

18 December 2020

SUBMITTED ELECTRONICALLY: baselcommittee@bis.org

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

Re : Revisions to the Principles for the Sound management of Operational Risk

Dear Sir/Madam:

The International Banking Federation (IBFed)¹ is pleased to respond to the Basel Committee on Banking Supervision's consultation proposing [Revisions to the principles for the sound management of operational risk](#). We agree that it is appropriate to review the Principles as the operational risk threat landscape has evolved since 2011 as banks have become more reliant on outsourced technology platforms and cyber threats have become more sophisticated and all pervasive.

We also note that the Committee's 2014 review of the implementation identified a number of areas where banks had yet to fully implement some elements of the Principles and that requirements in relation to these have been augmented in the proposed Principles revision. But we believe that with the proper and increased supervisory focus on governance, resilience testing, individual accountability and outsourcing arrangements has ensured that the gaps that were evident then will have closed albeit that operational risk challenges are always changing.

So we support the proposals made in the consultation paper to update the Principles, welcoming the continued exclusion of strategic and reputational risk from the definition of operational risk and the recognition that banks should adopt a proportionate approach, taking account of the nature, size, complexity and risk profile of their activities.

¹ *The International Banking Federation (IBFed) was formed in 2004 to represent the combined views of our national banking associations. The IBFed collectively represents more than 18,000 banks, including more than two thirds of the largest 1000 banks in the world. IBFed member banks play a crucial role in supporting and promoting economic growth by managing worldwide assets of over 75 trillion Euros, by extending consumer and business credit of over 40 trillion Euros across the globe, and by collectively employing over 6 million people. The IBFed represents every major financial centre and members' activities take place globally. This worldwide reach enables the IBFed to function as a key international forum for considering regulatory and other issues of interest to the global banking industry.*

In using the Principles, banks and supervisors alike should recognise the benefits of combining intelligibility with a degree of flexibility, as different banks to which they apply will have different structures, operational risk profiles and business models. Taking a proportionate risk-based approach and focusing on material risks, to avoid over-granularity of application and supervisory review should be an underpinning approach the operationalisation of the Principles. It would be beneficial to clearly state this in the introductory sections to Principles.

It is important too that the Principles should be internally coherent with other BCBS supervisory products, such as Pillar 3 disclosure. Harmonising regulatory requirements internationally by facilitating compliance and avoiding duplication and overlap is crucial for banks. So, the Principles should be aligned with other already existing practices and standards, such as the EBA Guidelines on ICT and security risk management.

We have only a few comments on the proposed changes, which are:

Principle 1

Attestation

Principle one builds on the concept of a Code of Conduct or Ethics Policy introduced in the 2011 Principles by proposing to require employees to attest to it. We do not support this attestation approach which is just one of a number of ways in which the board and senior management could ensure compliance. Indeed, the mere fact of an employee attesting does not prevent them from going on to breach the Code/Policy. A better mechanism would be strong leadership from the top of the bank (as noted in para. 18) coupled with a robust mechanism to identify and sanction those that do not adhere to the Code/Policy.

Oversight of Code/Policy

We agree that the Code/Policy should be overseen by the board, but the proposed wording may be interpreted as requiring banks to set up an ethics committee, as many, but not all, have already done. This task should remain a board responsibility and whether or not to delegate it to a subcommittee and which one, should be a decision for the board itself.

Conduct as an operational risk?

We recognise that Conduct Risk was identified in the 2011 Principles. However, since then banks' management of Conduct Risk has improved significantly and conduct risks are now recognised as an integral part of operational risks and managed as such by specialist teams. Our preference would be for the deletion of paragraph 14. However, if the Committee does not support our recommendation we have suggestions as to how paragraph 14 could be amended. These are:

Publication of Code of Conduct

We do not support publication of the Code of Conduct publicly. Doing so will not drive closer adherence (leadership and internal sanctions will) but will inevitably lead to an increase in potentially vexatious legal challenges as third parties assert that a bank has breached its own Code/Policy.

Code of Conduct scope

Differentiating Code/Policy requirements based on roles may send the wrong signals. All within a bank should abide by them regardless of roles or position.

So, we propose the following change to para. 14:

~~...whether wilful or negligent). The code or policy should be regularly reviewed, and approved and overseen by the board of directors and attested by employees; its implementation should be by a senior ethics committee, or another board level committee, and should be publicly available (e.g. on the bank's website). A separate~~ The code of conduct may be established for specific positions in the bank (e.g. treasury dealers, senior management).

Training

We support comprehensive operational risk training programmes which in our experience are modular, augmented by role specific training where appropriate. We suggest condensing para 17 as follows:

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 *and consideration given to which categories of staff it should be mandatory.*

Principle 4

Para 26 requires the Board to regularly review limits, the risk appetite and tolerance statements. We welcome that the Principles do not prescribe a periodicity to this. The review cycle should be determined by the Board taking into account changing circumstances, such as risk appetite revisions and modification of the business model.

Principle 6

Principle 6 has a helpful compendium of possible approaches to identifying and assessing operational risk, not all of which may be appropriate, depending on the operational risks a bank faces and its control environment. So, we suggest amending para 34, which introduces the different tools as follows:

34. ~~There are a range of tools used for identifying and assessing operational risk include.~~ *Examples of tools used for identifying and assessing operational risk include. Banks should determine which, if any, tools they should use based on the nature and materiality of the operational risks they face. Example include:*

Paragraph 35 links risk assessment with the concepts of 'internal pricing', 'performance measurement' and 'business opportunity assessments'. It is not clear what the BCBS understands by these terms or how operational risk assessments be taken into account for these processes. For example, Business opportunities come in many different sizes and it is not clear what is meant by this term. Is the intention to capture M&A activity or for instance, changes to a credit card marketing campaign? Our expectation is that it refers to new business initiatives, as described in para 20. To clarify this, and

importantly introduce a materiality assessment, we propose changing the wording of this para as follows:

35. Banks should ensure that the operational risk assessment tools' outputs are:

- a)
- b) Adequately taken into account in the internal pricing and performance measurement mechanisms as well as for *the assessment of material new business opportunities*-assessments;
- c)

Principle 7

Paragraph 37 is a helpful and succinct description of the three lines of defence. As we note above, we think there is every merit in a principles based approach that is applied proportionately and only to material operational risks. This point in the document would be a good point at which to re-emphasise this. So, we recommend an amendment of this paragraph as follows:

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, *which should be proportionality applied to the most material changes*. In particular:

Some banks may not have a central record of products and services as required by para. 40, for instance if they run a multi-point of entry business model. We suggest amending this paragraph as follows:

Banks should ~~maintain a central record~~ of *ensure that they have processes and procedures in place to enable them to record* their products and services (including the outsourced ones) ~~and access it in a timely fashion to the extent possible~~ to facilitate the monitoring of changes.

Principle 9

We note that para. 50 refers to strategic and reputational risks, which fall outside the scope of operational risk, so we suggest amending it as follows:

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.

Principle 10

We fully support the new Principle 10, particularly as the supporting material has been kept to a minimum

But we recommend the following amendment:

Achievement of strategic objectives

A sound ICT framework underpins a bank's achievement of its strategic objectives but so do many other elements of its business processes and controls. We do not see a need to specifically call out ICT in this respect so recommend the following deletion.

~~....sound ICT framework contribute to the effectiveness of the control environment and are fundamental to the achievement of a bank's strategic objectives. The ICT...~~

Principle 12

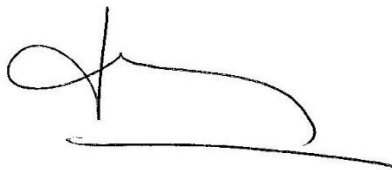
Pillar 3 disclosure requirements have evolved significantly since the operational risk Principles for were released in 2011, when the members of the Members of the SIG Operational Risk Subgroup would have been drawing on the BCBS's Pillar 3 requirements as issued in issued in 2004, and subsequently amended in July 2009. In our view to avoid ambiguity or divergent requirements on disclosure the Principles should refer directly to the DIs requirements of the Basel Framework as the single source of truth. As a result, paragraphs 61 to 63 should be deleted and replaced with:

Banks should ensure that they comply with the Pillar 3 operational risk disclosure requirements of the Basel Framework.

* * * * *

Should you have any questions or require additional input please contact us.

Yours sincerely,



Ms Hedwige Nuyens
Managing Director
IBFed



Mr. Hugh Carney
Chair of the Prudential Supervision Working Group
IBFed