BERMUDA MONETARY AUTHORITY

CONSULTATION PAPER

PROPOSED ADOPTION OF THE REVISED OPERATIONAL RISK PRINCIPLES FOR BANKS

CONTENTS

I. INTRODUCTION

1. The Bermuda Monetary Authority (Authority or BMA**)** requires a licenced institution to maintain risk management policies and procedures that are appropriate for their individual business profile and that it adopts and applies suitable arrangements for identifying, assessing, monitoring and controlling/ mitigating their operational risks. Consistent with the Basel Committee on Banking Supervision's (Basel) framework for assessing soundness and adequacy of capital, an institution must keep its operational risk frameworks under regular review to enhance the effectiveness of managing and controlling such risks.

2. Current guidance entitled *Banks and Deposit Companies Act 1999: The Management of Operational Risk* (2007 Guidance**)** was issued in 2007 and sets out the Authority's policy on managing operational risk by banks and deposit companies. These were largely based on Basel's *Principles for the Sound Management of Operational Risk* (Principles) issued in 2003.

3. Since 2003 the operational risk environment for financial institutions has changed significantly, with previous standards and practices proving to be inadequate and no longer commensurate with their evolving risk profiles.

4. In 2011, Basel revised the Principles to incorporate the lessons of the 2007-09 Financial Crisis and in 2014 performed a thematic review to gauge the extent to which banks had implemented the Principles. The 2014 review noted several implementation gaps which highlighted the need for further guidance related to:

    a. Risk identification and assessment tools, including risk and control self-assessments (RCSAs), key risk indicators, external loss data, business process mapping, comparative analysis, and the monitoring of action plans generated from various operational risk management tools
    b. Change management programmes and processes (and their effective monitoring)
    c. Implementation of the three lines of defence, especially by refining the assignment of roles and responsibilities
    d. Board of directors and senior management oversight
    e. Articulation of operational risk appetite and tolerance statements
    f. Risk disclosures

5. Basel also recognised that the 2011 Principles did not sufficiently capture certain important sources of operational risk, such as those arising from information and communication technology (ICT) risk, thus warranting the introduction of a specific principle on ICT risk management. Other revisions were made to ensure consistency with the new operational risk framework in the Basel III reforms.

6. In March 2021, Basel issued *Revisions to the Principles for the Sound Management of Operational Risk* (Revised Principles), which addressed the aforementioned

shortcomings. The Authority is seeking comment on the proposed adoption of the Revised Principles to replace the current 2007 Guidance.

7. Industry and other stakeholders are invited to provide feedback to the proposals outlined in this paper and in its various attachments, by emailing their comments to banking@bma.bm by close of business on 31 March 2022.

II. DEFINITION OF OPERATIONAL RISK

8. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. It must be noted that this definition includes legal risk but excludes strategic and reputation risk. Legal risk includes expenses (e.g., the establishment of a legal reserve) to fund litigation, adverse judgments or settlements, as well as fees and expenses for external legal advice for work related to specific incidents or cases. Therefore, such legal risks must be included within institutions' monitoring and reporting frameworks for operational risk. However, the operational risk would not include the cost of general legal advice on an institution's overall corporate strategy.

III. OPERATIONAL RISK MANAGEMENT FRAMEWORK

9. Banks commonly rely on three lines of defence: (i) business unit management, (ii) an independent corporate operational risk management function, and (iii) independent assurance. Depending on the nature, size, complexity and risk profile of a bank's activities, the degree of formality of how these three lines of defence are implemented will vary. A bank 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; and
    e. communicates with the other lines of defence to reinforce the operational risk management framework (ORMF).

10. In the Revised Principles, Basel outlines the expected roles and responsibilities for each of the three lines of defence. The Authority agrees with these Basel expectations and proposes to adopt them.

11. Institutions must put in place systems enabling them to identify and systematically track all material operational loss events. Generally, a materiality threshold of BM$10,000 should apply. Tracking must relate to operational risk loss event data rather than purely to losses occasioned by operational risk. This is because many operational risks may result in no financial loss or even in a profit (e.g., if a 'sell' instruction is incorrectly transacted as a 'buy', and, when unwound, the price proves to have moved in favour of the transacting institution). In such a case, where the potential risk of loss exceeds the reporting threshold, the case remains a 'loss event' since it could have resulted in a financial loss.

12. As part of the revisions, Basel summarises the current international consensus as to the seven major (Level 1) categories of operational risk as well as a breakdown of each Level 1 category into a number of sub-categories.[1]

IV. OPERATIONAL RISK CULTURE AND FRAMEWORK

PRINCIPLE 1 - OPERATIONAL RISK CORPORATE CULTURE

Sound operational risk management is a reflection of the effectiveness of the board of directors and senior management. 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 incentives for professional and responsible behaviour, and ensure that staff receives appropriate risk management and ethics training.

13. This principle addresses the need for the board of directors (board) to establish and maintain a robust operational risk corporate culture that is integrated into a bank's risk management framework, which includes the following:

    a. establishment of a code of conduct and/or ethics policy;
    b. setting clear expectations and responsibilities for the management of operational risk management; and
    c. alignment of compensation policies to approved risk appetite and tolerance statements.

PRINCIPLE 2 - OPERATIONAL RISK MANAGEMENT FRAMEWORK (ORMF)

Sound internal governance forms the foundation of an effective ORMF. A bank should develop, implement and maintain an operational risk management framework that is fully integrated into its overall risk management processes. The ORMF that is adopted will depend on a range of factors, including the bank's nature, size, complexity and risk profile.

14. This principle sets the expectation for a bank to implement a commensurate ORMF that addresses the need:

    a. for risk policies and procedures whilst also outlining the minimum critical elements these documents should cover;
    b. for the board to understand the nature and complexity of risks related to the bank's business operations;

[1] Paragraph 25.17: https://www.bis.org/basel_framework/chapter/OPE/25.htm?inforce=20230101&published=20200327

c. to be fully integrated into risk management processes by the bank's first line of defence, which is challenged by the second line of defence and reviewed by the third line of defence; and
d. to be embedded across all levels of the organisation (including business and strategy development).

V. GOVERNANCE

PRINCIPLE 3 – BOARD OF DIRECTORS

The board of directors should approve and periodically review the operational risk management framework, and ensure that senior management implements the policies, processes and systems for effective operational risk management at all decision levels.

15. This principle addresses the roles of the board in reviewing and maintaining an ORMF appropriate for the current operational risk profile of the bank.

PRINCIPLE 4 – OPERATIONAL RISK APPETITE AND TOLERANCE STATEMENT

The board of directors should approve and periodically review a risk appetite and tolerance statement for operational risk that articulates the nature, type and level of operational risks the bank is willing to assume.

16. This principle addresses the need for a bank to establish, monitor and review risk appetite and tolerance appetites that are proportional to the risks faced by the institution.

PRINCIPLE 5 – SENIOR MANAGEMENT

Senior management should develop a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility to be approved by the board. Senior management is responsible for consistently implementing and maintaining the organisation's policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the bank's risk appetite and tolerance statement.

17. This principle addresses the roles and responsibilities of a bank's senior management in implementing and maintaining a robust ORMF, including the need to:

a. establish policies and procedures;
b. implement and oversee operational risk tracking systems;

c. promote effective communication and coordination amongst staff to mitigate operational risk exposures;
d. designate an individual, with sufficient stature in the management structure, responsible for overseeing the ORMF;
e. ensure bank operations are conducted by staff with sufficient experience and skills; and
f. ensure that a bank's governance structure is commensurate with its risk profile;
g. ensure robust challenge mechanisms and effective issue resolution processes are implemented and maintained.

VI. RISK MANAGEMENT ENVIRONMENT

PRINCIPLE 6 – IDENTIFICATION AND ASSESSMENT

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.

18. This principle addresses the need for senior management to implement and maintain an effective operational risk identification and assessment process that includes the need for:

    a. *Event management* - analysis of events to identify new operational risks, understanding the underlying causes and control weaknesses, and formulating an appropriate response to prevent recurrence of similar events;
    b. *Operational risk event data* - operational risk event datasets that collect all material events experienced by the bank and serves as the basis for operational risk assessments;
    c. *Self-assessments* - evaluate inherent risk (before controls are considered), the effectiveness of the control environment, and residual risk (the exposure after controls are considered) and contain both quantitative and qualitative elements;
    d. *Control monitoring and assurance framework* - appropriate control monitoring and assurance framework facilitates a structured approach to the evaluation, review and ongoing monitoring and testing of key controls;
    e. *Metrics* - develop metrics to assess and monitor their operational risk exposure;
    f. *Scenario analysis* - method to identify, analyse and measure a range of scenarios, including low probability and high severity events, some of which could result in severe operational risk losses; and
    g. *Benchmarking and comparative analysis* - comparisons of the outcomes of different risk measurement and management tools deployed within the bank and comparisons of metrics from the bank to other firms in the industry.

PRINCIPLE 7 – CHANGE MANAGEMENT PROCESS

Senior management should ensure that the bank's change management process is comprehensive, appropriately resourced and adequately articulated between the relevant lines of defence.

19. This principle addresses the need for a bank to develop and maintain an effective change management process, which includes but is not limited to:

    a. establishing policies and procedures defining the process for identifying, managing, challenging, approving and monitoring change on the basis of agreed objective criteria, which should be reviewed periodically;
    b. having policies and procedures for the review and approval of new products, activities, processes and systems; and
    c. maintaining a central register of products and services to facilitate changes.

PRINCIPLE 8 – MONITORING AND REPORTING

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.

20. This principle addresses senior management's responsibility to implement and maintain an effective operational risk monitoring and reporting process that includes the need to:

    a. ensure operational risk reports are comprehensive and accurate;
    b. ensure production and issuance of operational risk reports are timely in normal and stressful environments;
    c. ensure reports describe the operational risk profile of the bank; and
    d. review data capture and risk reporting processes to ensure adequacy.

PRINCIPLE 9 – CONTROL AND MITIGATION

A bank should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

21. This principle addresses the need for a bank to implement and maintain a strong internal control environment that consists of four components:

    a. Risk assessment;
    b. Control activities;
    c. Information and communication; and
    d. Monitoring activities

VII. INFORMATION AND COMMUNICATION TECHNOLOGY

PRINCIPLE 10 – ICT RISK MANAGEMENT

A bank should implement a robust information and communication technology (ICT) risk management programme in alignment with its operational risk management framework.

22. This principle addresses the need for a bank to ensure that it retains appropriate oversight of its ICT framework, which should be reviewed regularly to ensure it remains commensurate with the risk profile. ICT risk management should include:

    a. ICT risk identification and assessment;
    b. ICT risk mitigation measures consistent with the assessed risk level (e.g., cybersecurity, response and recovery programmes, ICT change management processes, ICT incident management processes, including relevant information transmission to users on a timely basis);
    c. monitoring of these mitigation measures (including regular tests); and
    d. to ensure compliance with Authority issued guidance and/or codes related to cybersecurity.

VIII. BUSINESS CONTINUITY PLANNING

PRINCIPLE 11 – BUSINESS CONTINUITY PLANNING FRAMEWORK

A bank should have business continuity plans (BCPs) in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption. Business continuity plans should be linked to the bank's operational risk management framework.

23. This principle addresses the need for a bank to formulate and maintain commensurate BCP strategies and disaster recovery plans, including the need for:

    a. regular board review and approval;
    b. strong involvement of the senior management and business unit leaders in its implementation;
    c. the commitment of the first and second lines of defence to its design;
    d. regular review by the third line of defence; and
    a. utilisation of forward-looking BCP and scenario analyses.

IX. ROLE OF DISCLOSURES

PRINCIPLE 12 – ORMF AND OPERATIONAL RISK EXPOSURE DISCLOSURES

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

24. This principle addresses the scope of public disclosure requirements regarding a bank's operational risk management and operational risk exposures. A bank should:

    a. disclose relevant and commensurate operational risk information in a manner that allows stakeholders to determine the adequacy of its ORMF; and
    b. establish a formal disclosure policy that is subject to regular and independent review.

X. IMPLEMENTATION DATE

25. The Authority proposes to implement the revised principles effective 1 January 2023.