced*" and that "*traditional business continuity risk management… does not sufficiently capture the breadth of dependencies across the business; nor does it go far enough in creating a culture in which organizations assume that disruption will occur, and prepare and adapt accordingly*."[1]

The need for enhanced operational resilience is even more critical due to the significant increase in the digitization of financial services, greater connectivity within and between firms, and the deployment of new technologies, for example, application programming interfaces (APIs). As such, we fully agree with the comments made by the Australian Prudential Regulation Authority (APRA), that firms must be able to "*continue to deliver business services in the face of potential shocks, including... situations and events that require a more strategic response, such as regulatory developments, new competitors with more efficient operating models, risks associated with climate change, and innovative technology solutions.*"[2]

As highlighted throughout the Covid-19 crisis, operational resilience is a vital lens through which the public and private sector must evolve from viewing risks and threats as being mostly business or geography specific, to evaluating risk and infrastructure globally.

We welcome the BCBS principles, which we view as aligned with consultation documents or other statements on Operational Resilience from several jurisdictions such as Australia, Canada, the European Union, Singapore, the United Kingdom and the United States of America.

---

[1] OSFI, September 2020: "Developing financial sector resilience in a digital world", https://www.osfi-bsif.gc.ca/Eng/Docs/tchrsk.pdf.

[2] APRA, 202: "COVID-19: A real-world test of operational resilience": https://www.apra.gov.au/covid-19-a-real-world-test-of-operational-resilience.

Whilst the respective jurisdictions' papers and BCBS Principles may use different terminology and anchor to different points of reference, they take a similar approach, requiring firms to:

- understand their end to end processes with a view to both preventing and managing disruption events, and minimizing negative repercussions to market stability and integrity, to the end-users, for example, regulators, financial market infrastructures, counterparties and clients, and to the firm itself;

- understand the complexity and interdependencies of all the underlying components within the end to end processes;

- test and evidence their ability to deliver these commitments to external end-users ("resilience profile");

- provide appropriate linkage to resolution plans and booking models; and

- provide senior leaders, Group and Subsidiary Boards with transparency into their resilience profile, related risk posture and risk appetite.

We fully support the creation of "tolerance for disruption" as articulated by the US Agencies in their paper "Sound Practices to Strengthen Operational Resilience"[3], or named as "impact tolerances" per the UK supervisory authorities' discussion and consultation papers[4], as a new governance tool to complement firms' risk appetite statements through its focus on minimizing the impact of disruption when risk(s), threat(s) or vulnerabilities have crystallized. We feel that the creation of "tolerance for disruption" or "impact tolerances", will enhance ours and the financial system's ability to decrease the new and emerging commercial risks and threats posed to our clients and markets from greater digitization and inter-connected business models.

Reflecting on this, Citi structures its operational resilience work along the lines of five core themes:

1. A robust, integrated governance model alongside a culture focused on transparency of lessons learned and continuous improvement: strong accountability, partnership and ownership from Legal Entities and lines of business, supported by robust Group and Subsidiary Board challenge and oversight. Vulnerabilities are actively identified and escalated, with all employees feeling accountable for resilience, and comfortable to challenge and raise issues in other areas of the organisation.

2. Objective, defined prioritisation of important business services: ability to pre-determine how, and in what order, important business services need to be prioritised depending on the needs of clients and other stakeholders. The decision-making framework is adaptable and takes into account various scenarios, with clear understanding of the trade-offs between stakeholder expectations, decisions, and the integrity of all our legal entities, and aligns to our Recovery & Resolution Planning (RRP) core business lines, critical operations and critical economic functions.

3. Persistent preparedness and resilience: ability of firms, as much as practical, to provide important business services to our clients and stakeholders, even under sustained and prolonged operational disruptions. This could be by offering alternatives, by making recovery times as short as possible, or by minimising the impact of service degradation, including by communicating clearly with our stakeholders. A key principle is that important business services are designed, managed and invested in, such that they are able to adapt

[3] US Agencies, October 2020. "Sound Practices to Strengthen Operational Resilience": https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf

[4] Bank of England, PRA, FCA, July 2018. "Discussion Paper: Building the UK financial sector's operational resilience": https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf. December, 2019 package of consultation proposals from the same authorities: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp2919.pdf; https://www.fca.org.uk/publication/consultation/cp19-32.pdf; https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp2919.pdf.

to changing conditions – and operational resilience plans and assumptions are dynamic and kept relevant to the context of the current operating environment.

4. Graceful degradation: ability to maintain a degree of functionality even when a large portion of a system or process has been rendered inoperative. This principle expects that systems can operate in a degraded state, not just "on or off" / "up or down", such that important business services can be continued to be delivered within their impact tolerances.

5. Robust scenario planning, analysis and testing: ability to demonstrate safety and soundness through demonstrable resilience, based on robust stress testing and exercising, rather than only documented processes. More severe but plausible testing aims to actively uncover vulnerabilities and push beyond impact tolerances, whilst also supporting the focus on culture articulated in theme one.

With their Principles approach, the BCBS helps outline a framework that firms should apply in order to govern various programmes such as new product development, data protection, change and capacity management, incident response, third parties, business continuity, and scenario analysis.

Whilst we have contributed to the work of various trade associations, such as the Institute of International Finance (IIF), the Global Financial Markets Association (GFMA), the Bank Policy Institute (BPI), we wanted to underscore to you directly the importance of the following issues:

- globally coherent and consistent regulation underpinned by cross-border regulatory and supervisory co-operation; at a minimum, the willing ness of home and host regulators to grant mutual recognition and equivalence for non-conceptual areas such as different terminologies;

- organizational, reporting and governance structures, and appropriate accountability;

- ensuring a client-centric and business-driven approach is taken to defining important business services and impact tolerances; and

- strengthening and evolving public and private sector co-ordination and collaboration.

Operational resilience will require collaboration within firms, the industry, and with the public sector. It is not a business function, but a business ethos. As such, and given its relative newness as a topic, we strongly encourage deeper public and private sector collaboration globally. An effective feedback structure that supports an iterative process and continuous dialogue between regulatory authorities and industry is paramount, and we encourage regulators to embrace the opportunity to develop a regulatory regime that meets the resilience challenges of a new digital era.

We would be delighted to meet to discuss these opportunities at a mutually convenient time. In the meantime, please do not hesitate to contact me if Citi can help in any way.

Yours sincerely

Jennifer Kleinert

Chief Operating Officer,
Enterprise Infrastructure Operations and Technology
Citi

Appendix

There is an increasing risk of severe (but plausible) disruption in today's increasingly interconnected financial system. For example:

- The firm-to-firm digital connection tools, such as application programming interfaces (APIs), bring risks that may be transmitted quicker through the system, and impacts may materialize where they may not have before.

- With the current economic conditions and low interest rate environment, many corporates and small to medium enterprises will look to optimize their contingency and digitization processes through reliance on providers of financial services, resulting in greater dependency on a resilient financial system.

This will require a heightened level of international regulatory cooperation, collaboration and alignment, as well as greater focus on firms' decision-making around trade-offs, within the context of all other regulatory objectives. For example: client-centricity, reputational risk, culture and conduct, market stability and integrity, financial resilience, and corporate governance.

Q1. Has the Committee appropriately captured the necessary requirements of an effective operational resilience approach for banks? Are there any aspects that the Committee could consider further?

Whilst we welcome the Committee's principles, we have a concern that the BCBS paper is too broad in scope, and there is opportunity for further consideration regarding (i) areas of interpretive issues, (ii) resources required to reach a sufficient outcome, (iii) granularity of the information required (e.g. mapping), and (iv) clearly articulating in what way these principles are different from, or leverage, existing guidance to explain what outcomes are expected.

For example, we call for further explanation of certain concepts to avoid potential misunderstanding across authorities or firms:

- Critical operations, respective functions, and degree of cross reference to Recovery and Resolution Planning (RRP) terminology.
    - The definition of critical operations used in the Consultative Document is based on the Joint Forum's 2006 high-level principles for business continuity encompasses "critical functions" as defined by the Financial Stability Board (FSB) and is expanded to include, activities, processes, services and their relevant supporting assets, the disruption of which would be material to the continued operation of the bank or its role in the financial system.

    - We seek a clearer definition of "critical operations" as paragraph 13 says it is being expanded to include "critical functions", whereas footnote 12 on that same page refers back to "critical operations" in existing RRP terminology.

    - Without a clear scope, it will be significantly challenging for firms to develop a significantly "higher standard" of resilience for the critically important services it provides, and it will also means that mapping interdependencies / interconnections etc. could become significantly more challenging, and resource intensive, to the point it may unintentionally hinder "enhanced resilience".

    - Providing a narrow definition that focuses on the role banks play in the operation of the global financial infrastructure will ensure greater consistency on how banks and regulators interpret this, and it will ensure that investment and focus is kept on ensuring banks can continue to provide important business services to their clients and other market participants, to ensure consumer protection, market integrity,

market stability and firms' own safety and soundness is maintained to the highest of standards.

    - We recommend that the BCBS takes a more granular, narrowly defined focus by looking at what banks deliver to external entities, and their importance within the context of the global financial system. This allows a greater focus and clear "starting point" for firms as they undertake "end to end" (front to middle to back office) mapping, and an ability to deliver a significantly higher level of resilience to those services that are most critical.

- risk appetite, risk capacity and risk tolerance; and

- definition of criticality, e.g. critical vs. important, and clarity on how to determine whether a particular operation is "critical" given that it depends on the nature of the bank, its operating model, and the role it plays in the financial system.

These definitional issues would require practical discussions around examples (e.g., risk tolerance, risk capacity and risk appetite have not generally been used in a resilience construct.)

Finally, whilst harmonization and alignment with RRP is relevant for operational resilience, it would be useful for firms to have flexibility to determine to what extent this harmonization should be done, and what to do in cases where a critical operation is identified for operational resilience, but not for resolution planning, given that the underlying policy drivers for each are based on different scenarios and assumptions.

Additional aspects for the Committee to consider, particularly in their role as the primary global prudential standard setter, include:

- Critical infrastructure protection efforts and remediation have too often been focused on assets and organizations rather than underlying services and functions, which can result in the underestimation of sector-wide and cross-sector risks and dependencies.

- Further, risk management activities continue to be silo-ed at the industry level; opportunities exist for additional coordination across sectors and between government and industry, a distinct need given the cross-cutting nature of critical infrastructure technologies like industrial control systems.

Q2. Do you have any comments on the individual principles and supporting commentary?

Principle 1: Banks should utilize their existing governance structure to establish, oversee and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimize their impact on delivering critical operations through disruption.

We believe that a firm should be able to determine the specifics of their own operational resilience programs based on the services it delivers to clients, and proportionately to the firm's business and risk profile, including its role in the broader market.

Whilst we agree that firms should be able to leverage and evolve their existing structures, we do not believe that they should be required to do so. However, we believe it is important to note that firms do not typically take an end to end approach in the context of the concept of operational resilience that has emerged today, given the unprecedented level of digitisation and connectivity of today's world. For example, the firm-to-firm connection that digital tools, such as application programming interfaces (APIs), bring means risks may be transmitted quicker through the system, and impacts may materialise where they may not have before.

Today, banks are organised around “product” and “functions” i.e. a department by department basis within lines of business. For example, even Recovery & Resolution Planning (RRP) and business continuity are structured around products – not end-to-end services we offer clients – but in a crisis, particularly given heightened digitisation, it is the client business service view that is needed, and provides the best holistic view (for example, to manage down exposures and positions). A business service view of resilience, as opposed to a business product or function (department / process) approach, requires a front-to-back ‘line of sight’ across multiple teams, and helps to set impact tolerances to disruption.

For example, acting as a direct custodian to give clients access to HK (or UK or Australian or US) market infrastructures, involves not just a “direct custody and clearing” product view, but an end-to-end view covering various aspects including sales, technology, operations, cash management, foreign exchange, sanctions screening, product control, financial, risk and regulatory reporting among others. These teams may be located in different countries and legal entities, depending on the individual scenarios. Equally, our client may operate and use these services through multiple legal entities in different jurisdictions; Operational Risk, Recovery & Resolution Planning (RRP), and business continuity, for example, tend to operate in a product-b-product (or business-b-business) or market-by-market manner – whereas for operational resilience, a true end-to-end connected view is required.

As such, firms should be able to leverage existing broader risk management frameworks, if they choose, acknowledging that these may need to be augmented or supplemented, as necessary – but they should not be required to leverage existing frameworks.

In the areas of governance and (operational) decision-making, strategic decisions will usually be made at the board and senior level, but firms should have the flexibility to decide which decisions are taken at the appropriate level of management.

Principle 2: Banks should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with their operational resilience expectations.

We believe it’s important that operational risk and operational resilience are not conflated or treated as the same.

Operational resilience is broader than operational risk, and includes far many more risk considerations, For example, it touches on liquidity risk, strategic risk, conduct risk, market and credit risk, etc. Operational resilience is how a firm designs, invests in, governs and manages its organizational capabilities to absorb and adapt to shocks, to, as the APRA says, “continue to deliver business services”.

For example, an operational resilience event could impact liability funding risk, under liquidity risk, or, as the APRA notes, a resilience shock could be “new competitors with more efficient operating models” which falls under strategic risk (operating environment risk).

Whilst we understand the intention of the principle, we believe it is important to provide clarity on the broader scope of operational resilience compared to operational risk. Instead of linking operational resilience solely to operational risk, it should be noted that operational resilience depends on the effective management of all enterprise risk types.

Principle 3: Banks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption.

We recognise the importance of Business Continuity Plans (BCP) in delivering Operational Resilience but believe they are only one component of Operational Resilience. BCP only considers a "later stage" of resilience planning. It would be helpful if BCBS reference other aspects that support Operational Resilience – for example new product design, development and approval.

By promoting the concept of "operational resilience by design", firms, their customers and other market participants not only have more secure, trustworthy and reliable products and services, but the firms will have quicker time to market, less overhead costs, better user experience, and fewer errors.

Resilience at the idea inception, design and build phase of new products and business services, is critical – and in many ways more important than BCP which is planning for resilience of something that already exists.

Principle 4: Once a bank has identified its critical operations, the bank should map the relevant internal and external interconnections and interdependencies to set operational resilience expectations that are necessary for the delivery of critical operations.

We believe that "critical operations" are too high-level and broad in nature and since they are derived from the planning of a financial stress event (given their Recovery & Resolution Planning focus), they do not always easily translate to the outcome firms deliver to external entities. We believe this is where the focus should be (i.e. what we deliver to clients and other market participants, such as financial market infrastructures and central banks) as opposed to internal activities / operations which should be treated as components (within the end to end view) that enable a firm to deliver the end to end outcome to external entities.

With regard to the wording "*should map the relevant internal and external interconnections and interdependencies to set operational resilience expectations that are necessary for the delivery of critical operations*", the emphasis on "interconnections" is an explicit reminder that regulators expect firms to know who they are connected to and how, so they can articulate (1) how threats / vulnerabilities may be transmitted (into them or by them), and (2) contingency / substitutability options. The requirement to map a firm's important business services from end-to-end requires careful thought on the granularity of information and the ability to keep it "real-time".

Mapping for the purpose of identifying vulnerabilities requires information on key people (and their skillsets), data, applications, technology, controls, processes, capacity, software lifecycles, change management, third parties and governance, which, for a multinational firm, will span across different legal vehicles and jurisdictions. This poses a challenge of practicality and will require banks to take a judgment approach (i.e., if a vulnerability disrupts a critical operation/business service but was in a process not deemed "relevant" and thus not included in a map, what will be the regulatory response)? If mapping is too granular such that senior managers / the board do not use it to set tolerances and strategy, does it mean it is not serving the intended purpose?

We further note that, especially given evolving technologies and enhanced focus on client delivery, these processes will undergo continuous change rendering granular reviews challenging.

We would therefore suggest the BCBS align with the concept of important business services as set forth by the Australian and UK regulators.

Principle 5: Banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intra-group entities, for the delivery of critical operations.

We very much welcome the term "dependency management" as it better captures the need for more than just risk management and the requirement to be agile in its application.

There are potential challenges to be considered as firms apply principle 5 and dependency management across the ecosystem. For example, it cannot be ruled out that some suppliers maybe reluctant or slow to make the necessary changes and/or no immediate substitute suppliers exist. We would recommend that in such cases supervisors accept transition periods allowing banks time to find alternative solutions. These transition periods are needed to avoid cliff edge effects, especially if more firms use the same supplier or clients depend on the service provided by the bank.

In order to effectively manage risks associated with third party relationships and to comply with mandates set forth by regulatory bodies, financial institutions should build information security and resilience requirements into their contracts with third parties. However, this approach is not wholly effective as it results in financial institutions, each with their own standards and controls, engaging with each of their third party suppliers to ensure they have sufficient controls operating effectively throughout the lifecycle of the contract.

The lack of standardization in controls, processes, and reporting across industry results in unnecessary complexity and frustration for both the financial institutions and the third parties.

Furthermore, third parties may be reticent to disclose technical details or design vulnerabilities about their products and services as doing so could threaten the confidentiality of their IP or create a risk exposure if that material is compromised.

Additionally:

- It is difficult for firms individually to assess systemic concentration risk. We call for collaboration with the authorities to help address this challenge by, for example, aggregating our business service maps with their own, and identifying and publishing third-party supplier concentration risks.

- Further consideration should be given as to how the authorities can, and should, take action to remediate vulnerabilities occurring in third parties that operate outside the regulatory perimeter.

Principle 6: Banks should develop and implement response and recovery plans to manage incident that could disrupt the delivery of critical operations in line with the bank's risk tolerance for disruption considering the bank's risk appetite, risk capacity and risk profile. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.

We are supportive of principle 6 and recognise that continuous improvement in incident response and recovery in critical. Rather than establishing a Recovery Time Objective (RTO) time limits for specific systems, we support a principle that focuses more broadly on resumption of service, measured by the firm's best efforts to ensure the ability to safely meet contractual and regulatory service obligations - and benchmarked / guided by an impact tolerance.

An area where clarity would be helpful is the connection between ICT and non-ICT risks, and what is the scope of the incidents being covered here. We would welcome additional guidance around the scope of the BCBS incident reporting expectations given the many possible types of incidents and overlap with some existing reporting requirements. For example, FSB has just released its own final report on Effective Practices for Cyber Incident Response and Recovery[5].

Further clarification would be helpful to distinguish incident management from crisis management. Crisis management is not an elevated incident management approach but is a more strategic oversight to manage the impacts/consequences of an incident and to lead the strategic response.

[5] FSB 2020. "Effective Practices for Cyber Incident Response and Recovery: Final Report": https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/.

Crisis management is seen as the responsibility of the entity/function accountable for the critical operations in scope of the disruption. It would be very welcomed if the BCBS could add a distinct definition of crisis management to clarify this point.

As a global bank, when it comes to incident response, we note that no singular governance framework comes in a "one size fits all" format, so it's important to adjust and leverage capabilities where appropriate and focus on practical solutions that will be necessary and of use to the organization. For example, we believe it is important to highlight that for cyber, given its rapid evolution and variations, a playbook can't dictate every step like a "cook book"; governance structures, processes and playbooks should instead lay out a command structure and minimum essential activities that need to be executed during a response.

Principle 7: Banks should ensure resilient ICT including cyber security that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant information to users on a timely basis in order to fully support and facilitate the delivery of the bank's critical operations.

We agree with the ethos of principle 7. However, we believe that Operational Resilience is threat and vulnerability agnostic, with cyber just one threat out of many, that requires consideration. As such, it is not entirely clear why ICT including cyber security has received its own principle whilst there are many other critical resources at firms, including people / staff management, that have not been afforded their own principle.

Further, this principle should be flexible enough to capture risks arising from emerging technologies. Paragraph 41 is very specific to remote access (which seems to be targeted at a prolonged COVID-19 scenario) while other paragraphs are more generic.

We feel that it would be highly beneficial for the principles to reference common ICT capabilities that are of particular interest for operational resilience, including change management, capacity management, logical and physical security, backup management, environmental controls, etc.

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?

In a recent speech, Wayne Byres, Chair of the Australian Prudential Regulation Authority (APRA), also said that COVID-19 has been a "very real test of banks' operational resilience" and that over the past six months "there has been no significant degradation of services provided to customers."[6]

He also identified a number of initial lessons learned, around: board oversight of risks exceeding risk tolerance levels; the robustness and breadth of business continuity plans; increased risks to information security; impact of change freezes and deferrals; reliance on third-party service providers; ability to test contingency arrangements; and, the human toll of an extreme environment.

Covid-19 did show that operational resilience is really the combination of people resilience, organisational capabilities and financial resilience – and together these mean a firm should absorb and adapt to shocks, not contribute to them.

Select learnings from COVID-19:

Third party:

[6] APRA 2020. "APRA Chair Wayne Byres - Remarks to the BCBS outreach meeting on operational resilience": https://www.apra.gov.au/news-and-publications/apra-chair-wayne-byres-remarks-to-bcbs-outreach-meeting-on-operational.

- Need enhanced focus on concentration risks (by client service, external & internal in same location, and sector).

- Need to ensure 3rd party has identified its dependencies, including local infrastructure. For example, in some countries, an issue was reliable internet service. Going forwards, there needs to be greater coordination between different sectors such as telecommunications.

- Ensure greater focus on testing and thinking of "non-operational" risks that may arise fatigue/inability to "pass the book", site-specific capacity issues (such as personnel demographics and circumstances, fatigue, government infrastructure, broadband quality, staff access to required equipment) – and how these risks are amplified by volume increase in manual activities (for example, faxes) and market-driven volume increase.

Legacy market approaches:

- Countries that were not "physical" could be supported seamlessly with little additional risk or disruption. However, risks were amplified in physical settlement markets. For example, in relation to custody and clearing "Working from Home" policies impacted our and clients' abilities and timeliness as certain activities required staff to be on-site, such as CSD / central bank communications through specific terminals, processing of checks, access to on-site vaults, markets yet to adapt to accept electronic documentation, receipt of documents sent via post or courier.

Whilst Covid-19 is an example of a resilience event, from a reputational perspective, given it impacted all firms, market participants and clients, it, in some respects, is more unique and less impactful to a firm or market stability compared to a CCP having a technology outage or a firm suffering from a cyber-attack.

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

We believe it is important to keep operational resilience separate from operational risk. Traditionally, operational risk is concerned with reducing risk through preventative measures. We understand that operational resilience, however, is an outcome and requires an approach that assumes that a given risk (or threat) has crystallized, hence the focus on the ability to respond, recover and learn from disruptive events. Currently, the role of a firm's operational risk management in recovery measures is unclear, and clarity is important as this has not traditionally sat within operational risk frameworks.

Further, we call for the principles on operational resilience to include a greater focus on continuing to serve clients, and the inclusion of the principles on certain activities, such as new product design, development and approval, business growth strategies, setting of target markets, change and capacity management, etc. – with focus of additional principles on:

- Horizon-scanning and driving a more forward-looking approach to identifying risks, threats, vulnerabilities and opportunities;

- Operational and legal entity integrity, efficiency and excellence;

- Optimized balance sheet, and improved operating cost flexibility to adapt to disruptions;

- Improved decision-making;

- More integrated business and growth strategies; and

- Better control environment, infrastructure management and less manual intervention

Q5. What kind of metrics does your organization find useful for measuring operational resilience? What data are used to produce these metrics?

We agree that "*measuring a bank's operational resilience is in a nascent stage and further work is required to develop a reliable set of metrics that both banks and supervisors can use to assess whether resilience expectations are being met.*"

While there are several metrics used within the industry for the separate disciplines under the Principles, this is an area that requires very careful consideration not least due to several factors:

- The appropriateness and effectiveness of metrics vary for each discipline;
- The purpose / quality / usefulness of metrics needs to be made clear and outcomes driven;
- There could also be several metrics for thing being measured, for example, end of life metrics;
- Metrics can also be split into those that are lagging (historic) and those that are leading (control effectiveness) indicators;
- Metrics can represent and apply to either key controls or key risks. It is often difficult for metrics to reflect the aggregation of risks; and
- Metrics should not breach principles of competition.

Further, given operational resilience requires a degree of aggregation of measures across domains – namely an end to end approach – it must also be recognised that "operational resilience metrics", in the near term, will need to grapple with:

- high probability of false-positives which could both over-rate and under-rate risks, or vice versa;
- a lack of normalized and standardised data quality, availability, and granularity; and
- a lack of debated and common approach to the weighting given to data sets and the metrics they produce.

It is important to recognise that firms already manage and reduce risk. For example, firms manage cyber risk by choosing whether to use anti-virus protection, train staff, or to make cyber a Board level priority. What is lacking is a mature way to measure cyber risk, and a consistent way to understand what is being measured and how it is managed.

For banks, FinTech or 'Big Tech' providing financial services, in today's data economy the fundamental commodity at risk from disruptions increasingly appears to be trust. Capital reserves, credit ratings and other methods of attributing value using financial assets will increasingly serve as proxies for trust but will not be synonymous with the underlying reality.

Effective measurement of resilience will need to account for erosion of trust and assign relative responsibility to the various components of the end-to-end system and processes. This includes people (vendors, employees and customers), processes (system-wide processes, which may be operating in multiple jurisdictions), and technologies.

Current emphasis tends to lie with technology failures and related mitigations; as technology is only part of the problem, resilience metrics that do not incorporate people or processes will have limited effectiveness. As such, linking resilience metrics to the services provided by the firm, for example, holding customer data for accounts, access to payment systems, or managing data related to confidential transactions, will be important.

We propose, that before regulators and firms define metrics to measure operational resilience**, it must first be identified what questions we think will aid our understanding of resilience**.

Outlining what would give us assurance is a critical first step. We propose the following questions as "food for thought" for the BCBS and private sector to explore and refine, which we believe will then enable regulators and firms to define and produce metrics on operational resilience, much like the "The Information Security Hierarchy of Needs."[7] It is important to note that metrics may change over time due to new technologies and operating models, and may differ between firms. By starting from first principles and a series of questions we should be asking ourselves, there will be a degree of consistency and comparability across the sector.

These questions also provide a framework for Group and Subsidiary Boards to leverage.

<u>What does "operational resilience" mean?</u>

1. What do we mean by "resilience"? Is it:
    a. Meeting clients' / regulators' / market participants' / shareholders' expectations, i.e., 99% up-time (or is it down-time)?
    b. The external entity receiving what we committed to?
    c. Quality of client experience and service?
2. How do we know we are resilient?
    a. We know about the disruption first from ourselves, not from regulators, clients or other external parties?
    b. We never breach an impact tolerance?
    c. We know how clients will be / are impacted by the service degradation – and we can find other ways of meeting their needs (in most situations as appropriate)?
3. How do we know we are not resilient?
    a. Other parties tells us about the disruption?
    b. We cannot easily, quickly find information on legal entity or client impacts, internal and external contact details etc.?
    c. There is hesitation to escalate to higher severity level?

As we reflect on creating metrics, we feel it is helpful to group "resilience" under various categories, with relevant questions we would want to ask in order to understand our resilience - from these questions, we can then understand what data and metrics we would use to measure and track our operational resilience.

<u>Business service delivery</u>

1. Do we know what we deliver to clients (when / where / how)?
2. Do we have the maturity to know if an external entity, i.e., FMI or vendor, is disrupted / impacted?

[7] "The Information Security Hierarchy of Needs" by Matt Swann, formerly of Microsoft: https://github.com/swannman/ircapabilities.

3. Do we have the maturity to know if an important business service is disrupted / impacted?

4. How do we set an expectation with our clients around resilient?

Vulnerabilities, threats and risks

1. Do we have practical, current visibility across all the end-to-end components of important business services, incl. inter-affiliates and 3rd parties?

2. What are the known vulnerabilities (including manual touchpoints and "key subject matter expert" risk) in the enterprise and important business services?

3. What controls protect important business services from disruption vs. the controls that sustain important business services in disruption?

4. Can we detect unauthorized activity and/or an adversary that is already in our system? Can we respond at the same tempo as an adversary?

In disruption

1. What is our ability to continue to meet client needs, deliver high quality experience and be responsive to clients, when disruption is ongoing?

2. How do we communicate internally and externally during disruption?

3. Do we know the consequences of our external entities i.e., counterparties, vendors or clients, and wider Citi (boards, and employee) reactions to disruption, and of the trade-offs of our decision-making?

4. In disruption, can we return our important business services to normal? When would we know this has happened – and from what and whom would we take assurance from that our important business services, and their underlying processes and component parts, are operational with integrity?

5. After disruption, do we have adequate culture and technical capability to answer the question "*what just happened"*?

Investing

1. How do our legal entities and lines of business each demonstrate that their efforts have made us more resilient?

2. How do we ensure we are building resilience into "new things", i.e., products, systems, processes?

3. What is our confidence factor that all risks, threats, vulnerabilities – and opportunities – that need to be identified have been identified?