1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

November 5, 2020

Basel Committee on Banking Supervision
Bank for International Settlements
CH-4002 Basel
Switzerland

Response to Consultative Document
Revisions to the Principles for Sound Management of Operational Risk

Ladies and Gentlemen:

The Advanced Operational Risk Group (AORG) of The Risk Management Association is writing to share its observations and suggestions with respect to the Basel Committee's recent Consultative Document release entitled *Revisions to the Principles for the Sound Management of Operational Risk* (PSMOR).

RMA is a 501(c)(6) not-for-profit, member-driven professional association whose sole purpose is to advance the use of sound risk principles in the financial services industry. RMA helps its members use those principles to improve institutional performance and financial stability and enhance the risk competency of individuals through information, education, peer-sharing and networking. RMA has 2,600 institutional members that include banks of all sizes, as well as nonbank financial institutions. They are represented in the Association by more than 16,000 risk management professionals who are chapter members in financial centers throughout North America, Europe, and Asia/Pacific.

The AORG (formerly the AMAG) was formed by RMA in 2005 at the suggestion of the U.S. AMA-BQT (formerly the Inter-Agency Working Group on Operational Risk). The original purpose of the Group was to share industry views on aspects of Advanced Measurement Approaches ("AMA") implementation with the U.S. financial services federal regulatory agencies. Since then the Group has continued in that role, serving as a forum for operational risk practice-sharing and regulatory interface. Membership consists of operational risk

THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

management professionals working at financial service organizations throughout the United States. The AORG is open to any financial institution regulated in the U.S. that is pursuing advanced operational risk measurement and management practices, and/or is required to conduct CCAR / DFAST exercises. A senior officer responsible for operational risk management serves as the primary representative of each member institution on the AORG.

Consistent with the AORG's commitment to conduct regular practice-sharing exercises among the members and pursue an ongoing industry-regulatory dialogue toward the advancement of operational risk management, the Group has conducted a series of working group calls to discuss the BCBS' Consultative Documents. This industry comment letter is being submitted in the spirit of an open and ongoing dialogue with the regulatory community toward advancement of operational risk management and operational resilience practices discussed herein.

There are currently twenty-three (23) members of the AORG at the time of this writing. The members of AORG are listed in Appendix B, along with further background about the Group. The member institution names are provided for identification purposes only. This letter does not necessarily represent the views of RMA's institutional membership at large, or the views of the individual institutions whose staff have participated in the AORG.

General Summary Comments

At a combined high level, AORG offers observations on the Documents about principle-based regulation, integration for comprehensive whole, and appropriate ranges of practice that allow adaptability by unique firms' business operations and risk profiles.

Generally speaking, AORG favors and advocates for principles-based regulatory guidance as opposed to more prescriptive direction that may inadvertently restrict flexibility in aligning to unique corporate cultures and stifle creativity toward risk management solutions. AORG (and its former incarnation as AMAG) has promoted this position since its formation in 2005.

In reviewing the two Documents, AORG finds that while the newly issued Consultative Document on Principles for Operational Resilience strikes a reasonably good balance in that regard, the revised Principles for Sound Management of Operational Risk (PSMOR) is going in the opposite direction, becoming more and more prescriptive with each release. Certainly this 2020 revision is more prescriptive than its 2011 predecessor version.

Such prescriptiveness is counterproductive as banks work to implement their programs in these areas. No two firms are alike in product and service scope, risk profile, culture, management styles and jurisdictional footprint. They should be afforded flexibility to achieve

THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

sound programs in ways best suited to accomplishing the goal of sound risk management. This AORG comment letter, therefore, is generally reflective of this view.

AORG is supportive of the recognized interrelationship between operational risk and operational resilience, along with the Committee's interest in promoting that premise by introducing these two Documents concurrently. The papers seem to leave the disciplines in a somewhat awkward interim state, however. They are recognized as being interrelated, but are not yet fully intertwined or coordinated. The industry is left with redundancy between the papers and some confusion. In essence, AORG would support further integration of and clarity between them.

PSMOR - Summary of Detailed Comments

While AORG generally in agreement with and supportive of the PSMOR and its revisions, it also requests less prescriptiveness overall. As outlined in this comment letter, AORG believes that the Principles are reasonable overall at a high level, but that there are issues with the specific language of some of the detailed support paragraphs.

Of particular concern is the implication in Principle 12 that, whether intended or potentially misinterpreted, one might consider paragraph 62 to suggest the disclosure of legal findings and/or case reserves. AORG requests that language in this paragraph be amended and limited so as to avoid any possibility of misinterpretation or inclusion of confidential legal loss disclosures, including but not limited to reserves. AORG's comments on Principle 12, in the attached, about attorney-client privilege, attorney work product and legal reserves as they have been communicated previously to U.S. regulators. AORG submits that requiring banks to disclose their legal reserves for either pending and probable litigation, or even closed claims would be unwise, unsound and highly prejudicial, and should not be pursued (see detailed discussion in this letter).

Elsewhere, AORG has concerns relative to: (1) implications of framing compliance as a first line of defense (1LOD) control function, and not as part of the 2nd line; as well as details related to the lines of defense (Section 3); (2) quality assurance and validation (Section 3); (3) mandatory training by role (Principle 1); (4) control quality and alignment, documentation for monitoring limits and residual risk , and taxonomy (Principle 2); (5) Board challenge of design and effectiveness (Principle 3); (6) risk appetite, as well as the alignment of legal entities and business units (Principle 4); (7) nuances relative to risk identification and assessment (Principle 6); (8) change management expansion (Principle 7); and (9) metrics relative to emerging risks (Principle 8). AORG also seeks clarifications relative to the role of Supervisors (Principle 12).

THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

Last but not least, as noted above, AORG has some concerns about the redundancy of certain aspects of the Operational Risk and Operational Resilience documents taken together, and would suggest consideration of further integration of certain aspects including, but not limited to, business continuity and change management. Please see AORG's separate response to the BCBS Consultative Document entitled *Principles for Operational Resilience*.

AORG requests consideration of the specific suggestions outlined in this letter. Appendix A contains the Group's specific comments, organized by section and principle.

Respectfully submitted,

Edward J. DeMarco, Jr.,
Chief Administrative Officer & General Counsel

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

Appendix A

AORG - Specific Comments on:
Principles for the Sound Management of Operational Risk (PSMOR)

This appendix addresses AORG's specific concerns relative to the BCBS Consultative Document entitled *Revisions to the Principles for the Sound Management of Operational Risk* that was issued in August 2020. This detailed response should be read in conjunction with the RMA/AORG covering letter dated November 5, 2020.

Section 3 – Operational Risk Management

BCBS Text - Excerpts:

Paragraph 5 of this section reads:

"Banks commonly rely on three lines of defence: (i) business unit management …", and then there is a footnote further referencing "business unit" to mean "broadly to include all associated support, corporate, and/or shared service function, as for example: Finance, Compliance, Legal, Human Resources, Operations and Technology, etc. Risk Management and Internal Audit are not included unless otherwise specifically indicated."

Paragraph 9 of this section reads:

"A functionally independent corporate operational risk function (CORF) is typically the second line of defence. The responsibilities of an effective second line of defence should include …

(b) "Challenging the relevance and consistency of business unit's implementation of the operational risk management tools, measurement activities and reporting systems via a quality assurance programme, and providing evidence of this effective challenge …." [Emphasis added]

AORG Comments – Section 3

AORG offers suggestions relative on Paragraphs 5 and 9, as follows:

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

- *Par. 5 - AORG members note that Compliance is not considered a 1LOD business unit function at most banks regulated in North America and should either be clarified here by jurisdiction, or simply be designated as a 2LOD function.*

- *Par. 9 - The introduction of "a quality assurance programme", without a clear definition or explanation, in addition to already-established challenge, validation and verification practices is potentially problematical. It introduces a separate term and expectation for an additional independent review. AORG respectfully requests that the Committee either leverage the existing expectation of "a validation programme" with further clarification, or eliminate "via a quality assurance programme" from the statement.*

Principle 1 (BCBS Text):

"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….

> Par. 17 – "Senior management should ensure that an appropriate level of operational risk training is available at all levels throughout the organisation, and that customised training programs are mandatory for specific roles, such as heads of business units, heads of internal controls and senior managers. Training provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended…."

AORG Comments – Principle 1

The wording changes to the Sound Principles document of 2011 on this point is generally supportive of a strong accountability approach that begins with the Board and Senior Management. A concern noted by AORG members, however, is the potential challenge presented by an implied requirement to have customized training by role. We suggest adjusting the language in section 17, to reflect the need for appropriate training across the organization. This allows for flexibility to implement without misinterpretation.

Suggested re-phrased paragraph:

- *Par. 17 -- Senior management should ensure that an appropriate level of operational risk training is available at all levels throughout the organization. ~~and that customised training programs are mandatory for specific roles, such as heads of business units, heads of internal controls and senior managers.~~ Training provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended (Revisions: Strikethroughs indicate suggested deletions]*

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

Principle 2 (BCBS Text):

"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….

Par. 22 - "ORMF documentation should clearly…

Sub-part (b) – "Reference the relevant operational risk management policies and procedures …

Sub-part (d) - "Describe the bank's accepted operational risk appetite and tolerance; the thresholds, activity triggers or limits for inherent and residual risk; and the approved risk mitigation strategies and instruments;

Sub-part (e) - "Describe the bank's approach to ensure controls are designed, implemented and operating effectively ….

Sub-part (i) - "Provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives across all business units.[13] The taxonomy can distinguish operational risk exposures by event types, causes, materiality and business units where they occur; it can also flag those 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; … [Emphasis added]

Sub-part (j) - "Provide for appropriate independent review and challenge of the outcomes of the risk management process; and …

Sub-part (k) – "Require the policies to be reviewed and revised as appropriate based on continued assessment of the quality of the control environment addressing internal and external environmental changes or whenever a material change in the operational risk profile of the bank occurs."

AORG Comments – Principle 2

AORG appreciates that the Consultative Document allows for a range of practices, depending on the bank's size, complexity and risk profile, as stated in the introduction to Principle 2. AORG agrees that the Operational Risk Management Framework should be fully integrated into the processes of the bank by the first line of defense, which is where risk management becomes impactful for the organization, and the quality of the implementation is adequately reviewed and challenged by the second line.

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

AORG also agrees that the Operational Risk Management framework should be appropriately documented in board-approved policies, so that each line of defense understands its role and responsibilities in the management of operational risk.

Members suggest, however, that some revisions should be made to Principle 2, as follows.

- *Par. 22 (e and k) -- More flexibility -- The guidance should allow for more flexibility as to how each bank meets these objectives, and that the language as stated in the Consultative Document is too prescriptive. Operational Risk policies should be designed according to the organization's risk profile and establish the high-level framework elements for managing operational risk across the enterprise, while the first line's owned procedures should reflect how the framework is translated and implemented according in each business. Requiring a board-level policy to describe the "bank's approach to ensure controls are designed, implemented and operating effectively" and requiring they are "reviewed and revised as appropriate based on continued assessment of the quality of the control environment" may not be appropriate for every institution, with many documenting control design and implementation in first line owned procedures.*

- *Par. 22 (d) -- Documentation for monitoring limits and residual risk -- In addition, some AORG members believe that the reference to the requirement to include documentation for establishing the monitoring of limits of inherent and residual risk exposure is impractical in the context of operational risk, where there is no risk-reward analysis in the conventional sense. Rather, the analysis is a risk-cost one, where it needs to be determined how deeply an institution will invest in its control infrastructure in order to mitigate operational risk.*

  AORG suggests at least revising the language to include the word "material" such as "… risk appetite and tolerance; the thresholds, material activity triggers or limits for inherent and residual risk …." [Emphasis added]

- *Par. 22(i) -- Taxonomy -- Finally, a board-approved policy should include the requirement to maintain an operational risk taxonomy for indexing loss events and establishing the firm's risk profile, but there should be flexibility in how the taxonomy is designed. The requirement to maintain a taxonomy that is linked to event types, causes, materiality and business units where they occur would create a very inflexible schema that would likely be difficult to maintain over time.*

Governance

The Board of Directors

Principle 3 (BCBS Text):

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

"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.

Par. 23 - "The board of directors should:

Subsection (a) - "Ensure that the bank has adequate processes for understanding the nature and scope of the operational risk inherent in the bank's current and planned strategies and activities …

Subsection (c) - "Provide senior management with clear guidance regarding the principles underlying the ORMF, and ensure that corresponding policies developed by senior management are aligned with these principles;

Subsection (d) - "Regularly challenge senior management on the design and effectiveness of the bank's ORMF and approve and review the ORMF to ensure the bank has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes or systems, including changes in risk profiles and priorities (e.g., changing business volumes) …. [Emphasis added]

Par 24 – "Strong internal controls are a critical aspect of operational risk management. The board of directors should establish clear lines of management responsibility and accountability for implementing a strong control environment. Controls should be regularly reviewed, monitored, and tested to ensure ongoing effectiveness. The control environment should provide appropriate independence/separation of duties between operational risk management functions, business units and support functions." [Emphasis added]

AORG Comments – Principle 3

Overall, AORG is supportive of Principle 3 and its guidance. The Group suggests clarification, however, of the following points:

- *Par 23(a) – AORG notes that the words "establish a management culture…." has been removed from the Board of Directors' responsibilities. Members request clarification as to why this reference to risk culture was removed.*

- *Par. 23 (c) -- In the current Principle, "provide senior management with clear guidance and direction regarding the principles underlying the ORMF", the associated words "approve the" that appeared before "the corresponding policies developed by senior management …", were removed from the previous*

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

version. Some AORG members are seeking clarification of this deletion and whether this is intended to suggest that the Board is no longer required to approve corresponding policies. [Emphasis added]

- *Par. 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 defense using a variety of techniques and tools, in addition to operational risk data. [Emphasis added]*

  In the context of this paragraph, AORG members request clarification as to how the BCBS envisions Boards of Directors perform and evidence "challenge". Members would not expect that this reference is intended to imply that the Board perform similar activities, or apply similar techniques, to those typically associated with the second line of defense.

  In addition, and more specifically, AORG members do not believe that it is characteristic or an appropriate role for the Board of Directors to be expected to challenge the design of the ORMF. Rather, it would be more logical to expect their review and evaluation of its effectiveness.

- *Par. 24 – This section states that "…Controls should be regularly reviewed, monitored, and tested …." [Emphasis added] AORG requests clarification that this statement is not referring to independent Operational Risk Management inasmuch as this testing role is typically performed by Compliance and the 3LOD. AORG also notes that firms often relay on metrics in performing this role and seeks clarification that this could be a reasonable substitute.*

Principle 4 (BCBS Text):

"The board of directors should approve and periodically review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk the bank is willing to assume.

Par 25 – "The risk appetite and tolerance statement for operational risk should be developed under the
authority of the board of directors and linked to the bank's short- and long-term strategic and
financial plans. Taking into account the interests of the bank's customers and shareholders as well as regulatory requirements, an effective risk appetite and tolerance statement should …

> sub-part (d) – "Ensure the strategy and risk limits of each business unit and legal entity, as relevant, align with the bank-wide risk appetite statement; [Emphasis added]

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

sub-part (e) – "Be forward-looking and, where applicable, subject to scenario and stress testing to ensure that the bank understands what events might push it outside its risk appetite and tolerance statement." [Emphasis added]

AORG Comments – Principle 4

AORG views Principle 4 and its revisions and edits since the 2011 version of PSMOR to be reasonable for the most part. AORG has the following specific comments:

- *Part 25(d) – "Ensure the strategy and risk limits of each business unit and legal entity, as relevant, align with the bank-wide risk appetite statement…" [Emphasis added]. The word ensure would be difficult if not impossible to satisfy. AORG suggests substituting the words 'endeavor to' instead.*

  Also, the word 'each' is particularly problematical. Some firms have thousands of legal entities and/or business units. AORG suggests replacing it with the word 'material' (i.e., "… and risk limits of material business unit and legal entity …").

- *Par 25(e) – "… an effective risk appetite and tolerance statement should: … (e) Be forward-looking and, where applicable, subject to scenario and stress testing to ensure that the bank understands what events might push it outside its risk appetite and tolerance statement."*

  This language raises the bar to a problematically challenging degree. Linking risk appetite to scenario analysis would be challenging combination given the manner that scenario analysis is already a program that is being used for multiple purposes (capital calculation, stress testing, operational resiliency, business continuity, etc.) Keeping Scenario analysis in sync across objectives and assumptions is already challenging. Linking an additional requirement to Scenario analysis could dilute the focus of scenario exercises and potentially negatively impact their overall usefulness.

Senior Management

Principle 5 (BCBS Text):

"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,

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

processes and systems consistent with the bank's risk appetite and tolerance statement.

> Par. 27 – "Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes. These should include systems to report, track and, when necessary, escalate issues to ensure resolution. Banks should be able to demonstrate that the three-lines-of-defence approach is operating satisfactorily and to explain how the board of directors, independent audit committee of the board, and senior management ensure that this approach is implemented and operating in an appropriate manner….
>
> Par. 32 – "A bank's governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, a bank should take the following into consideration …
>
> > Sub-part (b) - "Committee composition – Sound industry practice is for operational risk committees (or the risk committee in smaller banks) to include members with a variety of expertise, which should cover financial activities, legal, technological and regulatory matters, and independent risk management; and …."

AORG Comments – Principle 5

AORG offers the following specific suggestions for improvement:

- *Par. 27 – AORG suggests that consideration be given to the updated 3-line-of-defense model proposed by the Institute of Internal Audit (IIA)[1], which has softened the demarcation between the first and second lines of defense. The current expectation seems to be for an adversarial relationship between the first and second line, casting the second line as more of an audit function. Whereas, the IIA update states "First and second line roles may be blended or separated. Some second line roles may be assigned to specialists to provide complementary expertise, support, monitoring, and challenge to those with first line roles."*

- *Par. 32(b) – This paragraph discusses the sound practices for Committee Composition. The 2020 revision has removed the "expertise in business activities" from the mix of committee membership. In AORG's view, it is crucial to have expertise in business activities on the committee.*

[1] *IIA Exposure Document: Three Lines of Defense*, June 2019.

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

Identification and Assessment

Principle 6 (BCBS Text):

"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.

Par. 34 – "Examples of tools used for identifying and assessing operational risk include:

Sub-part (a) – "Operational risk event data – Banks often maintain a comprehensive operational risk event dataset that collects all material events experience by the bank and serves as basis for operational risk assessments. The event dataset typically includes …

Sub-part (b) - "Self-assessments – Banks often perform self-assessments of their operational risks and controls on various different levels. The assessments typically evaluate inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered) and contain both quantitative and qualitative elements. The qualitative element reflects consideration of both the likelihood and consequence of the risk event in the bank's determination of its inherent and residual risk ratings. The assessments may utilise business process mapping to identify key steps in business processes, activities, and organisational functions, as well as the associated risks and areas of control weakness. The assessments contain sufficiently detailed information on the business environment, operational risks, underlying causes, controls and evaluation of control effectiveness to enable an independent reviewer to determine how the bank reached its ratings. A risk register can be maintained to collate this information to form a meaningful view of the overall effectiveness of controls and facilitate oversight by senior management, risk committees, and the board of directors. [Emphasis added]

Sub-part (c) - "Event management – When banks experience an operational risk event, the process of identification, analysis, end-to-end management and reporting of the event follows a predetermined set of protocols. A sound event management approach … [Emphasis added]

Sub-part (g) "Benchmarking and comparative analysis - Benchmarking and comparative analysis are comparisons of the outcomes of different risk measurement and management tools deployed within the bank, as well as comparisons of metrics from the bank to other firms in the industry. Such comparisons can be performed to enhance understanding of the bank's operational risk profile. For example, comparing the frequency and severity of internal losses with self-assessments can help the bank determine whether its self-assessment processes are functioning effectively. Scenario

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

data can be compared to internal and external loss data to gain a better understanding of the severity of the bank's exposure to potential risk events." [Emphasis added]

AORG Comments – Principle 6

Principle 6 was significantly updated and expanded. Generally speaking, AORG members do not have major concerns with the content of this Principle inasmuch as some of the updates provide clearer explanations. Members have concerns about its prescriptiveness, however. The revisions here are particularly indicative of a move further away from a principle-based document to one that is more characteristic of directive guidance. This principle seems to transition from 'what' is expected to 'how' the tools should be designed and executed.

- *Par. 34 (c) -- Certain institutions consider "Event Management" a part of their "Operational Risk Event Data" program. The committee could consider combining these into a single sub-paragraph.*

- *Par. 34 (b)- A reference to process mapping has been included within the "Self-assessment paragraph. Consideration should be given to keeping this reference as flexible as possible. AORG suggests revising the language as follows: "The assessments may utilise business process mapping or other methods to identify key steps in the business process …."~~"Process Mapping" a separate sub-paragraph as it is foundational to Operational Resilience programs, and those Operational Resilience programs will serve as an excellent tool for risk identification and assessment going forward.~~ [Strikethroughs indicate suggested deletions]*

- *Par. 34(b) -- While the "Self-Assessment" sub-paragraph may have been intended to capture it, "New Initiative/Business Risk Assessment" program contributes greatly to emerging risk identification and assessment and may warrant being addressed separately.*

- *Par. 34(g) -- Additional detail is needed for "comparisons of metrics from the bank to other firms in the industry." On the face of it, this seems clear enough, and in North America, AORG, ABA, ORX benchmarking provide good sources for some comparisons, however these sources are generally loss or capital oriented. It is not practical to require that firms benchmark metrics to one another. There are no such public – formal or informal -- sources available at the present time.*

Principle 7 (BCBS Text):

"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. [Emphasis added]

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

Par. 36 - "In general, a bank's operational risk exposure evolves when a bank initiates change, such as engaging in new activities or developing new products or services; entering into unfamiliar markets or jurisdictions; implementing new or modifying business processes or technology systems; and/or engaging in businesses that are geographically distant from the head office. Change management should assess the evolution of associated risks across time, from inception to termination (i.e., throughout the full life-cycle of a product). [Emphasis added]

Par. 37 - "A bank should have policies and procedures defining the process for identifying, managing,
challenging, approving and monitoring change on the basis of agreed objective criteria. Change implementation should be monitored by specific oversight controls. Change management policies and procedures should be subject to independent and regular review and update, and clearly allocate roles and responsibilities in accordance with the three-line-of-defence model, in particular:

> Sub-part (a) - "The first line of defence should perform operational risk and control assessments of new products and initiatives.
>
> Sub-part (b) - "The second line of defence (CORF) should challenge the operational risk and control assessments of first line of defence, as well as monitor the implementation of appropriate controls or remediation actions. CORF should cover all phases of this process, from the identification and evaluation of the required change, through the decision-making and planning phases, to the implementation and post-implementation review. In addition, CORF should ensure that all relevant control groups (e.g., finance, compliance, legal, business, ICT, risk management) are involved as appropriate.

Par. 38 - "A bank should have policies and procedures for the review and approval of new products,
activities, processes and systems. The review and approval process should consider:

> sub-part (f) -- "The procedures and metrics to assess, monitor, and manage the risk of new products, services, activities, markets, jurisdictions, processes and systems.

Par. 39 - "The review and approval process should include ensuring that appropriate investment has been made for human resources and technology infrastructure before changes are introduced. Changes should be monitored, during and after their implementation, to identify any material differences to the expected operational risk profile and manage any unexpected risks…." [Emphasis added]

AORG Comments – Principle 7

AORG members are generally in agreement with the inclusion of a principle on change management as a recognition that the activity has assumed a far more prominent place in operational risk management.

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

Change management has different meanings for different institutions, however, and Principle 7 would benefit from requesting that each institution establish a clearly articulated definition of change. The reference to "continuous risk and control assessments" in the BCBS description of Principle 7 would be challenging for banks to implement without understanding what it means and when implemented (i.e., when "enough is enough"). AORG suggests that the word "continuous" be replaced by "regular" or "regularly scheduled." Overall, this would be a difficult process for a bank to implement and should require a risk-based approach.

AORG members have the following suggestions for improving this Principle and its sub-sections:

- *Principle 7 – AORG suggestion for revision: Senior management should ensure that the bank's change management process appropriately defines change in its own context, is ~~is comprehensive~~, appropriately resourced and includes periodic ~~continuous~~ risk-sensitive ~~and control~~ re-assessments, adequately articulated between the relevant lines of defense. (Revisions: additions underlined / Strikethrough indicates suggestion deletions).*

- *Par. 36 -- The requirement to assess the evolution of change management-related risk over time would also benefit from additional context. What change management-related risks are being referenced here? Is it any risk that is associated with a change in the risk profile of the firm, projects and initiatives, firm-wide strategies, or something else? As stated above, it is vitally important for each institution to establish a definition of change and to document the scope of what is included in its management.*

- *Par. 37 – AORG does not agree with the roles of the first and second line of defense as described in this section. While the second line should be responsible for oversight and review and challenge, the first line should own many of the change management activities. AORG believes that some of the activities mentioned in this section, including the identification and evaluation of the required change, decision-making, planning and post-implementation reviews belong with the business and first line of defense.*

- *Par. 38 (f) – This paragraph calls for "… procedure and metrics to assess, monitor and manage the risk of new products services, activities, markets, jurisdictions, processes and systems." [Emphasis added] It is unclear what metrics would be applied for emerging and unknown risk emanating from change. Given that such metrics would be difficult to identify, they certainly will be difficult to demonstrate compliance with. AORG members suggest deleting the words "and metrics" referenced above.*

- *Par. 39 -- This section would also benefit from a revision in the language regarding the approval process and the requirement to ensure that the appropriate investment has been made in human resources and technology infrastructure. AORG is suggesting that the language should be changed to "will be made" because part of the change management process associated with new initiatives is an initial impact analysis of what investments will be needed for success.*

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

Monitoring and Reporting

Principle 8 (BCBS Text):

"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.

> Par. 41 -- "Banks should continuously improve the quality of operational risk reporting. A bank should
> ensure that its reports are comprehensive, accurate, consistent and actionable across business units and products. To this end, the first line of defence should ensure reporting on any residual operational risks, including operational risk events, control deficiencies, process inadequacies, and non-compliance with operational risk tolerances. Reports should be manageable in scope and volume by providing an outlook on the bank's operational risk profile and adherence to the operational risk appetite and tolerance statement; effective decision-making is impeded by both excessive amounts and paucity of data…. [Emphasis added]
>
> Par. 43 - "Operational risk reports should describe the operational risk profile of the bank by providing internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making. Operational risk reports should include:
>
> > Sub-part (a) - "Breaches of the bank's risk appetite and tolerance statement, as well as thresholds, limits or qualitative requirements;
> >
> > Sub-part (b) - "A discussion of key and emerging risk assessed and monitored by metrics; [Emphasis added]
> >
> > Sub-part (c) - "Details of recent significant internal operational risk events and losses (including root cause analysis);
> >
> > Sub-part (d) - "Relevant external events or regulatory changes and any potential impact on the bank…." [Emphasis added]

AORG Comments – Principle 8

AORG agrees that reporting is key at all levels. The sub-part details of this principle are written, however to a level of detail that will be very difficult to meet. In particular, repeated use of the word 'should' make the principle and its subpart make this section very prescriptive, and leave little room for flexibility and adaptability, and are therefore problematical. Examples:

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

- *Par 41 – The requirement that "banks should continuously improve the quality of operational risk reporting" language is problematical. AORG members request clarification as to how one would one measure this improvement. [Emphasis added]*

- *Par 43(b) – "Operational risk reports should include: … emerging risks assessed and monitored by metrics." AORG requests clarification of this point. It is unclear how one would monitor emerging risks by metrics or what metrics one would use.*

- *Par 43(d) -- "Operational risk reports should include: … regulatory change and any potential impact on the bank …" This not likely plausible given volume of regulatory changes and impact. It also begins to blur the roles of Operational Risk Management and Compliance and could present legal entanglements in assessing impact if taken by monetary value.*

Repeated use of the word "should" is particularly problematical in this section, and is generally an indication of the amount of prescriptiveness in the document. AORG respectfully requests limiting its use.

Control and Mitigation

Principle 9 (BCBS Text):

"Banks should have a strong control environment that utilizes policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies….

> Par. 54 -- "Banks should have unified classification, methodology, procedures of operational risk management established by the CORF."

AORG Comments – Principle 9

While a great deal of detail underlying this Principle, AORG members do not see them as new or particularly controversial.

- *Par. 54 - The last paragraph, however, may be worthy of note. It states that "Banks should have unified classification, methodology, procedures or operational risk management established by the CORF" may actually be helpful to operational risk practitioners. This item speaks to the issue of taxonomy, which is always a challenge. Creating and maintaining a taxonomy requires many other*

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

people and groups within a bank to coordinate toward making progress. AORG members request further clarification, however, on this point.

Information and communication technology

Principle 10 (BCBS Text):

"Banks should implement robust ICT[23] 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….

Par. 56 - "To ensure data and systems' confidentiality, integrity and availability, the board of directors and the senior management should routinely evaluate the design, implementation and effectiveness of the ICT framework. This requires regular alignment of the business, risk management and ICT strategies to be consistent with the bank's risk appetite and tolerance statement as well as with privacy and other applicable laws. Banks should continuously monitor its ICT and regularly report to senior management on ICT risks, controls and events. [Emphasis added]

Par. 57 - "The ICT framework together with complementing processes set by the banks should:

> Sub-part (a) - "Be reviewed on a regular basis for completeness against relevant industry standards and best practices as well as against evolving threats (e.g., cyber) and evolving or new technologies …."

AORG Comments – Principle 10

This Principle is entirely new in the 2020 Document and is generally viewed by AORG members as a positive addition, which is reflective of changes already taking place in the industry. Specific comments follow:

- *Par. 56 – "To ensure data and systems' confidentiality, integrity and availability, the board of directors and the senior management should routinely evaluate the design, implementation and effectiveness of the ICT framework." [Emphasis added]. Once again, AORG members believe that it is unreasonable to expect the board of directors to have expertise to evaluate the design of the ICT*

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

framework, inasmuch as this is a management role. AORG suggests that this particular Board level evaluation roles be eliminated.

- *Par. 57(a) – "The ICT framework, together with complementing processes set by the banks, should: (a) Be reviewed on a regular basis for completeness against relevant industry standards and best practices as well as against evolving threats (e.g., cyber) and evolving or new technologies …." AORG is seeking clarity, but not prescriptiveness or directives, as to what the Committee would consider to be relevant standards in this case.*

Business continuity planning

Principle 11 (BCBS Text):

"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.[24]

Par. 58 - "Sound and effective governance of banks' business continuity policy[25] requires:

Sub-part (a) "The validation and regular review by the board of directors … [Emphasis added]

Par. 59 - "Banks should prepare forward-looking business continuity plans (BCP) with scenario analyses associated with relevant impact assessments and recovery procedures….

Sub-part (c) "Each disruption scenario should be subject to thresholds or limits (such as maximum tolerable outage) 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.

Par. 60 -- "A bank should periodically review all components of its business continuity 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 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 reported to senior management and the board of directors." [Emphasis added]

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

AORG Comments -- Principle 11

AORG members are generally supportive of this principle. As discussed in our introductory comments, this is a point at which the PSMOR and Principles on Operational Resilience should be better aligned and integrated. As for the subpart details:

- *Par. 58(a) calls for "validation and regular review" of banks' "business continuity policy" by the Board, but it is unclear what would be involved in these activities. AORG members request clarification, particularly with respect to use of the word 'validation'. Members note that the word is used only on a few occasions in the entire Consultative Document.*

- *Par. 59(c) may be rather difficult to comply with as written and are excessively prescriptive in the context of a principle-based approach. At a minimum AORG suggests that the language "Each disruption scenario ..." should be replaced with "Each critical disruption scenario involving important business services …" [Emphasis added]*

- *Par. 60 -- To perhaps a somewhat lesser degree, members also note that Paragraph 60, and the words "A bank should periodically review all components of its business continuity policy …" [Emphasis added] could be subject to misinterpretation. AORG members suggest language such as "…periodically review critical components of its …."*

Role of Disclosure

Principle 12 (BCBS Text):

"A bank's public disclosures should allow stakeholders to assess its approach to operational risk management and its operational risk exposure….

Par. 62 - "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).[26] A bank should disclose its ORMF in a manner that allows stakeholders to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively." … [Emphasis added]

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

Role of supervisors

Par. 64 - "Supervisors should regularly assess banks' ORMF by evaluating banks' policies, processes and systems related to operational risk. Supervisors should ensure that there are appropriate mechanisms in place allowing them to remain apprised of banks' operational risk developments.

Par. 65 - "Supervisory evaluations of operational risk should include all areas described in the principles for the sound management of operational risk. Where banks are part of a financial group, supervisors should ensure that there are processes in place to ensure that operational risk is managed in an appropriate and integrated manner across the group. In assessing banks' ORMF, cooperation and exchange of information with other supervisors, in accordance with established procedures, may be necessary.[27] In certain circumstances, supervisors may choose to use external auditors in these assessment processes. [Emphasis added].

Par. 66 - "Supervisors should take steps to ensure that banks address deficiencies identified through the supervisory review of banks' ORMF. Supervisors should use the tools most suited to the particular circumstances of banks and their operating environment. To ensure that supervisors receive current information on operational risk, supervisors may wish to establish reporting mechanisms directly with banks and external auditors (e.g., internal bank management reports on operational risk could be made routinely available to supervisors)…." [Emphasis added]

AORG Comments – Principle 12

Although in agreement with Disclosures and the Role of Supervisors in principle, once again some details are potentially problematical and both the industry and regulatory community would benefit from clarifying revisions, as follows.

- ***Par. 62 - Whether intended, or potentially misinterpreted, one might consider the reference in paragraph 62 to include legal findings and/or case reserves. AORG requests that language in this paragraph be amended and limited so as to not be misinterpreted as a requirement to include confidential legal loss disclosures, including but not limited to, legal reserves. See below for AORG's position, as it has been communicated previously to U.S. regulators on this point.***

Disclosure of Legal Reserves

The AORG reiterates its strong support of the preservation of the attorney-client privilege and work product doctrine and opposes governmental policies, practices and procedures that have the effect of the eroding the privilege or doctrine. Any attempt to include illegal reserve information is a case in point.

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

As RMA has previously stated, as indicated above, a financial institution or other corporate defendant upon being sued undertakes a litigation assessment, which is tantamount to the lawyer's underlying thinking about the case. At the outset, counsel will evaluate the case from multiple perspectives, including, management's; the business unit's; the public's; the regulators'; and the lawyers'. Counsel will consider the type of case, whether the corporate defendant is the sole defendant or whether there are multiple defendants; what the key issues are; who the plaintiff is; whether there are similar cases and the outcome of such cases.

The attorney-client privilege enables corporations and other limited liability entities, through their employees, to communicate with their lawyers in confidence, and it encourages corporations to seek out and obtain guidance in how to conform their conduct to the law. A privilege facilitates self-investigation into past conduct to identify shortcomings and remedy problems, to the benefit of corporate institutions, the investing community and society at large. The work product doctrine underpins our adversarial justice system and allows attorneys to prepare for litigation without fear that their work product and mental impressions will be revealed to adversaries. The lawyers the evaluation of the case will shape his or her litigation strategy and budget.

Member institutions believe that including legal reserve information in public disclosures would be highly problematical not merely because of the attorney-client privilege and the attorney work product doctrine but also because, by definition, they consist of loss events that have been reserved for, but have not been settled or fully and finally adjudicated. In particular, the AORG members' legal departments concerns center around discoverability of the information once released in regulatory reports. Discovery of such information would quite possibly compromise an institution's legal position if it became known.

The AORG submits that requiring banks to disclose their legal reserves for either pending and probable litigation, or even closed claims would be unwise, unsound and highly prejudicial, and should not be pursued. Legal reserves for litigation claims are established by banks in receiving legal advice from their legal counsel and often, if not always, entail the exercise of significant professional judgment by experienced legal counsel in weighing the relative strengths of claims and defenses in light of existing law and factual developments. Hence, legal reserves are both privileged and highly confidential. Any public disclosure of legal reserves would subject banks to significant prejudice, as it would both inform their adversaries of how the bank weighs the strengths/weaknesses of the subject claims and establish a floor for plaintiffs' settlement demands on those claims.

AORG Comments – Principle 12, the Role of Supervisors

Overall, AORG is supportive of the role of supervisors in assessment of the ORMF and its supporting policies, processes and systems. We further agree that banks should establish mechanisms to apprise supervisors of ongoing developments. With that said, AORG believes that increased clarity may be required in several areas since the revised principles establish expectations for embeddedness of the ORMF across all levels of the

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

organization. As such, this will accentuate the need for cooperation amongst supervisors, e.g. amongst home and host countries:

- *The original High-level principles for the cross-border implementation of the New Accord and the Principles for home-host supervisory cooperation and allocation mechanisms in the context of Advanced Measurement Approaches (AMA) established expectations for approval of certain approaches. Given the expansion of the principles relative to the referenced papers, AORG respectfully requests that the Committee provide incremental guidance on what aspects of the revised principles and associated ORMF may require approval from relevant host country supervisors in addition to home country supervisors. Further, AORG requests that the Committee confirm that home country supervisors will continue to have final determination on matters related to the ORMF and its assessment across the group to the extent allowable by local law.*

- *Par. 65, it is noted that "Supervisory evaluations of operational risk should include all areas described in the principles for the sound management of operational risk." Given the breadth of the principles established and reference in the document to implementation across the organization, AORG respectfully requests that the Committee add its insights on expectations, if any, on the review schedule expected, and whether the assessment will look at all businesses or those deemed material.*

- *Par. 66, it is noted that "Supervisors should use the tools most suited to the particular circumstances". AORG requests that the Committee provide added insights into the tools being considered.*

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

Appendix B

The Advanced Operational Risk Group (AORG)

AORG was formed in 2005 as the AMA Group by The Risk Management Association (RMA) at the suggestion of senior U.S. regulators. RMA is a member-driven professional association whose purpose is to advance the use of sound risk management principles in the financial services industry.

AORG's mission is to conduct regular practice-sharing exercises among members, and pursue an ongoing industry-regulatory dialogue toward the advancement of operational risk management. In fulfilling its mission, AORG sponsors a series of working groups, periodic range-of-practice surveys, and roundtable discussions. AORG consists of operational risk management professionals working at financial service organizations operating in the United States. Institutional membership in the AORG is by arrangement with RMA, and is open to any financial firm regulated in the U.S. that is pursuing advanced operational risk measurement and management practices, and/or is required to conduct CCAR / DFAST exercises. A senior officer responsible for operational risk management serves as the primary representative of each member institution on the AORG.

Since its inception, the Group has supported advanced operational risk management and the fundamental goals of improving operational risk management practice and ensuring capital adequacy. To achieve these goals AORG has promoted the view that regulatory agencies must address two broad themes as they continue to move from policy development to supervisory and examination practice, including: 1) Operational risk regulation should remain principles-based vs. prescriptive in nature; and 2) A proper balance between management and measurement should be maintained.

There are currently twenty-three (23) institutional members of AORG. They are listed below.

Bank of America
Bank of the West
BMO Financial
BNY Mellon
Capital One Bank
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC North America
JP Morgan Chase
Keycorp
M&T Bank
Morgan Stanley
MUFG Union Bank
Northern Trust
PNC Financial
Royal Bank of Canada
State Street
TD Bank Financial Group
Truist
US Bank
Wells Fargo

Support for AORG is provided by RMA and Operational Risk Advisors LLC

1801 Market Street, Suite 300 •
Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

November 2020