ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Darren Hannah
Vice-President
Finance, Risk & Prudential Policy

Tel (416) 357-2361
dhannah@cba.ca

November 6, 2020

Secretariat of the Basel Committee
on Banking Supervision (BCBS)
Bank for International Settlements
CH-4002 Basel, Switzerland

Dear Basel Committee members:

Re: CBA[1] Comments on BCBS consultative documents on principles of operational risk and resilience

We appreciate the opportunity to review the BCBS consultative documents dated August 6, 2020, "*Revisions to the principles for the sound management of operational risk*" (Revised PSMOR) and "*Principles for operational resilience*" (POR).

We understand that the BCBS is proposing a number of updates to the PSMOR, including the introduction of guidance on information and communication technologies (ICT). The POR is built on the PSMOR and draws from previously issued principles on corporate governance for banks, as well as outsourcing, business continuity, and relevant risk management guidance.

Overall, we continue to support a principles-based approach to the guidance. Given the changing landscape, which includes increased technology adoption and the spread of third-party service providers, a principles-based approach will be particularly important in providing the flexibility needed to address emerging risks and to develop enhanced operational resilience within the banking industry going forward. We are also supportive of the additional guidance on various components of the operational risk management framework contained in the Revised PSMOR, which enhance the common understanding of the principles' requirements.

With the introduction of the POR, we believe that ongoing discussion on the alignment between the Revised PSMOR and POR is required to provide clarification on how the two documents complement each other to achieve their purpose. This will help the industry in achieving effective and efficient implementation.

A summary of key issues and questions for clarification is provided below. Detailed comments, including responses to the BCBS's questions posed in the documents, are included in Appendices 1 and 2.

[1] The Canadian Bankers Association is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals. www.cba.ca

Alignment of the principles of operational risk management and principles of operational resilience

We believe that resilience is not an additional risk but an evolving practice, as stated in the POR:

> [Para 8] "*Operational resilience is an outcome that benefits from the effective management of operational risk*".

In order to achieve the operational resilience outcome stated above, we believe there needs to be stronger alignment of the Revised PSMOR and POR to provide audiences with additional context on the two documents.

In particular, we are concerned that similar concepts and principles are included in both consultative documents (e.g. three lines of defense, business continuity planning, ICT), which can lead to duplication and/or inconsistent interpretation of the requirements. We believe it is important for the BCBS to clarify the role/purpose of the two documents and how they complement each other to achieve the BCBS's objectives/vision of enhanced operational risk management and operational resilience.

If two separate documents are required, we recommend that common definitions and concepts be provided in one document (e.g. PSMOR), and cross referenced in the other document (e.g. POR) to ensure a common understanding and consistency of application.

Interpretation of the three lines of defence

(PSMOR, Sections 3.0; PMO, Para 14)

We note that the revised PSMOR provides additional guidance for the design of the risk management model, including the roles and responsibilities of the three lines of defence. Revised PSMOR [Para 5] stated that:

> "*Banks commonly rely on three lines of defence: (i) business unit management, (ii) an independent corporate operational risk management function (CORF), and (iii) independent assurance."*

As the role of corporate functions has multiple aspects (e.g. compliance, risk management, governance, information security), it has led to corporate functions being categorized as either the first or second line of defence in different jurisdictions.

We ask that the BCBS clarify that it is not changing the current PSMOR requirements, but rather documenting the roles and responsibilities of the three lines of defence for consistency across different BCBS guidelines. We understand that supervisors continue to have national discretion in the interpretation of the three lines of defence model as appropriate for their jurisdiction.

Please see more detailed questions and suggested alternative text in the attached Appendix 1.

Principles for business continuity planning

(PSMOR, Principle 11; PMO, Principle 3)

Business continuity management by its very nature is meant to drive improvements to the overall resilience of an organization. Adoption of an operationally resilient corporate mindset requires clear articulation of operational resilience in the corporate strategy that is translated into actions (i.e. forward planning, communication, training, as well as day-to-day operations).

There is currently some overlap in business continuity statements between the two documents. We believe that it would be preferable to have one overarching statement in the POR and refer to the PSMOR document for all details. Over time, this will reduce duplication of effort and potential discrepancies in implementation.

We note that the Joint Forum (i.e. BCBS, IOSCO, IAIS) paper, *High-level principles for business continuity*[2], is dated. For example, the paper places emphasis on recovery rather than on continuity/resiliency. Since it is referenced in the Revised PSMOR (footnote 24) and POR (footnote 16), we recommend that the Joint Forum update the 2006 guideline to incorporate current industry standards and practices. We also recommend that the Joint Forum's paper should reflect the recent learnings from COVID-19 regarding severity and duration of a pandemic. However, we recognize that the process of reaching international consensus on BCBS principles-based guidance on evolving issues, such as resilience and business continuity, is ongoing and will take time to align.

Please see more comments in our response on Question 1 in the attached Appendix 2.

Definition of information and communication technology

(PSMOR, Principle 10; PMO, Principle 7)

The Revised PSMOR introduced a new principle on ICT. It is unclear why ICT differs from other types or categories of operational risk as the governance and risk processes outlined in this principle are the same as other operational risk types. We ask the BCBS to clarify the significance or rationale for a separate principle. We are of the view that there are varied definitions used for ICT, both inside and outside the financial sector. We request that the BCBS exercise flexibility as this risk is being captured in different ways in a financial institution's enterprise-wide risk management function.

Further, we ask for the view of the BCBS on the relationship between operational resilience, operational risk management, and ICT, and how institutions should integrate these concepts into their broader enterprise risk management.

Please see more detailed questions in the attached appendices.

[2] August 2006, www.bis.org/publ/joint17.pdf

Thank you for considering our comments when developing the final updates on the PSMOR and POR. We look forward to ongoing engagement on these evolving topics.

Sincerely,

Attachments:

- Appendix 1 – detailed comments on "*Revisions to the principles for the sound management of operational risk"*
- Appendix 2 – detailed comments on "*Principles for operational resilience*"

CC OSFI:

- Sanjiv Talwar, Assistant Superintendent, Risk Support Sector
- Angie Radiskovic, Senior Director, Non-Financial Risk Group

CBA comments on Basel Committee on Banking Supervision (BCBS) consultative document: *Revisions to the principles for the sound management of operational risk*

CBA Members' Comments and Requests for Clarification
1. INTRODUCTION *(Pages 1 - 2)*
Question 1: Has the Committee incorporated and appropriate revisions to the Principles? Do you have any specific comments on the revisions to the Principles and supporting paragraphs?
▪ In summary, the revised Principles are helpful as they provide additional guidance on components of the operational risk management function (ORMF). Please see below for specific comments on the revisions to the Principles and/or the supporting paragraphs. ▪ We believe a more principles-based approach is more appropriate, and recommend the use of the qualifier "may include" instead of "should include" for examples in the document to provide flexibility as appropriate.
Question 2: Are there any aspects that the Committee should consider further?
We believe that the BCBS should consider: ▪ More explicit commentary to articulate the linkages between operational resiliency and the objectives of operational risk management. This may include expanding the definition of operational risk beyond the "risk of loss" to include the "*risk of being unable to deliver critical operations"*, which may have repercussions for both the organization and the wider financial system beyond financial loss. ▪ Providing further commentary on the management of emerging risks. Current operational risk management practices are heavily focused on the identification, assessment and monitoring of existing/known risks. As operational risk management should be forward-looking, equally important is the proactive identification, assessment, and monitoring of emerging risk. ▪ We observed that reference to "operational resiliency" was removed from the Principles. We believe we need to discuss the linkage between the Principles of Sound Operational Risk Management to Operational Resilience.

Appendix 1

CBA Members' Comments and Requests for Clarification
2. COMPONENTS OF OPERATIONAL RISK MANAGEMENT *(Page 2)*
▪ No comments.
3. OPERATIONAL RISK MANAGEMENT *(Pages 2 - 5)*
▪ The revised PSMOR continues to take the approach that the concept of the three lines of defence is generally an organizational view. While this is generally accurate, all lines of defence can contribute risk to the organization, not just the first line as alluded to in the document. Furthermore, when the second line generates the risk, the second line cannot be an independent review of the risk. ▪ [Para 5]*: "Banks commonly rely on three lines of defence: (i) <u>business unit management</u> 5, (ii) an independent corporate operational risk management function (CORF) and (iii) independent assurance."* *Footnote 5: "The term "<u>business unit"</u> is meant broadly to include all associated support, corporate, and/or shared service functions, as for example: Finance, Compliance, Legal, Human Resources, Operations and Technology etc. Risk Management and Internal Audit are not included unless otherwise specifically indicated."* "*Business line management*" in the 2011 document, was changed to "*Business unit management*" in the consultative document. Paragraph 5 of the consultative document could be confusing in that it includes in the first line of defence, functions that are also considered as part of the second line of defence. We believe that the composition of each line of defence should be better clarified. In addition, we note that some financial institutions consider the Compliance group as a second line of defence function, but in footnote 5 it is listed as an example of a business unit (i.e. first line of defence). We assume that this is an example, and that there is some flexibility for national discretion in its interpretation. ▪ [Para 6(c)]: Consider replacing the word "*continuously*" with "*regularly"* as a more practical and measurable term - *"Is ~~continuously~~ <u>regularly</u> and adequately trained;"* ▪ [Para 7]: Consider elaborating on the *"confusion around roles and responsibilities*" noted by the BCBS with respect to the three lines of defence model.

CBA Members' Comments and Requests for Clarification
▪ [Para 7] This paragraph states; *"The Committee recently highlighted that despite the three lines of defence model being widely adopted by banks, confusion around roles and responsibilities sometimes hampers its effectiveness. Thus, the review of the Principles is also the opportunity to stress that this model should be adequately and proportionally used by financial institutions to manage every kind of operational risk sub-category, including ICT risk."* Would the BCBS please clarify why ICT risk is being specified from other types and categories of operational risk. ▪ [Para 9 (a)]: "*A functionally independent corporate operational risk function (CORF) is typically the second line of defence. The responsibilities of an effective second line of defence ….."* Does this mean that we recognize there are other second line of defence functions that are not part of the corporate operational risk function? ▪ [Para 9 (b)]: *"<u>providing evidence</u> of this effective challenge"* – We believe that it is unnecessary to explicitly call this out in this case, as most risk management activities should and are evidenced in some form or fashion, but are not called out in other sections of the principles. ▪ [Para 9 (e)]: "*Designing and providing operational risk training and awareness.*" – should the first line of defence have the responsibility too? The second line of defence can provide training on op risk program/tools/awareness at the enterprise level, but the first line of defence needs to develop business-specific training that is more specific/applicable to the business unit. ▪ [Para 10]: "*CORF should have a reporting structure independent of the risk generating business units and be responsible for the design, maintenance and ongoing development of the ORMF within the bank."* Similar to our question above on [Para 5], how do we treat corporate control groups (e.g. Legal, HR)? Are they first or second line of defence? In some jurisdictions, regulators only view "Risk Management" as the second line of defence. ▪ [Para 11]: *The scope and frequency of reviews should be sufficient to cover <u>all activities and legal entities of a bank</u>"* Why do we need to specify "legal entities"? Why do legal entities need to be separately called out? ▪ [Para 11]: This paragraph seems to suggest that the third line of defence (i.e. Internal Audit) should not be using any of the ORMF tools and or executing its processes. In other words, Internal Audit would not report on any operational losses incurred, or document and assess any controls that it owns, etc. Is this the intent of this paragraph? As Internal Audit's own activities have inherent operational risks, we believe that such risks should be managed through the organization's ORMF in the same way as risk exposures owned by business units. We believe

CBA Members' Comments and Requests for Clarification
that the BCBS should clarify the expectations of the third line of defence in using the tools outlined in the organization's ORMF to manage its own risk exposures. ▪ [Para 12]: "*…. ensure that operational losses are adequately addressed in a timely manner.*" Should we say "*operational risk events*" are adequately addressed in a timely manner, rather than "*operational losses*" as losses are after the fact? ▪ [Para 12]: "*Improvements in operational risk management depend heavily on senior management willingness to be proactive and also act promptly and appropriately to address operational risk managers' concerns.*" We are uncertain if we agree with this statement, as senior management may also identify operational risk, and not just act on items identified by operational risk managers. Is it suggested that senior management is a "roadblock"?
4. PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK GOVERNANCE *(Pages 5 - 19)*
***Principle 1**: The board of directors should take the lead in establishing a strong risk management culture, implemented by senior management. The board of directors and senior management should establish a corporate culture guided by strong risk management, set standards and incentives for professional and responsible behaviour, and ensure that staff receives appropriate risk management and ethics training.*
▪ [Para 17]: This paragraph related to training is very specific as it states that customized training programs should be mandatory for specific roles. In what way should these be customized compared to the standard training program for all employees? ▪ The clause, *"the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation*", was removed from Principle 1 but replaced by *"ensure that staff receives appropriate risk management and ethics training."* Who is responsible for the risk management culture under the revised Principle? Why was the reference to "risk culture" removed?
***Principle 2**: Banks should develop, implement and maintain an operational risk management framework (ORMF) that is fully integrated into the bank's overall risk management processes. The ORMF adopted by an individual bank will depend on a range of factors, including the bank's nature, size, complexity and risk profile.*

CBA Members' Comments and Requests for Clarification
▪ [Para 22(d) and (f)]: We disagree with the need to set risk appetite and tolerance limits/triggers for both inherent and residual risk. The nature of determining risk appetite and tolerance requires that controls and other mitigants be considered in determining appropriate limits/triggers, so there is no perceived value to setting limits/triggers for inherent risk. ▪ [Para 22 (i)]: *"…operational exposures that partially or entirely represent legal (including conduct), model and ICT (including cyber) risks as well as exposures in the credit or market risk boundary*". Why specify only legal, ICT and model risk? ▪ [Para 22 (i)]: The paragraph noted that the operational risk taxonomy can flag *"exposures in the credit or market risk boundaries*". We would like more clarity regarding what exactly is meant by this and what an example would look like.
GOVERNANCE *(pages 8 - 10)*
The Board of Directors *(pages 8 - 9)*
Principle 3: The board of directors should oversee material operational risks and the effectiveness of key controls, and ensure that senior management implements the policies, processes and systems of the ORMF effectively at all decision levels.
▪ In the current Principle *"28 (a) establish a management culture,….*" is removed for the board of director's responsibilities. Does this mean board is not responsible for establishing culture? Why was the reference to "risk culture" removed? ▪ In the current Principle "*28 (b) provide senior management with clear guidance and direction regarding the principles underlying the Framework and approve the corresponding policies developed by senior management*", they underlined text is removed in the revised principle. Does this mean the board is no longer required to approve corresponding policies? ▪ [Para 23(d)]: This paragraph points to the need for the board to challenge senior management on the design and effectiveness of the organization's ORMF. In the context of operational risk management, challenge is typically associated with the activities performed by the second line of defence using a variety of techniques and tools, in addition to operational risk data. In the context of this paragraph, how does

CBA Members' Comments and Requests for Clarification
the BCBS see the board perform "challenge" and is this reference intended to imply that the board perform similar activities, or using similar techniques to those typically associated with the second line of defence? ▪ [Para 24]: This paragraph states "*The control environment should provide appropriate independence/separation of duties between operational risk management functions, business units and support functions*", which seems to conflict with footnote 5, which states "*The term "business unit" is meant broadly to include all associated support, corporate, and/or shared service functions…*".
Principle 4: The board of directors should approve and periodically review a risk appetite and tolerance statement16 for operational risk that articulates the nature, types and levels of operational risk the bank is willing to assume.
▪ This principle is clear as stated.
Senior Management *(Pages 9 - 10)*
Principle 5: Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the bank's risk appetite and tolerance statement.
▪ [Para 27]: *"Banks should be able to demonstrate that the three-lines-of-defence approach is operating satisfactorily and to explain how the board of directors, <u>independent audit committee of the board</u>, and senior management ensure that this approach is implemented and operating in an appropriate manner."* Why the audit committee? Is it assumed the ORMF oversight is provided by the audit committee?
RISK MANAGEMENT ENVIRONMENT *(pages 10 – 18)*
Identification and Assessment *(pages 10 - 13)*

CBA Members' Comments and Requests for Clarification
<u>Principle 6</u>: Senior management should ensure the comprehensive identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.
▪ [Para 34 (a)]: *"…as external is often informative of risks that are common across the industry."* The statement seems to be duplicated in the paragraph.
<u>Principle 7</u>: Senior management should ensure that the bank's change management process is comprehensive, appropriately resourced and include continuous risk and control assessments, adequately articulated between the relevant lines of defence.
▪ [Para 36]: The cost of implementing processes and systems to monitor the impact of a change throughout the life of a product/service outweighs any perceived value. We propose that the impact of changes be monitored up to implementation and that once implemented monitoring be focused on the risk profile of the revised product/service rather than on the delta of the change. ▪ [Para 36]: With reference to the guidance that *"change management should assess the evolution of associated risks across time, from inception to termination"*, would the assessment of risks post-inception be performed through other operational risk management tools such as RCSA? As the life of a product can, in theory, be perpetual, it does not seem feasible that *"change management"* would be responsible for assessing the evolution of associated risks throughout the entire life-cycle. At some point, as the management of the product transitions into a business-as-usual state, the management of associated risks should shift from change management to other mechanisms/processes. ▪ [Para 38]: We appreciate the suggested list of considerations, but would be concerned if the suggested list was made mandatory for all new product/service assessments, as all items would not be applicable in all instances. We recommend that the BCBS add "where feasible" to qualify this list. ▪ [Para 38 (a)]: *"Inherent risks – including legal, ICT and model risks…"* Why do we have to specify legal, ICT and model risks?
Monitoring and Reporting *(pages 13 – 14)*

CBA Members' Comments and Requests for Clarification
***Principle 8**: Senior management should implement a process to regularly monitor operational risk profiles and material operational exposures. Appropriate reporting mechanisms should be in place at the board of directors, senior management, and business unit levels to support proactive management of operational risk.*
▪ The principle is clear as stated.
Control and Mitigation *(pages 14 – 16)*
***Principle 9**: Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.*
▪ [Para 48 (g)]: This seems to be overly prescriptive with "*officers and employees being absent from their duties for a period of not less than two consecutive weeks*" without supporting evidence or research for the stated two week period, and it may not be suitable, feasible, or appropriate for all jurisdictions and institutions. Rather than prescribing a specific absence period, we believe that the BCBS should consider focusing on the importance of mandatory absence requirements that are commensurate with the risk profiles of roles, and the size/complexity of the organization. As a more principles-based approach, we recommend replacing "*two consecutive weeks*" with "*an appropriate consecutive period".* ▪ [Para 50]: Unlike Principle 10, which contains items specific to information and communication technology, Paragraph 50 simply reiterates that technology risk should be managed using similar approaches as operational risk. As such, this paragraph seems to imply or portray technology risk as being separate and distinct from operational risk. Given that it does not introduce any new requirements or concepts, we believe that the BCBS should consider removing this paragraph, and rely on Principle 10 to articulate incremental expectations for managing risks related to information and communication technology. ▪ [Para 51]: We suggest additional consideration regarding data protection and privacy risk.

CBA Members' Comments and Requests for Clarification
▪ [Para 54]: "*Banks should have unified classification, methodology, procedures of operational risk management established by the CORF.*" This paragraph seems to be a high-level summary of Paragraph 22. Is this paragraph designed to introduce any new ideas, or can this paragraph be removed given the details already provided in Paragraph 22?
Information and communication technology NEW *(pages 16 – 17)*
<u>Principle 10</u>: Banks should implement robust ICT23 governance that is consistent with their risk appetite and tolerance statement for operational risk and ensures that their ICT fully supports and facilitates their operations. ICT should be subject to appropriate risk identification, protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness, and convey relevant information to users on a timely basis.
▪ The section for ICT is focused on "*identifying their critical information assets and the infrastructure upon which they depend*". We suggest this should be rewritten to focus on (see underscored text), "*identifying their critical information <u>and communication technology (ICT), which includes</u> the infrastructure upon which they depend*". This would help reinforce that resilience should be focused on the technology (information resides here) and infrastructure (information rails). ▪ It should be clearly stated if disaster recovery is in-scope or out of scope for this section as disaster recovery has been stricken from the new section 11, therefore. appears nowhere (additional comments provided in Principle 11). That is, is disaster recovery included in this principle? ▪ Further to our comment on page 2 of this feedback related to the elevated focus on ICT risk, it is somewhat unclear how this principle differs from other types or categories of operational risk and what is specifically "exceptional", in terms of focus on ICT risk, and the need for a separate principle. ▪ [Footnote 23]: We wish to highlight that there are varied definitions used for ICT, and request that the BCBS exercise flexibility in this regard.

CBA Members' Comments and Requests for Clarification
Business continuity planning *(pages 17 – 18)*
Principle 11: Banks should have business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption.

- Overall this principle seems to miss the essence of "*operational resilience*" by having reactionary language; that is, the principle is founded on the legacy approach to business continuity management where planning is based on "if" an event were to happen, as opposed to the current accepted approach that banks assume the event has, or will, impact their organization and considerations move towards operating "through disruption". The basis is that we assume disruptive events will happen; therefore, pivoting from "*reactive planning*" to "*proactive consideration in advance for critical business operations*".
- The current principle is "*Business Resiliency and Continuity: Principle 10: Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.*" Why is "resiliency" removed when we are trying to promote operational resilience? It seems the BCBS is intentionally separating operational risk management from operational resilience.
- [Principle 11]: We suggest "*business continuity plans"* be replaced with "*business continuity program*". This would be a more holistic term that could then be defined in a footnote to be inclusive of not only the plans but also training & awareness, governance, etc.
- [Footnote 25]: We believe that it should be clearly identified if the scope of business continuity includes disaster recovery (see comment above in Principle 10.
- [Para 58 (c)]: *"The commitment of first and second lines of defence to its design*" Does the second line of defence challenge constitute "commitment" to its design?
- [Para 59]: As written, this principle suggests firmer alignment of core groups accountable for business continuity, scenario planning, and overall severe business disruption management and reporting. It is not clear if this is the intent. We believe that it should be noted that fragmented oversight between groups may make it challenging to meet the requirements of this principle, with multiple groups owning or executing on requirements resulting in potential oversight gaps.

CBA Members' Comments and Requests for Clarification
▪ [Para 59 (b)]: We suggest that this should be from a products and/or services perspective, as opposed to based solely on the BIA to provide for a comprehensive understanding of the end-to-end process for a "*critical business operations*" (i.e. end-to-end mapping of critical business products/services) ▪ [Para 59 (c)]: It is unclear whether this paragraph is alluding to *"impact tolerances*". If it is, then we suggest it be more specific, as the expectation is for "*impact tolerances*" to include more than MTO (Maximum Tolerable Outage), RTO (Recovery Time Objective) and RPO (Recovery Point Objective), but also additional potential impacts such as customers impacted, financial impacts, regulatory impacts, etc. ▪ We suggest the following edits (see underscore and strikeouts) to the paragraphs listed below: ○ [Para 58]*: "Sound and effective governance of banks' business continuity policy requires:* *a) A business continuity policy endorsed and regularly reviewed by the board of directors. ~~The validation and regular review by the board of directors~~;* ○ [Para 59]: *"Banks should prepare ~~forward-looking~~ business continuity plans (BCP) ~~with scenario analyses associated with relevant impact assessments and recovery procedures.~~".* *a) A bank should ground its business continuity ~~policy~~ plan on loss/disruption scenarios ~~analyses~~ ~~of potential disruptions~~ that identify and categorise critical business operations and key internal or external dependencies. In doing so, banks should cover all their business units as well as critical providers and major third parties (e.g. central banks, clearing house).* *b) Each loss/disruption scenario should reference ~~be subject to~~ a quantitative and qualitative impact assessment or business impact analysis (BIA) with regards to its financial, operational, legal and reputational consequences."* *c) Recovery Strategies should address e~~E~~ach loss/disruption scenario should ~~be subject to~~ identify recovery strategies and procedures to minimize impact to critical business operations and respect thresholds (such as maximum tolerable outage, recovery time objectives, and recovery point objectives) identified during the assessment or BIA ~~for the activation of a business continuity procedure. The procedure should address resumption aspects, set recovery time objectives (RTO) and recovery point objectives (RPO) as well as communication guidelines for informing management, employees, regulatory authorities, customer, suppliers, and – where appropriate – civil authorities.~~*

CBA Members' Comments and Requests for Clarification
d) Each business continuity plan should include or reference communication guidelines for informing management, employees, regulatory authorities, customer, suppliers, and – where appropriate – civil authorities. ○ [Para 60]: *"A bank should periodically review all components of its business continuity program ~~policy~~ to ensure that ~~contingency~~ strategies remain consistent with current operations, risks and threats. Training and awareness programmes should ~~be customised based on specific roles to~~ ensure that staff can effectively execute contingency plans. Business continuity plans ~~procedures~~ should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in business continuity testing with key service providers. Results of formal testing and review activities should be documented and reported to senior management and made available to the board of directors."*.
ROLE OF DISCLOSURE *(page 18)*
Principle 12: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management and its operational risk exposure.
▪ Regarding the revised principle added to the end of the current principle, *"…and its operational risk exposure*", is the disclosure of exposure referring to Basel III Pillar 3 disclosure requirement? ▪ [Para 62]: With regards to the underlined text *"Banks should disclose relevant operational risk exposure information to their stakeholders (including significant operational loss events), while not creating operational risk through this disclosure (e.g. description of unaddressed control vulnerabilities).",* it is not entirely clear what is meant by this guidance. The wording seems to imply that when making disclosures that an organization should refrain from disclosing any unaddressed control vulnerabilities. If the intent of BCBS is to allow the banks to weigh the benefits and costs of disclosure , then we recommend that the BCBS remove the example *(e.g. description of unaddressed control vulnerabilities)*.

CBA Members' Comments and Requests for Clarification
ROLE OF SUPERVISORS *(pages 18 – 19)*
▪ The word "*should*" was added to various paragraphs in this section. Is there any significance to these changes? For example, [Para 64]: *"Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at a bank.*" vs the current Principle of "*Supervisors ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at a bank."* ▪ [Para 65]: *"In certain circumstances, supervisors may choose to use external auditors in these assessment processes.*" What is the BCBS's view of *"certain circumstances*", and could you provide examples? ▪ *"Further, to the extent that there are identified reasons why certain development efforts have proven ineffective, such information could be provided in general terms to assist in the planning process.*" This is in the current Principle (para 9). Why was this removed in the revised principles? It would be helpful to banks if we can learn from others.

CBA comments on Basel Committee on Banking Supervision (BCBS) consultative document: *Principles for operational resilience*

CBA Members' Comments and Requests for Clarification
I. INTRODUCTION *(Pages 1 - 2)*
▪ Is there a general intent for the BCBS to streamline guidance on operational risk and resilience; if so, is there any planned timeline? ▪ We support the concept of these principles being embedded into the PSMOR, which we believe is suggested in paragraph 3 (i.e. "*further streamlining of …. Related guidance*").
II. AN EVOLVING OPERATIONAL RISK LANDSCAPE *(Page 2)*
▪ It may be recognized that there are still opportunities to enhance on resilience in the changing landscape with the increase in technology adoption and reliance on third-parties. This part of the consultative document states: "*The Committee's guidance on operational resilience will continue to be informed by its monitoring of the impact of the Covid-19 pandemic and any lessons learned*"; therefore, we wonder if any additional monitoring practices are being implemented in addition to the existing ones? ▪ [Para 7]: While the pandemic is a current concern, we suggest that this document should use more generic terminology when it comes to "*events*". For example, referring to "disruptions" would be more generic.. The focus on pandemic may lead to being blind-sided by other disruptions and associated impacts.
III. ESSENTIAL ELEMENTS OF OPERATIONAL RESILIENCE *(Pages 2 - 3)*
▪ We support the BCBS' recognition that existing frameworks and risk management practices can be leveraged in the pursuit of Operational Resiliency. As well, we support the reference to harmonization with recovery and resolution plans and agree that this implies an appropriate level of alignment.

CBA Members' Comments and Requests for Clarification
▪ Should there be some emphasis put on operational resilience controls related to change (i.e. delivering changes within the organization – both technical and business)? Change itself can create resilience issues and change is the primary means by which new resilience gaps can be introduced. ▪ [Para 8]: "*Operational resilience is an* <u>*outcome*</u> *that benefits from the effective management of operational risk."* Is there opportunity to incorporate the resilience principles in the operational risk management principles and ensure linkage and connection? This paragraph presents operational resilience as an outcome that benefits from effective management of operational risk. However, we believe that the BCBS should consider linking operational resilience to business processes/activities that pose a risk to the financial stability and safety & soundness of an institution (if they were disrupted) as this would further provide the basis to measure resiliency end to end. ▪ [Para 9]: We suggest referring to "*ICT*" as opposed to "*technology*", which would be consist with PSMOR document. ▪ [Para 10]: We suggest including "*ICT*" in addition to *"existing risk management frameworks, business continuity plans and third-party dependency-management are implemented consistently within the organisation.*" ▪ **[**Para 11]: We support a pragmatic principles-based approach and believe this is preferable to a more prescriptive approach.
IV. DEFINITION OF OPERATIONAL RESILIENCE *(Pages 3 - 4)*
▪ [Para 13]: *"…the disruption of which would be material to the continued operation of the bank or its* <u>*role in the financial system*</u>*."* Does "*role in the financial system*" include our commitment to the clients?
V. OPERATIONAL RESILIENCE PRINCIPLES *(Pages 4 – 9)*
▪ [Para 15]: The paper cites *"business continuity planning and testing"* rather than the broader "*business continuity management*", which incorporates the broader practices related to enhancing resiliency. We suggest referring to the latter in the guidance.

CBA Members' Comments and Requests for Clarification
▪ [Para 15]: How is change management being is considered as part of the operational resilience principle? Change management plays a key role in ensuring resilience through change (i.e. avoiding major disruptions during change) and will ultimately improve the way we conduct activities through a resilient mindset.
GOVERNANCE *(pages 4 - 5)*
<u>Principle 1</u>: Banks should utilise 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 minimise their impact on delivering critical operations through disruption.
▪ Similar to proposed guidance in other jurisdictions, one of the key points of operational resilience is to conduct "*Operational Resilience Self-Assessments*" as the final step in the life-cycle, which should be approved by the board. We suggest a similar principle should be included in this consultative document. ▪ The concept of *"operational resilience approach*" is noted numerous times in this section. Would the BCBS please provide clarity on this approach or provide an example in perhaps an appendix. ▪ [Para 17]: *"The board of directors should review and approve the bank's <u>operational resilience expectations</u>*". What is "*operational resilience expectations"*? Does this simply mean its overall tolerance for disruption considering risk appetite, risk capacity, etc.? In what format should the operational resilience expectations be delivered (e.g. a plan, framework, risk appetite/limits and tolerances)? Can it essentially be expressed / articulated / measured as risk appetite metrics? ▪ [Para 17, 18, 20]: Can any of the board requirements in paragraphs 17, 18, 20 be delegated to an appropriate sub-committee of the board? ▪ [Para 19]: Please clarify if these reports to the board only relate to deficiencies or all the reports that relate to ongoing resilience, not only when there are deficiencies. If the former, we suggest the following additional text for the consideration of the BCBS (see underscored text), *"<u>When there are deficiencies that could affect the delivery of the bank's critical operations, s</u>~~S~~enior management should provide timely ~~reports~~ <u>updates</u> on the ongoing operational resilience of the bank's business units ~~in~~ <u>to</u> support ~~of~~ the board's oversight ~~that could affect the delivery of the Bank's critical operations~~.*"

CBA Members' Comments and Requests for Clarification
▪ [Para 20]: We agree that the board of directors should understand the operational resilience approach; however, is it realistic that the board take an active role in establishing the bank's operational resilience approach "*through clear communication of its objectives to all relevant parties, including bank personnel, third parties and intra-group entities"*? Alternatively, should the board challenge the operational resilience approach presented by management?
OPERATIONAL RISK MANAGEMENT *(Pages 5 - 6)*
<u>Principle 2</u>: 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 agree with taking an integrated approach. ▪ [Para 21]: We suggest this should include fraud, project management, technology, and information security risks as well. It seems to miss the point that operational resilience is more than just business continuity and third-party. We recommend the following edited text, *"For operational resilience purposes, appropriate coordination with ~~business continuity planning, third-party dependency management, recovery and resolution planning and other~~ relevant risk management frameworks may yield greater harmonisation in delivering a consistent approach to operational resilience across the enterprise."* ▪ [Para 21]: This sounds like the second line of defence (i.e. Corporate Operational Risk Management function) should drive operational resilience. In a third line of defence model, shouldn't the first line of defence "*manage and address any risks that threatened the delivery of critical operations*" and the second line of defence challenge their operational resilience approach? We suggest that this paragraph could be reworded to be less prescriptive without mention of a specific function to allow banks to determine the optimal approach based on their operating model, which could be first or second line of defence.

CBA Members' Comments and Requests for Clarification
BUSINESS CONTINUITY PLANNING AND TESTING *(page 6)*
***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.**

- Plans need to align to the bank's overall continuity and recovery objectives. Presumably this includes the need for/expectations regarding validation and verification of the processes, which will maintain and sustain business operations and are aligned with the bank's overall continuity and recovery objectives.
- Would the BCBS consider referring to *Principles of Operational Risk* for paragraphs 24 to 28?
- [Para 24]" *"Business continuity exercises should be conducted and validated for a range of severe but plausible scenarios that incorporate disruptive events and incidents.*" We suggest enhancing the language in that scenarios/exercises should also validate that critical operations can continue to operate within impact tolerances during a disruption.
- [Para 24]: We recommend striking-out "forward-looking". Alternatively, since this is new language in PSMOR and POR, perhaps the BCBS could define it in a footnote, including expectations on how a bank could demonstrate that a plan is "forward looking".

  "An effective business continuity plan should ~~be forward-looking when assessing~~ assess the impact of potential disruptions. Business continuity exercises should be conducted and validated for a range of severe but plausible scenarios that incorporate disruptive events and incidents."
- [Para 27]: We request better clarity in this document, as well as *Principles of Operational Risk*, on the importance of a disaster recovery program.
- [Para 28]: We believe that this should be split into two parts – the first sentence is related to crisis/incident management, which belongs in the *Principles of Operational Risk,* while the second sentence would be more appropriate in Section III paragraph 9.
- [Para 28]: This paragraph suggests a stronger connection to recovery and resolution plans in the delivery of critical operations. Clarification on the intention would be helpful.

CBA Members' Comments and Requests for Clarification
MAPPING INTERCONNECTIONS AND INTERDEPENDENCIES *(page 6 – 7)*
<u>Principle 4</u>: 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.
▪ It's important for banks to identify and understand the interconnectedness, interdependencies (internal and external) amongst critical functions and processes; however, it is not essentially through "mapping". Is mapping the correct word or should it be replaced with "*identify and understand*"? To be less prescriptive, we recommend that "map" be replaced with "assess" in Principle 4: *"Once a bank has identified its critical operations, the bank should <u>assess</u> ~~map~~ the relevant internal and external interconnections and interdependencies to set operational resilience expectations that are necessary for the delivery of critical operations."* ▪ [Para 29]: Overlapping content. Appears in section 58/59/60 of Principles of Operational Risk ▪ [Para 29]: We suggest this should refer to *"comprehensive assessment of end-to-end process*" for critical operations. ▪ [Para 29]: The reference to a *"Business Process Map"* was removed from the revised PSMOR as one of the operational risk assessment tools. If PSMOR is to support operational resilience, we suggest the BCBS include a reference to "assessment", which would allow banks to have the flexibility to determine the appropriate tool, which could include a Business Process Map. ▪ [Para 31]: It would be helpful to understand the expectations on the granularity of mapping activities. This is a significant undertaking as related to critical services, clarity would be helpful. We suggest adding more detail to "*approach and granularity of mapping should be sufficient*", as it is vague. However, we would prefer that any references to process mapping maintain flexibility. ▪ [Para 31]: We propose extending paragraph 31 to include a requirement to remediate vulnerabilities to within tolerance levels once assessment is complete, or if vulnerabilities are identified through testing. We prefer any references to type of assessment have the greatest degree of flexibility, which could include process mapping.

CBA Members' Comments and Requests for Clarification
THIRD-PARTY DEPENDENCY MANAGEMENT *(page 7)*
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 agree with the idea of managing dependencies, but we request that the BCBS further define *"intra-group entities"* to ensure alignment with our internal definition. ▪ [Para 33]: We propose specifying that this requirement only relates to third parties supporting critical operations as noted in paragraphs 32 and 34. We propose the following wording change (see underscored text): *"…which should cover how to maintain operational resilience with respect to related critical operations in both normal circumstances and in the event of a disruption."*
INCIDENT MANAGEMENT *(pages 7 - 8)*
Principle 6: Banks should develop and implement response and recovery plans to manage incidents 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 agree that the implementation of response and recovery plans to manage incidents that could disrupt the delivery of critical AI operations is important and should be developed in line with our risk tolerance, appetite, capacity and profile. The principle states that a formalized lessons learned practice be implemented to improve recovery and response practices, suggesting that the organizational structure, including roles and responsibilities, be established in operational resilience plans. We request that the BCBS provide some clarity on whether resolution planning should be considered in our response & recovery plans. ▪ The application of lessons learned can be for more than just response and recovery plans. We believe that they should be considered more broadly and used to improve the overall operational resilience program, inclusive of the response and recovery plans.

CBA Members' Comments and Requests for Clarification
▪ Most of what is being mentioned in Principle 6 is covered in 58/59/60 of Principles of Operational Risk, so we propose that instead the POR refer to the details in the PSMOR. We believe that the focus is the incident and/or crisis management program/policy/processes and protocols in place that compliment the continuity or resolution plan. ▪ Does incident management in this principle refer only to IT incidents? Would the BCBS please clarify this point in footnote 20? ▪ [Para 37]: We believe that this paragraph should include a requirement to proactively update response and recovery playbooks to speed timely recovery given the likely recurrence of IT and cybersecurity incidents for which the root cause remains unknown.
INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) INCLUDING CYBER SECURITY *(pages 8 - 9)*
<u>Principle 7</u>: 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.
▪ The section points to an ICT Framework. Where is the ICT Framework defined? As the PSMOR does not define the ICT framework, is the expectation that banks should establish their ICT Framework outside of the ORMF? Additional guidance would be helpful. ▪ [Para 39]: *"Banks should have a documented <u>ICT policy</u>, including cyber security,…."* vs PSMOR para 55 "…*The appropriate use and implementation of a sound <u>ICT framework</u> contribute to the effectiveness of the control environment and are fundamental to the achievement of a bank's strategic objectives…*" Are these two concepts the same; if so, should they be consistent in the two documents? ▪ The BCBS may wish to consider adding reference to availability, capacity management and redundancy issues. ▪ Principle 7 has been framed with a strong emphasis on cyber, which is a critical component of technical resilience; however, other aspects of technology that make up the ecosystem for the bank have been omitted (e.g. cloud, third party). We note that PSMOR, Principle 10, did not spell out ICT including cyber security. We recommend that any list be provided as "for illustrative purposes", as any definitive list may not be complete given the changing landscape. We are also of the view that it is important to acknowledge institutions may have their own definition of ICT governance and capture risks in different ways. Flexibility in this regard is key.

CBA Members' Comments and Requests for Clarification
▪ It is not entirely clear what is meant by the term "*incorporate appropriate situational awareness*" in the Principle 7. ▪ Remote access is included as an example of assets in the principle requirements, suggesting formal asset management for critical assets is required - additional guidance on the proposed requirements would be helpful. ▪ [Para 41]: We suggest also including consideration of cyber security arrangements with third-parties when they implement remote-access arrangements.
VI. QUESTIONS ON THE PROPOSED PRINCIPLES *(Page 9)*
***Question 1*: 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?**
▪ The requirements captured appear to appropriately reflect a comprehensive approach to operational resilience. As Canadian FI's go through the process of developing and implementing their respective resilience programs, there will undoubtedly be opportunities for further development of the principles and practices associated with operational resilience. ▪ The BCBS has appropriately recognized that further work is necessary for financial institutions to strengthen their ability to absorb operational risk-related events/disruptions, such as pandemics, cyber incidents, technology failures and other disruptive events. The building of resilience based on operational risk principles is also well captured as it helps banks' leverage existing structures and frameworks to enhance their resilience. ▪ We believe the prudential mandate of the BCBS has influenced their definition of operational resilience that focuses on safety & soundness and financial stability. We feel that a broader definition that includes the dimension of consumer harm should be considered.

CBA Members' Comments and Requests for Clarification
***Question 2**: Do you have any comments on the individual principles and supporting commentary?* *[CBA note to draft: To assist in the consolidation of feedback, please include your comments in the sections above on individual principles.]*
▪ One overall observation is that the consultative document seems to be focused on operational resilience within a firm. We believe that the BCBS should consider the concept of operational resilience to include ".*harm to….other market participants in the financial system…and cause instability in the financial system*". BCBS may want to consider adding language that demonstrates how strong operational resilience within a firm can reduce harm to other market participants in the financial system and promote financial stability. ▪ We believe the distinction between senior management vs. board roles and responsibilities is appropriate; however, we would note that the consultative document sometimes gets a little too prescriptive when describing the board's challenge role, which seems more in-line with risk management's role.
***Question 3**: Are there any specific lessons resulting from the Covid-19 pandemic, including relevant containment measures, that the proposed principles for operational resilience should reflect?*
▪ The COVID-19 pandemic highlighted the need for further global consistency and coordination in the approach to operational resilience, the value of a cross-sectoral approach to the development of global operational resilience principles, and the need to maintain flexibility for financial institutions to adapt to challenging circumstances and to their own respective business models. ▪ Reliability and resilience of key technology third parties/outsourcers has been well demonstrated during this time. Given this reliance and the inherent limitations of control and visibility into a vendor's operations, our third party risk management and operational resilience programs take on greater priority in this operating environment and worked well. Remote access has played a vital role. We also note the importance of communication and the establishment of communication strategies and playbooks with respect to internal and external stakeholders. ▪ Prior to COVID-19, the network was designed to allow critical employees to perform work activities remotely from home during unique circumstances (e.g. snow days, public transportation issues). A prolonged period like COVID, which required the majority of the workforce to operate from home due to a pandemic scenario (considered a 1 in 100 year event), required additional assessment and enhancements to meet the demands. The environment had not been stressed and tested to this degree to expose some of the capacity limitations under

CBA Members' Comments and Requests for Clarification	
these conditions. The increased capacity requirements were designed and implemented while maintaining operations during the event. This proved challenging but overall was well executed. ▪ All operations/processes are carried out by "people", should the Principles for operational resilience include a "people" component? ▪ The principles should reflect: o regulatory forbearance, o the vital role of enterprise supply chain management (i.e. not just third-party management), and o the importance of ensuring business continuity plans are properly and regularly tested and are fully enabled to be operational when invoked. ▪ We believe that one of the learnings from COVID-19 is that crisis management/leadership and communication is key. The biggest lesson we are in the process of learning is that the "return to work" portion is more complex and time consuming than we ever planned for in the past.	
<u>Question 4</u>: Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience?	
▪ While there is always room for improvement, we do think that the operational risk and resilience principles have been presented in a thoughtful fashion. We feel the organization of the BCBS principles across seven categories is appropriate and would encourage any further linkage. ▪ We do see merit in further exploration of such possibilities to achieve maximum efficiencies where possible and to ensure operational risk management programs are truly focused on bank capabilities that are most critical. Consolidation will eliminate overlap and duplication of effort, confusion and cost. ▪ There are overlaps/duplications between the PSMOR and operational resilience documents. We believe that the main difference is operational resilience focuses on critical operations. ▪ There is opportunity to update and merge the 2006 Business Continuity Management paper into the BCBS Principles on Operational Risk and Resilience. However, given the relevant immaturity on the topic of operational resilience, there may be value in maintaining the principles	

CBA Members' Comments and Requests for Clarification
on operational resilience. This is the first attempt at resiliency principles and going forward there will undoubtedly be further opportunities for consolidation between PSMOR and POR principles.
VII. **MEASURING OPERATIONAL RESILIENCE** *(Page 9)*
***Question 5**: What kind of metrics does your organisation find useful for measuring operational resilience? What data are used to produce these metrics?*
▪ It is still a too early to be definitive on which and what type of metrics will be the most pertinent and/or relevant for measuring operational resilience. The following list is intended as illustrative examples that could be used to measure operational resilience: o IT-related metrics such as service level objectives (SLOs) and service level agreements (SLAs), measures of availability of services and speed of recovery. o For third parties, concentration risk metrics, financial health assessments for critical suppliers and general performance metrics based on contractual SLAs. o Fraud related metrics. o Customer sentiment metrics. o Employee absences. o Contact centre performance metrics.