November 6, 2020

Pablo Hernández de Cos, Chairman
Carolyn Rogers, Secretary General
Basel Committee on Banking Supervision
Centralbahnplatz 2
4051 Basel
Switzerland

Via Electronic Mail

RE: Basel Committee on Banking Supervision Consultative Document "Revisions to the principles for the sound management of operational risk"

Dear Mr. Hernández de Cos and Ms. Rogers:

On behalf of the Institute of International Finance (IIF) and the Global Financial Markets Association (GFMA), or ("the Associations"), we welcome the opportunity to comment on the Basel Committee on Banking Supervision's (BCBS) Consultative Document "Revisions to the principles for the sound management of operational risk."[1]

We welcome that some of the suggestions we raised with regard to the 2011 version of the Principles are reflected in this updated version, for instance a clearer distinction between the responsibilities of the board of directors and senior management and clarification on the three lines of defense. We also welcome the introduction of a specific principle on information and communication technologies (ICT) risk management.

However, more clarity is needed on how the consultation is interlinked with the BCBS Consultative Document "Principles for operational resilience" since these two documents are overlapping in different items (for example on risk appetite, taxonomy, business continuity, tolerance thresholds).

[1] BCBS 2020. "Consultative Document: Revisions to the principles for the sound management of operational risk" August 6, 2020

These concepts should be defined in the same way to avoid different interpretations or implementations.

Across both documents, the role of the board of directors should be seen as to ensure that the overall Operational Risk Management Framework (ORMF) is established, approved, and periodically reviewed. Additionally, board of directors should oversee material operational risks and the effectiveness of key controls, while ensuring that senior management implements the policies, processes, and systems of the ORMF effectively at all decision levels.

We also consider the principles too prescriptive and granular at times. The principles should ideally focus on materiality and provide institutions with the flexibility to tailor them to their respective organizations and the broader market convention in the region. We flag examples and provide drafting suggestions in the Annex.

Separately, the industry recommends that the BCBS clarifies what is the aim of the examples and that they are not exhaustive. We also suggest that in some cases clarity is provided to identify the principle behind the example but that the example may not present the only way to establish the controls. We provide drafting suggestions in Annex II accordingly.

With regards to the broader benchmarking and comparative analysis, we recommend that the policymakers provide support in developing the appropriate benchmarks to facilitate comparative analysis. Supervisory expectations in terms of industry-wide standards should be limited until reliable and accepted benchmarks are in place.

Discussion within our membership showed that some of the terminology is used differently across stakeholders and requires clarification in the guidelines; e.g. the difference between “event” and “incident” as well as terms such as “accountability” and “responsibility.” We suggest a simplification of some of the principles in favor of others, and cross-references between both sets of principles. It is also important to distinguish clearly between “risk appetite” and “tolerance” so that these concepts are not confused.

Additionally, it is crucial that regulatory requirements are harmonized to facilitate compliance and to avoid duplication and unnecessary overlap. Therefore, both set of principles should be linked with already existing international and regional practices and standards.

In that sense, we consider any disclosure requirements on operational risk should be aligned within Pillar III Disclosure to ensure the comparability between different entities, being at the same time respectful with competitive and proprietary information. Disclosed information becomes more

effective and meaningful when it is comparable avoiding inconsistent information across banks that may mislead users of information.

We would also appreciate more clarity on how to use these Principles in parallel with the final Basel III package. In particular, while firms that use internal models broadly use a multitude of data sources to achieve better estimates of operational risks, the updated global standard only requires firms to compute a simplistic capital charge based on past loss events and a multiplier. We raise further points on the Basel III linkage in Annex I.

In the Annexes I and II, we provide more details on your questions as well as specific drafting suggestions, respectively. We hope that you will find our comments useful and constructive. If you have any questions, please feel free to contact the undersigned at mboer@iif.com or aparent@gfma.org.

Yours sincerely,

Allison Parent
Executive Director
Global Financial Markets Association (GFMA)
aparent@gfma.org

Martin Boer
Director, Regulatory Affairs
Institute of International Finance (IIF)
mboer@iif.com

ANNEX I – THEMATIC POINTS AND PRINCIPLES FEEDBACK

Thematic points

In general, it is important that the BCBS clarifies the relationship between operational risk and operational resilience, and how to think about operational risk management in the context of resilience. Further, more clarity is needed on how this Consultative Document is related to the BCBS Consultative Document "Principles for operational resilience" since these two documents are overlapping in different items (e.g. risk appetite, taxonomy, business continuity, tolerance thresholds, etc.). These concepts should be defined in the same way to avoid different interpretations or implementations. It would also be useful to explain in more detail the difference between operational risk scenarios and operational resilience scenarios.

On page three, when defining "Operational Risk" in paragraph 3 the BCBS could consider adding all non-financial risks, rather than referring to specific ones throughout the document (e.g. legal risk, cyber risk, conduct risk.) Similarly, perhaps "Technology Risk" could be used as a catch-all for the references to "technology risks" and "ICT risks."

In the section "Operational Risk Management," paragraph 5 reads as follows: *"Banks commonly rely on three lines of defence: (i) business unit management (ii) an independent corporate operational risk management function (CORF) and (iii) independent assurance."* With the following footnote: *"The term 'business unit' is meant broadly to include all associated support, corporate, and/or shared service functions, as for example: Finance, Compliance, Legal, Human Resources, Operations and Technology etc. Risk Management and Internal Audit are not included unless otherwise specifically indicated."* It is worth nothing that Legal and Compliance are considered as second line in US banks, but first line in the BCBS paper.

In paragraph 6d, where it says "*promotes a sound risk management culture across the organization*" the BCBS may want to provide additional guidance on "culture" or refer to recently published guidance by the Institute of Operational Risk.[2]

In the chapter preceding the principles it says about the third line of defense, in paragraph 11: *"This function's staff should not be involved in the development and implementation of operational risk management processes by the other two lines of defence."* In this case we believe that development and implementation should not be part of internal audit, but operations need to remain across the firm and therefore include internal audit.

[2] Institute of Operational Risk. "Sound Practice Guidance."

Feedback on specific principles

Principle 1 – Risk management culture

The statement "*…that customised training programs are mandatory for specific roles, such as heads of business units, heads of internal controls and senior managers…*" (paragraph 17) seems overly detailed. Separately, both "incentives" and "consequences" should be included. This would also pertain to Principle 6.

Principle 2 – Operational risk management framework

This includes conduct risk as part of legal risks (paragraph 22i). Some firms would consider both separately and we would like more clarity on the definition of conduct risk. In general, there seems to be a disparity between how European and US institutions consider conduct risk. We would welcome a broader recognition that definitions can be different and—as already stated above—and a simplification of some principles in favor of others.

We would support including model risk under the scope of operational risk to the extent that some incidents/losses are related to model validation and governance. However, we would need to distinguish between losses and management/design of model risk (which is handled separately from the ORMF.)

We would also ask for clarity regarding the establishing of limits and thresholds on inherent risk exposure. It might make more sense to establish limits only on residual risk.

Principle 3 – Board of directors

This principle states that the "*board of directors should oversee material operational risks.*" This is quite specific. As firms get larger, some of these risks are treated by Risk Committees.

The principle also states that the board of directors should "*ensure that senior management implements the policies, processes and systems of the ORMF effectively at all decision levels.*" We would appreciate clarification on what "ensure" means exactly in this context.

Also, the previous version of the Principles stated: "*The board of directors should establish, approve and periodically review the Framework.*" This text should stay in addition to the new (and clarified) text.

The use of the word “challenge” has specific meanings for different banks. A clarification of what is meant by this word in paragraph 23d) would be helpful.

Principle 5 – Senior management

This describes the relation between the board of directors and senior management. However, there should be room for firms to determine the appropriate level of oversight. For instance, the responsibilities of senior management as described in paragraph 31 are too prescriptive.

In paragraph 29, we would also like to emphasize that senior management have a holistic approach with regards to operational risk.

Principle 6 – Identification and assessment

In this principle references to risk event datasets were more commonly used for the Advanced Measurement Approach and there could be further clarification on how this reconciles with the Standardized Measurement Approach (SMA). For example, in the current SMA proposal there is a loss component based on 10 years of loss data, which has not been mentioned in Principle 6, nor the possibility to exclude some losses, as far as the excluded losses are rare, supported by strong justification, approved by supervisors and publicly disclosed (BCBS d424 (§27-28-29), nor the BCBS precision that exemptions as “settled legal exposures and divested businesses” are “examples”, and thus opening the door for other situations on a case by case basis. We would like clarification on the distinction between “event” and “incident” management (if there is any and beyond the scope of BCM). Mapping to Basel business lines and loss categories requirement, as referenced in the 2011 paper, should be re-instated even though we recognize that categories are outdated and would benefit from review.

In the case of section 34a, this describes the use of external data as a useful tool to complement internal loss data. With the changes to the Basel standards and the abolition of the AMA framework, the linkage—especially when the framework is applied to smaller banks—may need reconsideration in terms of proportionality. However, some banks and supervisors still prefer to have external data for benchmarking and Pillar 2 purposes in their toolboxes.

Section 34c on “event management” seem overly prescriptive. We are concerned that supervisors would expect all those tools/reports listed during the inspections even they are not supposed to be binding. We suggest that these examples are moved to an appendix.

With regards to paragraph 34 (g) benchmarking and comparative analysis, we recommend support from the policy makers in developing the appropriate benchmarks to facilitate comparative analysis. Supervisory expectations should be limited until reliable and accepted benchmarks are in place.

Paragraph 35b) indicates "*banks should ensure that the operational risk assessment tools' outputs are*" "*[a]dequately taken into account in the internal pricing and performance measurement mechanisms as well as for business opportunities assessments.*" It is unclear what "*adequately taken into account in the internal pricing*" means and what "performance measurement" and "business opportunity assessments" are, which can mean different things in different banks.

Principle 7 – Change management

In paragraph 36 "unfamiliar markets or jurisdictions" and "that are geographically distant from the head office" could be understood to refer to strategic risk, which is specifically excluded from the definition of operational risk whereas operational risk is clearly involved in new business/products process assessment. It would be useful to know how to align when excluded categories (such as strategic risk and reputational risk) should be used and how they should be differentiated for a clear and consistent distinction to be factored into the risk taxonomies. It should also be clarified that when banks go to unfamiliar markets or jurisdictions operational risk applies in the same when as when they enter new products.

This principle should not be too prescriptive as banks have their individual first and second line of defense approaches. For instance, the statement "*The first line of defence should perform operational risk and control assessments of new products and initiatives*" (paragraph 37a) is too prescriptive; this should be *ex ante* and also not in the responsibility of first line of defense.

Paragraph 37b) states that "*second line of defence (CORF) should challenge the operational risk and control assessments of first line of defence.*" We would recommend that includes concepts of control, design, and effectiveness.

Principle 8 – Monitoring and reporting

Paragraph 41 states that "*Banks should continuously improve the quality of operational risk reporting…*" We would ask the BCBS to consider using another adjective for "continuously." It is difficult to demonstrate continuous improvement. In addition, it is hard to show quarter over quarter trends in board reporting when the reporting continues to change.

Principle 9 – Control and mitigation

The BCBS principles have recognized the invaluable role insurance plays in providing adequate risk mitigation and going beyond its use as a tool to circumvent control deficiencies. In fact, insurance is used as a forward-looking risk mitigation tool which provides an incentive for banks to protect and transfer tail risk rather than transfer recurring losses. Furthermore, given the mitigation capability of insurance is not dependent on whether a bank is using a model-based (AMA) or standardized approach (SA), the use of insurance to offset a certain proportion of operational risk RWA should remain an option even after the transition to Basel III.

As such, certain elements from previously issued guidance around the use of insurance under AMA remain applicable and thus, we urge the BCBS to include a recommendation to supervisory bodies to consider how its benefit can be recognized in ways that are compatible with the new Basel framework (e.g. capital deductions and/or Pillar 2). Our suggested wording to that effect can be found in Annex II.

Paragraph 46 states that "*Control processes and procedures should include a system for ensuring compliance with policies, regulations and laws.*" We would ask the BCBS to clarify that ownership is not prescribed to be with the Operational Risk function. Compliance systems ought to be leveraged to ensure overall compliance with policies, regulations, and laws.

Paragraph 48—which refers to "internal controls"—covers much more than controls of meeting norms, targets, or limits. Hence, we propose to rephrase this paragraph changing the word "controls" to "mitigants." Separately, 48g includes an example that "*Vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.*" Here we would ask that exceptions can be carved out based on the nature of job descriptions (e.g. risk management, internal audit.) This section is overly prescriptive and could be more outcomes-based.[3]

In paragraph 51, the establishment of an effective control environment at the bank and service provider should include having proper metrics and reporting to facilitate oversight of the third party. Third parties and outsourcing risk might merit their own Principle considering the relevance of this risk.

[3] See for example the US Federal Reserve 1996. "Supervisory Guidance on Required Absences from Sensitive Positions." Dec. 20, 1996

Principle 10 – Information and communication technology

As previously stated, we welcome Principle 10 on information and communication technologies (ICT) risk management. However, it could be interpreted that ICT was complement but different to the operational risk framework. We propose that the BCBS makes clear that ICT is fully embedded in the operational risk framework (definitions, methodologies, etc.), for instance by starting Principle 10 with: "*As part of the operational risk management framework…*".

The BCBS should also consider including Cyber Risk policies. Operational risk has several pillars including cyber and third-party risks. As the world is moving to digital and the industry relies heavily on data privacy on information risk, it could perhaps be added under the umbrella of ICT risk.

In terms of paragraph 57 (b), the industry understands that "regularly tested" is aligned with ICAAP scenario and disaster testing frequencies. This could be further confirmed in the document.

Principle 11 – Business continuity planning

This principle should be aligned with the Principles for operational resilience (beyond mentions in the footnote). This includes strengthening language beyond the governance of business continuity and confirm the relevance/value of the paper on operational resilience principles. While the coverage of business continuity should continue in its current form, more focus should be given to ensure continuity of critical operations/material business units, aligned with the Operational Resilience objectives.

The requirements for scenario components (paragraph 59b/c) are overly prescriptive in the context of a principles-based approach. The BCBS should clarify that periodic review should focus on business continuity program (as opposed to policy) and remain consistent with current operations etc. This principle would also benefit from more explicit references to non-financial risks (e.g. fraud, conduct risk) and should also include lessons learned and remediation steps into board updates.

We also believe that the guidelines would benefit from a further definition on the envisaged time horizon regarding the notion of 'forward-looking' under paragraph 59.

Principle 12 – Role of disclosure

Here a clearer link is needed to Basel III Pillar III operational risk disclosure requirements. There are also sensitivities around the requirement to disclose sensitive information, such as significant operational loss events, because as well as exposing the bank to risk by disclosing potentially

unaddressed vulnerabilities, the wider disclosure of significant operational loss events could lead to the publication of market sensitive, legally privileged or material non-public information relating to a bank's transactions, strategies or business activities.

Furthermore, such a disclosure could create operational risk itself (internal revenue and loss information). For instance, if banks do not disclose the events because the remediation is ongoing, regulators might challenge banks for not disclosing it.

Links to the final Basel III package

The guidelines continue to promote appropriate and sound operational risk management culture and practices across the three lines of defense. However, in terms of Risk Management Environment and Principle 6, the guidelines with regards to tools used for identifying and assessing operational risk are very much tailored to the current Basel standards and for example in the context of operational risk data events are not fully aligned with the expectations set out in the updated SA-OR.

The minimum loss data standards (outlined in paragraphs 19 to 31) of SA-OR are very different to the operational risk event data suggested in the principles in terms of scoping (no 3rd party data and no recording of near misses, i.e. event/incident vs loss event data gathering). Furthermore, the loss data is subject to periodic reviews by the national supervisors and the SA-OR standard already establishes a control framework to guide the procedures and processes relevant to operational loss event identification, collection, and treatment. In this context, we recognize that the PSMOR is aimed at operational risk management and the SA-OR capital approach is necessary for measurement. The implementation of SA should not inhibit the enhancement in loss data collection processes as these are essential or the advancement of op risk management as a discipline. However, a distinction between the two could be strengthened in the guidelines.

The standardized approach for measuring minimum operational risk capital requirements replaces all existing approaches in the Basel II framework and only banks with a BI greater than €1bn are required to use loss data as a direct input into the operational risk capital calculations. In terms of governance and quality of operational loss data, the soundness of data collection and the quality and integrity of the data are crucial to generating capital outcomes aligned with the bank's operational loss exposure. This is inconsistent with the new revised principles that require more extensive data gathering for a wider group of firms.

ANNEX II – MARKED DRAFT GUIDELINES

This annex is a marked industry version of the draft BCBS guidelines issued for comment, with our targeted suggestions in bold and deleted text with a strikethrough. The sections where we do not have directly proposed changes, although we may provide comments towards in Annex I and in our general remarks, are excluded and marked […].

1 Revisions to the Principles for the Sound Management of Operational Risk

1. Introduction

…

2. Components of operational risk management

…

3. Operational risk management

1. […]
2. […]
3. […]
4. […]
5. […]
6. […]
7. […]
8. […]
9. […]
10. […]
11. The third line of defence provides independent assurance to the board of the appropriateness of the bank's operational risk management framework. This function's staff should not be involved in the development **and implementation** ~~, implementation and operation~~ of operational risk management processes by the other two lines of defence. The third line of defence reviews generally are conducted by the bank's internal and/or external audit, but may also involve other suitably qualified independent third parties. The scope and frequency of reviews should be sufficient to cover all activities and legal entities of a bank**, applying a risk-based approach**. An effective independent review should:

    a) […]

    b) Review validation processes to ~~ensure~~ **verify whether** they are independent and implemented in a manner consistent with established bank policies;

    c) ~~Ensure~~ **Verify whether** ~~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;

e) […]

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. Improvements in operational risk management depend heavily on senior management willingness to be proactive and also act promptly and appropriately to address operational risk managers' concerns.

4. Principles for the sound management of operational risk

1.1.1.1 Principle 1: The board of directors should take the lead in establishing a strong risk management culture, implemented by senior management.[11] 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.

13. […]

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 **appointed by the Board**, ~~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).

15. […]

16. […]

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.~~

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, 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.

18. […]

1.1.1.2 Principle 2: 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.

19. […]

20. […]

21. […]

22. ORMF documentation should clearly:

a) […]

b) […]

c) […]

d) Describe the bank's **approach for determining its** ~~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;

e) […]

f) […]

g) […]

h) […]

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, risk causes, materiality and business units where they occur; it can highlight the non financial risk it refers to it can also flag those operational exposures that partially or entirely represent legal (**may in some jurisdictions include** ~~including~~ conduct), model and ICT **related operational risks** (including cyber) risks as well as exposures in the credit or market risk boundary;

j) […]

Governance[14]

1.1.2 The Board of Directors

~~1.1.2.1 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.~~

Principle 3: The board of directors should ensure that the overall Operational Risk Management Framework is established, approved and periodically reviewed and oversee material operational risks and the effectiveness of key controls, while ensuring

that senior management implements the policies, processes and systems of the ORMF effectively at all decision levels.

~~**1.1.2.2**~~

23. The board of directors should:

    a) […];

    b) […]

    c) […]

    d) Regularly **review** ~~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 (eg changing business volumes);

    e) […]

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.~~

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.

1.1.2.3 Principle 4: […]

25. […]

26. […]

1.1.3 Senior Management

1.1.3.1 Principle 5: […].

27. […]

28. […]

29. Senior management should **have a holistic approach to operational risk and** ensure that staff responsible for managing operational risk coordinate and communicate effectively with

staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services such as insurance risk ~~transfer and other third party arrangement~~s (including outsourcing). Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

30. […]

31. […]

32. […]

1.2 Risk Management Environment

1.2.1 Identification and Assessment

1.2.1.1 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 risks and incentives are well understood.

33. […]

34. Examples of tools **that can be** used for identifying and assessing broader operational risk**s beyond the scope of risks captured under the SA-OR** include:[18]

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 internal loss data, near misses, and, when feasible, external operational loss event data (as external data is informative of risks that common across the industry). Event data is typically classified according to a taxonomy defined in the ORMF policies and consistently applied across the bank. Event data typically includes date of the event (occurrence date, discovery date, and accounting date) and, in the case of loss events, financial impact. When other root cause information for events is available, ideally it can also be included in the operational risk dataset. When feasible, banks are encouraged to also seek **voluntarily** to gather external operational risk event data and use this data in their internal analysis, as external is often informative of risks that are common across the industry.

b) […]

c) […]

d) […]

e) **Key risk indicators** ~~Metrics~~ – 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.

f) […]

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

a) Based on accurate data, whose integrity is ensured by strong governance and robust verification and validation procedures;

b) Adequately ~~taken into account~~ **considered** in the internal pricing and performance measurement mechanisms as well as for business opportunities assessments;

c) Subject to CORF monitored action plans or remediation plans when necessary.

1.2.1.2 Principle 7: 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.

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 (ie, throughout the full life-cycle of a product). [19]

It is also important to recognise that entering new markets will result in strategic and reputational risks, which are specifically excluded from the definition of operational risk whereas operational risk is clearly involved in new business/products process assessment. Therefore, the overlap between operational risk and the excluded categories such as strategic risk and reputational risk (which are commonly taken into account in firms' RCSAs) should be specified for a clear and consistent distinction to be factored into the risk taxonomies.

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**. Recognising diversity of first and second line of defence approaches across jurisdictions and bank risk management practices, the below example provides guidance on how the approach can be implemented**~~, in particular~~:

38. […]

39. ~~Banks should maintain a central record of their products and services to the extent possible (including the outsourced ones) to facilitate the monitoring of changes.~~

Monitoring and Reporting

1.2.1.3 Principle 8: 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.

40. […]

41. […]

42. […]

43. […]

Control and Mitigation

1.2.1.4 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.

44. […]

45. […]

46. […]

47. In addition to segregation of duties and dual controls, banks should ensure that other traditional internal ~~controls~~ **mitigants and controls** are in place, as appropriate, to address operational risk. Examples of these ~~controls~~ **mitigants and controls** include:

    a) […]

48. […]

49. […]

50. […]

    a) […]

    b) […]

    c) […]

    d) […]

    e) establishment of an effective control environment at the bank and the service provider (what should include a register of outsourced activities) **with appropriate metrics and reporting to facilitate oversight of the third party)**;

    f) […]

    g) […]

20 The Committee's paper Framework for Internal Control Systems in Banking Organisations, September 1998, discusses internal controls in greater detail.

21 For example, where a supposedly low risk, low margin trading activity generates high returns that could call into question whether such returns have been achieved as a result of an internal control breach.

51. ~~In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party such as through insurance. The board of directors should determine the maximum loss exposure the bank is willing and has the financial capacity to assume, and should perform an annual review of the bank's risk and insurance management programme. While the specific insurance or risk transfer needs of a bank should be determined on an~~

~~individual basis, many jurisdictions have regulatory requirements that must be considered.~~

52. **In those circumstances where exiting the risk or adequately addressing it through the use of internal controls do not constitute reasonable options, management can seek to transfer the risk to another party for example through insurance. Insurance can hence be used as a forward-looking risk mitigation tool that provides an incentive for banks to protect and transfer tail risk rather than transfer recurring losses[28]. In doing so, the board of directors should determine the maximum loss exposure the bank is willing and has the financial capacity to assume, and should expect senior management to perform a review of the bank's risk and insurance management programme when substantial changes to insurance coverage are introduced.**

Given the mitigation capability of insurance is not dependent on whether a bank is using a model-based (AMA) or standardised approach (SA), the use of insurance to offset a certain proportion of operational risk RWA should remain an option even after the transition to SA-OR. As such, certain elements from previously issued guidance around the use of insurance under AMA remains applicable[29] and thus, supervisory bodies should consider how the risk mitigation benefits can be recognised in ways that are compatible with the new Basel framework (e.g. capital deductions and/or Pillar 2).

28. Migueis 2019

29. See also the Committee's paper, Recognising the risk-mitigating impact of insurance in operational risk modelling, October 2010

52. ~~Because risk transfer is an imperfect substitute for sound controls and risk management programmes, banks should view risk transfer tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly identify, recognise and rectify distinct operational risk errors – or specific legal risk exposure – can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, transfer the risk to another business sector or area, or create a new risk (eg counterparty risk).~~

52. **In the same way as the use of controls to manage risk can result in some residual risk, it is important to recognise potential shortcomings of risk transfer mitigation techniques and therefore, institutions should have mechanisms in place to quickly identify, recognise and rectify distinct residual operational risk stemming from insurance policies (namely, legal, outsourcing and counterparty risk).**

53. Banks should have unified classification, methodology, procedures of operational risk management established by the CORF.

1.3 Information and communication technology

1.3.1.1 Principle 10: **As part of the operational risk management framework,** 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.

54. […]

55. […]

56. […]

1.4 Business continuity planning

1.4.1.1 Principle 11: **As part of the operational risk management framework, b**anks 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]

57. […]

a) […]

b) […]

c) […]

d) […]

58. […]

a) A bank should ground its business continuity policy on scenario analyses of potential disruptions that identify and categorise critical business operations and key internal or external dependencies. In doing so, banks should cover all ~~their~~ **material** business units as well as critical providers and major third parties (eg central banks, clearing house).

b) […]

c) […]

59. A bank should periodically review all components of its business continuity ~~policy~~ **program** to ensure **it** ~~that contingency strategies~~ remain**s** 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 **(including lessons learnt and remediation activities)** should be reported to senior management and the board of directors.

1.5 Role of Disclosure

1.5.1.1 Principle 12: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management and its operational risk exposure.

60. […]

61. ~~Banks should disclose relevant operational risk exposure information to their stakeholders (including significant operational loss events), while not creating operational risk through this disclosure (eg 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.~~

Banks should disclose relevant and non-publicly sensitive operational risk exposure information to their stakeholders (including significant operational loss events), while not creating operational risk through this disclosure (eg description of unaddressed control vulnerabilities). Sensitive events (e.g. cyber) should be reported to the relevant supervisory bodies in accordance with local requirements. In certain circumstances where this is not prohibited by law, it is recommended to share such information amongst peers and sector participants in order to raise awareness.

62. […]

1.6 Role of supervisors

63. […]

64. […]

65. […]

66. […]