THE RISK MANAGEMENT ASSOCIATION

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
Principles for Operational Resilience

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 *Principles for Operational Resilience*.

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 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 intentionally or 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 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.

THE RISK MANAGEMENT ASSOCIATION

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

Operational Resilience – Summary of Detailed Comments

AORG is generally in agreement with the content of the Operational Resilience Document. Members support the Committee's high-level aims of pragmatism (see par. 11); principle-based expectations and proportionality; generally applaud their recognition that an entirely new framework for operational resilience is unnecessary; agree that the Operational Risk Management Framework (ORMF) is a logical foundation upon which to build; agree with the Committee's view on collective consideration of otherwise discrete guidance (par 9); and support a view on harmonization with Recovery and Resolution Planning (RRP) to avoid duplication of effort and drive consistency/efficiency (par. 10 and 21). AORG also concurs with the view that tone-from-the-top is fundamental to effective implementation, both as a COVID-19 lesson and to embed this initiative within the book of existing priorities (par 20).

AORG members request clarification (par. 80 that Operational Resilience is the management of a subset of a wider operational risk taxonomy to avoid blurring that issue.

In terms of material concerns with the document, AORG members sense that it (par. 8-11) should advocate sector-wide collaboration and action (per the BoE) for this to be effective; currently it implies that each bank can resolve this in isolation. Second, the Document should indicate how the Principles deliver a distinct outcome and link together (par. 16), whether in sequence or as concurrent activities. Third, that tolerance for disruption should be agnostic as to cause (scenario) (i.e., eliminate lists) (par 17); however, AORG agrees that Board should have assurance that a range of scenarios have been designed and examined (par. 1), and that tolerance can be met across this range.

Last but not least, as noted, AORG has some concerns about the redundancy of certain aspects of the Operational Risk and Operational Resilience documents taken together and, in particular, suggests consideration of further integration of certain aspects including, but not limited to, business continuity and change management. Please also see AORG's separate response to the BCBS Consultative Document entitled *Revisions to the Principles for the Sound Management of Operational Risk* (PSMOR).

AORG also 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 Operational Resilience

This appendix addresses AORG's specific concerns relative to the BCBS Consultative Document entitled *Principles for Operational Resilience*, which was issued in August 2020. This detailed response should be read in conjunction with the AORG covering letter dated November 5, 2020.

AORG Comments by Principle

Principle 1 (BCBS Text):

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

> Par. 17 – "The board of directors should review and approve the bank's operational resilience expectations considering the bank's risk appetite, risk capacity and risk profile. In formulating the bank's risk tolerance for disruption to its critical operations, the board of directors should consider a broad range of severe but plausible scenarios (e.g., lockdown due to pandemics, destructive cyber security incidents, catastrophic natural disasters, etc.). …
>
> Par. 20 – "The board of directors should take an active role in establishing a broad understanding of 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."

AORG Comments – Principle 1

In general, the AORG membership is in agreement with this principle, but has some concerns about the references to Board roles and responsibilities in three sub-paragraphs (Par. 17 and 20). In particular, AORG suggests greater clarity, especially the amount of information and reporting that the Board must consider and digest. Also:

- *Par. 20 – Active vs. Oversight: Practically speaking there is also only so much that can be assigned to the Board as an active vs. an oversight role, and that most suggestions of active management by the Board be eliminated and addressed instead by bank management. AORG finds the "active role in establishing a broad understanding" (Par 20) to the most logical and highest priority of the 3 paragraphs and Board roles. AORG supports the view that tone-from-the-top is fundamental to effective implementation, both as a COVID lesson and to embed this initiative within its agenda of existing priorities.*

- *Par. 17 - With reference to this paragraph, AORG notes the limitation and inflexibility that lists produce and, therefore suggests that ~~(e.g., lockdown due to pandemics, destructive cyber security incidents, catastrophic natural disasters, etc.)~~. be removed from this paragraph. AORG believes that tolerance for disruption should be agnostic to cause (scenario). With reference also back to paragraph 1 of the Consultative Document, however, AORG agrees that the Board should have assurance that a range of scenarios that has been designed and examined and that that tolerance can be met across this range. [Strikethroughs indicate suggested deletions]*

Principle 2 (BCBS Text):

"Banks should leverage their respective functions for the management of operational risk to identify the 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.

> Par. 21 – "The bank's operational risk management function should work alongside other relevant functions to manage and address any risks that threaten the delivery of critical operations. 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."

AORG Comments -- Principle 2

AORG members generally support the alignment of operational resilience to operational risk management. In terms of specifics:

- *Par. 21 – AORG calls out its support for the reference to appropriate coordination with "…other relevant risk management frameworks" and "harmonization in delivering a consistent approach to operate resilience across the enterprise" in order to avoid duplication of effort and drive consistency / efficiency.*

- *Par. 21 – Once again, the Group suggests avoiding the limitations of finite lists however, such as in Par. 21, and suggests deleting the words ~~business continuity planning third-party dependency management, recovery and resolution planning and~~ [Strikethroughs indicate suggested deletions]*

Principle 3 (BCBS Text):

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

> Par. 24 – "An effective business continuity plan should be forward-looking when assessing the impact of potential disruptions. Business continuity exercises[17] should be conducted and validated for a range of severe but plausible scenarios that incorporate disruptive events and incidents.
>
> Par. 25 –"An effective business continuity plan should identify critical operations, key internal and external dependencies to assess the risks and potential impact of various disruption scenarios on operations and ensure appropriate resilience levels. These plans should incorporate business impact analyses, recovery strategies and business continuity plans as well as testing programmes, training and awareness programmes, and communication and crisis management programmes."

AORG Comments -- Principle 3

AORG is in agreement with this principle, but members have concerns about overlap between PSMOR Principle No. 11 on Business Continuity Planning and this Principle No. 3 on Business Continuity Planning and Testing that may give rise to confusion.

In addition, AORG has specific suggestions, including:

- *Par 24 – AORG suggests striking the words "forward looking" because this would be difficult if not impossible to demonstrate.*
- *Par 24 – AORG members suggest clarification of the use of the word validation. It is not at all clear what validation would consist of here, whether it be its scope, breadth and/or limitations.*
- *Par 25 – AORG suggests revising this language to include "components such as …"*

Principle 4 (BCBS Text):

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

Par. 30 – "Internationally active banks may leverage their recovery and resolution plans for definitions of critical operations and should consider whether their operational resilience efforts are appropriately harmonised with the organisational mappings of critical operations and critical third-party services contained in their recovery and resolution plans.

Par. 31 – "The approach and level of granularity of mapping should be sufficient for banks to identify vulnerabilities and to support testing of their ability to stay within the bank's risk tolerance for disruption considering the bank's risk appetite, risk capacity and risk profile."

AORG Comments – Principle 4

This principle promotes the tracing of "relevant internal and external interconnections and interdependencies to set operational resilience expectations…." The difficulty, however, is that it makes specific use of the term "mapping" to achieve this goal. Industry practitioners have encountered challenges with regard to mapping exercises. Their reality encountered by many has been that mapping exercises are typically very detailed take significant time to complete, where in contrast organizational and operational change is ongoing. Such changes all too often take place before the mapping exercise can be completed. In fact, mapping is but just one means of achieving the goal of understanding and addressing interdependencies.

AORG members suggest abandoning the specific use of the term "mapping" in this context. Other terms, such assessment, could achieve a comparable regulatory objective. That is:

- *For the subsection title, AORG members suggest using "Assessing interconnections and interdependencies" rather than "Mapping interconnections and interdependencies"*
- *Par 30 – Use "assessments" rather than mapping*
- *Par 31 – Suggest "granularity of assessments" rather than "granularity of mapping"*

Principle 5 (BCBS Text):

"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.

Par. 32 – "The *respective functions* should perform a risk assessment and due diligence before entering into arrangements including those of, but not limited to, third parties or intra-group entities, consistent with the bank's operational risk management framework,[19] outsourcing/third-party risk management policy and operational resilience expectations. Prior to the bank entering into such an arrangement, the bank should verify whether the third party, including, if relevant, the intra-group entity to these arrangements has at least equivalent operational resilience conditions to safeguard the bank's critical operations.

Par. 33 – "Banks should formalise their relationships with third parties and intra-group entities through written agreements which should cover how to maintain operational resilience in both normal

circumstances and in the event of disruption. These written agreements should reflect: the *respective functions'* due diligence; banks' supervisory and resolution authorities' access to third parties; and the bank's operational resilience expectations."

AORG Comments – Principle 5

Here, again, the AORG is generally in agreement with this principle, but some of its details are problematical. For instance, paragraph 32 states that "Prior to the bank entering into such an arrangement, the bank should verify whether the third party including, if relevant, the intra-group entity to these arrangements has at least equivalent operational resilience conditions to safeguard the bank's critical operations." [Emphasis added]

The word "equivalent" in this context is vague, and the reality is that these "equivalent operational resilience conditions" would be difficult, if not impossible to measure.

AORG instead suggests re-wording such as:

- *Par 32 -The respective functions should perform a risk assessment and due diligence before entering into arrangements including those of, but not limited to, third parties or intra-group entities, consistent with the bank's operational risk management framework, outsourcing/third-party risk management policy and operational resilience expectations. Prior to the bank entering into such an arrangement, the bank should assess and identify ~~verify~~ whether the third party, including, if relevant, the intra-group entity to these arrangements has effective risk management policies and practices to support the bank in safeguarding critical operations, and consistent with its risk appetite. ~~at least equivalent operational resilience conditions to safeguard the bank's critical operations.~~ [Revisions: additions are underlined. Strikethroughs indicate suggested deletions.]*

- *Par 33 – AORG members question the practicality of the specifics in this paragraph and suggest that the opening sentence include the word "endeavor" in recognition of the difficulty of entering into these relationships. That is, "Banks should endeavor to formalize …" [Revisions underlined]*

Principal 6 (BCBS Text):

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

Par. 35 – "Banks should maintain an inventory of incident response and recovery, internal and third-party resources to support the bank's response and recovery capabilities.

Par. 36 – "The scope of incident management should capture the life cycle of an incident,[21] typically including, but not limited to:

a) "the classification of an incident's severity based on pre-defined criteria (e.g., expected time to return to business-as-usual), enabling proper prioritisation of and assignment of resources to respond to an incident;

b) "the development, maintenance and testing of incident management procedures, including thresholds for triggering business continuity, disaster recovery and crisis management procedures; and

c) "the implementation of communication plans to report incidents to both internal and external stakeholders (e.g., regulatory authorities), including performance metrics during, and analysis of lessons learned after an incident.

Par. 37 – "Incident response and recovery procedures should be periodically reviewed, tested and updated. Root causes should be identified and eliminated to prevent the serial recurrence of incidents.

Par. 38 – "Lessons learned from previous incidents including incidents experienced by others, should be duly reflected when updating the incident management programme. A bank's incident management programme should manage all incidents impacting the bank, including those attributable to dependencies on, but not limited to, third parties and intra-group entities."

AORG Comments – Principle 6

AORG members find this principle to be reasonable in highlighting the value of incident reviews, however:

- *Broader focus than incident management -- it is the sense of AORG that the Consultative Document has singled out incident reviews disproportionately relative to other useful tools. AORG believes that the Committee could have simply underscored the need for risk assessment and vulnerability analysis using tools that are deemed appropriate for each bank. Although the Group does not advocate for including a prescribed list of tools, AORG envisions that those tools might include reviews of incidents, along with scenario analysis, loss analysis, audit findings, and the like.*
- *Less prescriptiveness -- As written, if incident management is retained as the sole focus of the Principle, AORG sees a need be far less specific and prescriptiveness in par. 36 subparts (a), (b) and (c) to a higher, less detailed level of incident management.*

Principal 7 (BCBS Text):

"Banks should ensure resilient ICT including cyber security that is subject to protection, detection, response and recovery programs 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.

Par. 39 – "Banks should have a documented ICT policy, including cyber security, which stipulates governance and oversight requirements, risk ownership and accountability, information security measures (access controls, critical information asset protection, identity management, etc.), periodic evaluation and monitoring of cyber security controls, and incident response, as well as business continuity and disaster recovery plans.

Par. 40 - "Banks should identify their critical information assets and the infrastructure upon which they depend. Banks should also prioritise their cyber security efforts based on the significance of the critical information assets to the bank's critical operations, while observing all pertinent legal and regulatory requirements relating to data protection and confidentiality. Banks should develop plans to maintain the integrity of critical information in the event of a cyber event. Banks should regularly evaluate the threat profile of their critical information assets, test for vulnerabilities and ensure their resilience to ICT-related risks.

Par. 41 – "When facilitating the implementation of wide-scale remote-access, rapid deployment of physical assets and/or significant expansion of bandwidth to support remote user connections and customer data protection banks should ensure that:

a) "appropriate risk mitigation strategies are developed for potential risks associated with a disruption or compromise of technology systems and applications. Banks should evaluate whether the risks, taken together with these strategies, fall within the bank's risk appetite and risk tolerance for disruption;

b) "well defined processes for management of remote assets, privileged users and application development are in place; and

c) "regular updates are made to ICT including cyber security in order to maintain an appropriate security posture to accommodate remote access as a longer-term option."

AORG Comments – Principle 7

This Principle is generally viewed by AORG members as a positive addition, and is reflective of changes already taking place in the industry.

++++++++++++++++++++

BCBS Questions

Q. 2 – Do you have any comment on the individual principles and supporting commentary?

A*: See narrative above.*

Q. 4 – Do you see merit in further consolidation of the Committee's relevant principles on operational risk and resilience?

A: *AORG members generally agree with the principles as outlined subject to revisions at the subparagraph level.*

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

November 2020