THE BANKING ASSOCIATION SOUTH AFRICA

Tel +27 11 645 6700
Fax +27 11 645 6800
P O Box 61674
Marshalltown 2107
www.banking.org.za

3rd Floor Building D
Sunnyside Office Park
32 Princess of Wales Terrace
Parktown 2193

06 November 2020

Basel Committee on Banking Supervision
Centralbahnplatz 2
4051 Basel
Switzerland
Via direct upload on BIS
https://www.bis.org/bcbs/commentupload.htm

Doc Ref: MARKB/#287373_V1

Your ref:

Direct ☎: +27 11 645 6753

E-✉: nobambom@banking.org.za

Dear Sirs

Consultative Documents: Principles for operational resilience and Revisions to the principles for the sound management of operational risk

The Banking Association South Africa appreciates the opportunity to comment on both consultative documents released by the Basel Committee on Banking Supervision, relating to operational risk and resilience. The consultative document "Principles for operational resilience" (the Document) poses five questions that will be answered below and we will make reference to the consultative document "Revisions to the principles for the sound management of operational risk" (the Principles) as required.

As an industry, we have actively adopted the principles for the sound management of operation risk and with the Covid-19 pandemic, operational risk management has received heightened attention, validating investment decisions and testing procedures.

We provide our comments for your consideration as follows:

Q1. Has the Committee appropriately captured the necessary requirements of an effective operational resilience approach for banks?

We believe that as a rapidly evolving discipline, the document contains sufficient information for both banks and supervisors to work towards a common objective.

Are there any aspects that the Committee could consider further?

The Document recognises at Paragraph 8, "*While it may not be possible to avoid certain operational risks, such as a pandemic, it is possible to improve the resilience of a bank's operations to such events*.". Despite banks having pandemic plans, the sheer scale of the pandemic and the co-ordinated and timely responses of governments introduced two important elements.

The first is the possibility that the government may need to close the banking industry, where transactions are not processed for value of the day of closure. In some jurisdictions this may require additional powers to be granted to the central bank.

The second element is the reliance on the banking industry to be impervious to exogenous shocks, establishing a dependency on the banking industry that may be unrealistic and detrimental to our reputation. Operational resilience will need to take a more holistic approach to key service providers in this digital age and the appropriate authority within the financial sector may have to be empowered to set rules for the non-bank service providers to ensure their systemic importance forms part of the overall resilience landscape.

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

Principle	Description	Comment
Section 3: **Operational risk management**	**Paragraph 1** Operational risk is defined in the	**Comment:**

Principle	Description	Comment
	capital framework as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.	The term "legal risk" could be replaced by non-financial risk, retaining the exclusion for strategic and reputational risk. Non-financial risk could be introduced as a footnote and replace the reference in Para 22(i) to conduct and cyber, Para 29 to procurement and outsourcing
	Paragraph 5 Banks commonly rely on three lines of defence: (i) business unit management,5 (ii) an independent corporate operational risk management function (CORF) and (iii) independent assurance.6 Depending on the bank's nature, size and complexity, and the risk profile of a bank's activities, the degree of formality of how these three lines of defence are implemented will vary. **Paragraph 6** Banks should ensure that each line of defence: a) Is adequately resourced in terms of budget, tools and staff; b) Has clearly defined roles and responsibilities; c) Is continuously and adequately trained; d) Promotes a sound risk management culture across the organisation; e) Communicates with the other lines of defence to reinforce the ORMF. If in one business unit there are functions of both the first and second line of defence, then banks should document and distinguish the responsibilities of such functions in the first and second line of defence, emphasising the independence of the second line of defence.	**Comment:** The three lines of defence articulation provides the latitude for both 1st and 2nd line roles to be in the same business unit but seems to discourage this, suggesting that the three lines of defence is a structural consideration. The recent publication by The Institute of International Auditors paper "An update of the Three Lines of Defense" differs markedly from this view and advocates an approach whereby structure is of less significance and role is more important, particularly independence of the 2nd line. While there needs to be appropriate, mandatory separation of responsibility across the lines of defence for Design, Execution, Monitoring, and Independent Assurance, there ought to be some room for non-mandatory, value-adding risk management activities across the Design<->Assurance spectrum regardless of which line of defence one sits in. In other words, and by way of illustration, someone in a 1st Line role should not feel constrained from conducting an assurance activity within a business area simply because Assurance may be deemed the exclusive purview of a 3rd Line role. This hypothetical assurance exercise by a 1st Line role does not, and should not, in any way obviate an independent assurance exercise to be

Principle	Description	Comment
		conducted by a 3rd Line role. If anything, the two assurance exercises should be seen as complementary, with the exercise conducted by the 1st Line function seen as an attempt to manage risk where it arises and the exercise conducted by the 3rd Line function seen as the organisation's formal, audited position on the state of affairs within the business area. The layers of defence mindset and approach might prove particularly positive in the 1st Line, as role players in that space start to take full ownership of risks and controls in their space rather than approaching risk management as an obligation and something to be done under compulsion.
	Paragraph 7 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.[7] 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. **Paragraph 50** The use of technology related products, activities, processes and delivery channels exposes a bank to operational, strategic and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks along the same precepts as operational risk management.	**Comment** There is reference to "technology risks" and "ICT risks" as distinct terms and concepts. There is also an indication that the former has implications for operational risk, strategic risk and reputational risk, whilst the latter appears to be positioned as an operational risk only matter. We would suggest that the term be standardised as "technology risk" and that the recognition that it spans operational, strategic and reputational risk be made explicit. This distinction and view is supported in the King IV Report on Corporate Governance for South Africa, with a statement which reads "…in King IV it is recognised that information and technology overlap but are also distinct sources of value creation which pose individual risks and opportunities. It is to reinforce this distinction that the Code now refers to technology and information instead of information technology". In addition, all risk types must be considered, not only ICT risks.

Principle	Description	Comment
	Paragraph 11 An effective independent review should: a) … b) Review validation processes to ~~ensure~~ verify they are independent and implemented in a manner consistent with established bank policies; c) ~~Ensure~~ Verify that the quantification systems used by the bank are sufficiently robust as (i) they provide assurance of the integrity of inputs, assumptions, processes and methodology and (ii) result in assessments of operational risk that credibly reflect the operational risk profile of the bank; d) ~~Ensure~~ Verify that business units' management promptly, accurately and adequately responds to the issues raised, and regularly report to the board of directors or its relevant committees on pending and closed issues;	**Comment:** In changing the verb from "ensure" to "verify", the objective of the 3Rd line of defence could be strengthened. Verification requires an active intervention rather than a more passive delegated alternative.
	Paragraph 12 Because operational risk management is evolving and the business environment is constantly changing, senior management should ensure that the ORMF's policies, processes and systems remain sufficiently robust to manage and ensure that operational ~~losses~~ risks in the context of risk appetite and tolerance are adequately addressed in a timely manner.	**Comment:** By replacing the noun "losses" with the words "risks in the context of risk appetite and tolerance", an earlier intervention point is possible. The benefit of a remedial approach to future losses captures the changing environment component of the ORMF.
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		**Comment:** Consequences should be added along with incentives.

Principle	Description	Comment
incentives for professional and responsible behaviour, and ensure that staff receives appropriate risk management and ethics training.		
	Paragraph 14 The board of directors should establish a code of conduct or an ethics policy to address conduct risk. This code or policy should be applicable to both staff and board members, set clear expectations for integrity and ethical values of the highest standard, identify acceptable business practices, and prohibit conflicts of interest or the inappropriate provision of financial services (whether willful or negligent). The code or policy should be regularly reviewed and approved by the board of directors and attested by employees; its implementation should be overseen by a senior ethics committee, or another board-level committee, and should be publicly available (eg on the bank's website). A separate code of conduct may be established for specific positions in the bank (eg treasury dealers, senior management).	**Comment:** Conduct risk may be heightened in certain areas of the bank and the example provided of treasury dealers and senior management provides useful references. The provision of a separate code of conduct for these positions may inadvertently create inconsistencies. An entity wide code of conduct should include all aspects of the various positions rather than targeting a special class of employee. Training in ethics or risk management could target these positions, providing the necessary differentiation and personalisation.
	Paragraph 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~~ tailored to the responsibilities of individuals in the organisation. Training provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended.	**Comment:** Although guidance is provided for customised training with examples, more emphasis could be placed on providing the bank with the flexibility to structure operational risk training in a way that makes practical sense for the bank. In this way the tile does not drive training but rather the function.
Principle 2: Banks should develop, implement and maintain an operational risk	**Paragraph 22:** ORMF documentation should clearly:	**Comment:** The reference to membership, if interpreted as specific individuals,

Principle	Description	Comment
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.	a) Identify the governance structures used to manage operational risk, including reporting lines and accountabilities, and the mandates and membership of the operational risk governance committees; b)…	makes the ORMF unwieldy.
	d) Describe the bank's approach for determining the banks ~~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;	**Comment:** Instead of requiring that the accepted operational risk appetite and tolerance be described in the ORMF, the ORMF should rather describe the bank's approach for determining the bank's operational risk appetite and tolerance, thresholds, etc, as such risk appetite and risk tolerance may change more frequently than the ORMF itself.
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	**Paragraph 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, applying a risk-based approach, to ensure ongoing effectiveness. The control environment should provide appropriate independence/separation of duties between operational risk management functions, business units and support functions, in line with responsibilities based on an established 3 lines of defence model.	**Comment:** We would propose that the review, monitoring and testing of controls take place using a risk-based approach for the most efficient use of resources.
Principle 6: 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		**Comment:** Consequences should be added along with incentives.

Principle	Description	Comment
risks and incentives are well understood.		
	Paragraph 34: Examples of tools used for identifying and assessing operational risk include: a)… e) ~~Metrics~~ – Key Risk Indicators Using operational risk event data and risk and control assessments, banks often develop metrics to assess and monitor their operational risk exposure. These metrics may be simple indicators, such as event counts, or result from more sophisticated exposure models when appropriate. Metrics provide early warning information to monitor ongoing performance of the business and the control environment, and to report the operational risk profile. Effective metrics clearly link to the associated operational risks and controls. Monitoring metrics and related trends through time against agreed thresholds or limits provides valuable information for risk management and reporting purposes.	**Comment:** Instead of referring to this paragraph as "Metrics" which is a very broad term and can also be interpreted to include the other operational risk tools like self-assessments , it is suggested that the term "Metrics" be replaced with the term "Key Risk Indicators", as this best describes what the intention of this paragraph is and aligns with terminology used in the current version of the Principles for Sound Management of Operational Risk.
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.		**Comment:** All risk strategies should be noted including risk acceptance and avoidance.
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.	**Paragraph 60:** A bank should periodically review all components of its business continuity policy and business continuity plans to ensure that contingency strategies remain consistent with current operations, risks and threats**.**	**Comment:** Once the policy is finalized, the review should be automatic however, the Business Continuity Plan is the living tool that ensures resilience and it in implementation where there are often challenges.

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

The operational risk practitioners must have the flexibility to adapt their processes in times of systemic stress. Circumstances are often fluid; however, this does not reduce the oversight function envisaged

in the Principles. Collaboration between banks should be encouraged with dynamic learning shared between competitors. Competition policies must be flexible enough to adjust rapidly to an emerging crisis.

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

A single reference work is always preferable.

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

At this time, we are not in a position to provide this information.

We trust that our comments will be of some value in your deliberations.

Yours faithfully

_____

Mark Brits
Senior General Manager – Prudential