Dr Luke Carrivick
Operational Riskdata eXchange Association (ORX), c/o VISCHER Genève Sàrl,
Rue du Cloître 2, 1204
Genève, Switzerland

Arthur Lindo
Chair, Operational Resilience Working Group
Basel Committee on Banking Supervision
Centralbahnplatz 2
Basel, Switzerland

Re: d508 - Revisions to the principles for the sound management of operational risk

Dear Arthur,

ORX values the opportunity to respond to the Basel Committee on Banking Supervision's (BCBS's) proposed revisions to the principles for the sound management of operational risk (PSMOR). Our response is informed by discussions with, and formal feedback from, our banking membership. Our contribution can be summarised in the following statements:

- ORX welcomes a refresh of the principles, bringing many of them in line with contemporary practice, and highlighting what are currently the most material operational risks.
- However, assuming the BCBS expects the principles to remain effective for some time, our view is that they may not support, and could even constrain, the innovation needed in operational risk management practice for increasingly digital banking. Within our membership, 62% of banks feel the principles support current ORM practice, but this drops to 39% when asked if they support necessary innovation over the next 5 years.
- One emergent industry practice we see is where banks are targeting an efficient baseline risk management framework, supplemented by an agile dynamic approach for the most material, new or changing risks. It is unclear if the principles would support this approach.

We hope our comments have been constructive and that the BCBS considers our points before finalising its recommendations.

Yours sincerely,

Luke Carrivick, Director of Research and Information, ORX

Formal Response

The remainder of this letter provides direct responses to the two questions. Our response is informed by discussions with, and formal feedback from, our banking membership[1].

Q1. Has the Committee incorporated the appropriate revisions to the Principles? Do you have any specific comments on the revisions to the Principles and supporting paragraphs?

62% of members agreed that the principles support efforts to manage operational risk today, with 38% remaining neutral. The consensus is that the updated principles are now more comprehensive, they cover the key components of good operational risk management and reflect practice that is already widely adopted.

Also welcome is the attempt to cover more contemporary sources of operational risk such as change, ITC, data quality and model risk. It is hoped this additional guidance will ensure these risk silos are integrated within the overall operational risk framework and comply with the overall principles.

On this point, throughout the document there is no mention of non-financial risk. Whilst this is not a universally adopted term, it does encourage the consistent treatment of risk silos in a unifying framework (the umbrella risk function is a key emergent theme over the last few years[2]) and helps extend the view of impacts beyond financial ones.

ICT inclusion is welcome and long overdue

We think the inclusion of a principle on ICT is welcome and beneficial for several reasons:

- It removes any ambiguity around whether ICT activities constitute as operational risk, and to support this ICT is consistently highlighted throughout the document
- With digital innovation in banking (accelerated by the pandemic) set to continue, we expect the operational risk management of ICT, data and cyber risks to be vital[3].

There are several suggestions for your consideration:

[1] ORX is a not-for-profit industry association dedicated to advancing the measurement and management of operational and non-financial risk in the global financial services industry. Please see https://managingrisktogether.orx.org/about for more detail.

[2] https://managingrisktogether.orx.org/research/operational-risk-umbrella-function

[3] https://managingrisktogether.orx.org/coronavirus/covid-risk-review

- The ability of the board (or the 2nd line providing an independent view to the board) to challenge is critical here and relies on the need for them to have sufficient understanding of ICT concepts and framework. This could be emphasised in the principles by stating that the board *must*, rather than *should* "evaluate the design, implementation and effectiveness of frameworks".
- ICT risk is mentioned within the section on change (principle 7), but the extent of the expectation on the governance and risk management of ICT risks relating to technology change within 3rd parties would be welcome.
- While not a majority view, some felt that a greater emphasis needed to be placed on the importance of this principle, with further specificity and definition.

Other specific comments

Compliance role in 3LOD: In the introduction which sets out the 3LOD model it appears that compliance is being treated as a "business unit", largely a support function to the 1st line, rather than also having a significant 2nd line role (like operational risk management). This is a more simplified view that we have seen through our industry experience.

Clarity on code of conduct: On the code of conduct (Principle 1 Section 14), can maintenance and approval of the code be delegated to senior management in keeping with some other responsibilities set out in the paper?

Clarity on 3rd line documentation: Greater clarity is needed on the expectations of the 3LOD around the tools for risk and control identification and assessment (Principle 2 Section 22(c)). Here, the roles and responsibilities for the third line of defence, the Internal Audit Department (IAD), are governed by the IAD. IAD defines its roles and responsibilities in executing its mandated oversight of the ORMF, which includes risk identification systems and reporting tools. The expectation of this Principle is therefore unclear as the description would be included in IAD related documentation, so additional clarification is warranted. The 2020 ORMF Principle denoting the ORMF documentation specify the roles and responsibilities of the three lines of defence is an enhanced principle component from 2011. This point requires further clarification.

Ambition of internal pricing and performance: Internal pricing and performance should be included in risk assessment (Principle 6 Section 35(b)) and poses a question on the ambition of implementation. If the expectation is simple (e.g. internal equity allocation and new business initiatives) this is feasible, but if it is complex (e.g. marginal pricing of new business with significant operational risk) this may be a challenge. As this is a new principle in comparison to the 2011, clarification of the ambition would be welcome.

Other recommended additions

- **Focus on purpose**: There is a slight concern that the principles may encourage only the formality of Operational Risk management without necessarily improving the quality of outcome. Although themes on the fundamental purpose of ORM are scattered throughout the document, one of the clearest articulations "Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively" does not appear until section 6.33.
- **Be more explicit on dynamic risk management**: A recurring theme in the update is to make framework elements more dynamic. For example, risk appetite is made forward-looking, change management includes "continuous risk and control assessments" and emerging risks should be reported and monitored by metrics. This is a theme we observe across the industry, where banks are targeting an efficient baseline risk management framework, supplemented by a more agile dynamic approach for material, new or changing risks.
- **Control design**: A recurring and welcome theme throughout the document is how much an institution should understand its control framework. However, within principle 9, on control and mitigation, more detail could be given on principles for good control design and performance. Through our work on controls we see that good design is often supported by control taxonomies and libraries[4][5][6].
- **Should be principles**: It is possible that in some areas the principles have become a little too precise, particularly since they will no doubt be cascaded with increasing prescription into regional and local regulation. An example of this is the detail provided in sections on governance where the most appropriate implementation will be dependent on the size of the institution. In general, the text is most powerful where it states robust principles and is less prescriptive in the detail.
- **Disclosure**: Within the section on disclosure (principle 12), it stresses the significance of sharing information with external shareholders. This is delicate, and as the principles acknowledge, in disclosing exposures care must be taken to inadvertently create more operational risk. Furthermore, this may also be challenging without a commonly established metric for operational risk exposure. This is an area where we see innovation being beneficial, and one in which the principles could support advancements.

Principles on Resilience

[4] https://managingrisktogether.orx.org/research/understanding-control-management-practices

[5] https://managingrisktogether.orx.org/research/control-management-benchmark

[6] https://managingrisktogether.orx.org/cyber-risk-management/controls-indicators

The majority (65%) of our members think that the principles of resilience need to be further consolidated. This lack of consensus may reflect difference in jurisdiction, the maturity of resilience frameworks and the existing governance of resilience within individual banks[7].

Q2. Are there any aspects that the Committee should consider further?

Lacking a view of innovative practice

It is also clear that updates to the proposed tools for the identification and assessment of operational risks (Principle 6) reflect a desire to move to a more forward looking and dynamic approach. This focus on evolution of risk profiles is welcome, but there is little on the future evolution of practice. Leading to a concern that the principles could become a constraining factor when banks innovate the ORM practice in what are increasingly digital institutions.

On this point, only 29% think that the principles will support innovation in operational risk over the next 5 years. Whilst the principles bring clarity, they do not appear to bring new ideas or challenge the current thinking. Furthermore, the detail within the principles can be focused on analogue risk management as we enter a digital age. An emergent picture we observe is one where banks are pursing efficiency and automation where possible, removing manual steps and allowing resources to focus on the most material risks. We would welcome the opportunity to discuss what appetite for innovation in risk management exists within the supervisory community and, if innovation is considered necessary, how it can be supported.

[7] https://managingrisktogether.orx.org/news-blogs/operational-risk-community-discuss-resilience