مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

OPERATIONAL RISK STANDARDS

CONTENTS

INTRODUCTION

1. These Standards form part of the Operational Risk Regulation. All Banks must comply with these Standards, which expand on the Regulation. These Standards are mandatory and enforceable in the same manner as the Regulation.

2. Operational risk is inherent in all dimensions of a Bank, including all banking products, activities, processes and systems. Accordingly, the effective management of operational risk is a fundamental element of a Bank's risk management program. Banks with a sound operational risk management framework, a strong risk management culture and ethical business practices, are less likely to experience potentially damaging operational risk events and better placed to deal effectively with those events that do occur.

3. A Bank's Board is in ultimate control of the Bank and accordingly ultimately responsible for operational risk management. There is no one-size-fits-all or single best solution. Accordingly, each Bank could meet the minimum requirements of the Regulation and Standards in a different way and thus may adopt an organizational framework appropriate to the risk profile, nature, size and complexity of its business and structure. The onus is on the Board to demonstrate that it has implemented an appropriate approach to operational risk management. Banks are encouraged to adopt leading practices that exceed the minimum requirements of the Regulation and Standards.[1]

4. The Standards follow the structure of the Regulation, with each article corresponding to the specific article in the Regulation.

ARTICLE 1: DEFINITIONS

1. **Affiliate:** An entity that, directly or indirectly, is controlled by, or is under common control with another entity. The term control as used herein shall mean the holding, directly or indirectly, of voting rights in another entity, or of the power to direct or cause the direction of the management of another entity.

2. **Bank:** A financial entity, which is authorized by the Central Bank to accept deposits as a Bank.

3. **Board:** The Bank's Board of Directors.

4. **Central Bank:** The Central Bank of the United Arab Emirates.

5. **Central Bank Law:** Federal Law No (10) of 1980 concerning the Central Bank, the Monetary System and Organization of Banking as amended or replaced from time to time.

[1] The Central Bank will apply the principle of proportionality in the enforcement of the Regulation and Standards, whereby smaller banks may demonstrate to the Central Bank that the objectives are met without necessarily addressing all of the specifics cited in the Standards.

6. **Central Bank regulations:** Any resolution, regulation, circular, rule, standard or notice issued by the Central Bank.

7. **Group:** A group of entities that includes an entity (the 'first entity') and:

   a. any Parent of the first entity;

   b. any Subsidiary of the first entity or of any Parent of the first entity; and

   c. any Affiliate.

8. **Higher Shari'a Authority:** The Higher Shari'a Authority for Islamic banking and financial activities that was established by the Cabinet Resolution no. 2016 (1/35/102) at the Central Bank.

9. **Inherent risk**: The risk existing if no controls or other mitigating factors are in place.

10. **Islamic Financial Services:** Shari'a compliant financial services offered by Islamic Banks and Conventional Banks offering Islamic banking products (Islamic Windows).

11. **Operational risk:** 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.

12. **Parent:** An entity (the 'first entity') which:

   a. holds a majority of the voting rights in another entity (the 'second entity');

   b. is a shareholder of the second entity and has the right to appoint or remove a majority of the Board or managers of the second entity; or

   c. is a shareholder of the second entity and controls alone, pursuant to an agreement with other shareholders, a majority of the voting rights in the second entity;

   Or;

   d. If the second entity is a subsidiary of another entity which is itself a subsidiary of the first entity.

13. **Residual risk:** The risk exposure after controls are considered.

14. **Risk appetite:** The aggregate level and types of risk a Bank is willing to assume, decided in advance and within it risk capacity, to achieve its strategic objectives and business plan.

15. **Risk governance framework:** As part of the overall approach to corporate governance, the framework through which the Board and management establish and make decisions about the Bank's strategy and approach to risk management; articulate and monitor adherence to the risk appetite and risks limits relative to the Bank's strategy; and identify, measure, manage and control risks.

16. **Risk limits:** Specific quantitative measures that may not be exceeded, based on, for example, forward looking assumptions that allocate the Bank's aggregate risk appetite to business lines, legal entities or

management units within the Bank or Group in the form of specific risk categories, concentrations or other measures, as appropriate.

17. **Risk Management function:** Collectively, the systems, structures, policies, procedures and people that measure, monitor and report risk on a Bank-wide and, if applicable, Group-wide basis.

18. **Senior Management:** The executive management of the Bank responsible and accountable to the Board for the sound and prudent day-to-day management of the Bank, generally including, but not limited to, the chief executive officer, chief financial officer, chief risk officer and heads of the compliance and internal audit functions.

19. **Subsidiary:** An entity (the 'first entity') is a subsidiary of another entity (the 'second entity') if the second entity:

    a. holds a majority of the voting rights in the first entity;

    b. is a shareholder of the first entity and has the right to appoint or remove a majority of the Board or managers of the first entity; or

    c. is a shareholder of the first entity and controls alone, pursuant to an agreement with other shareholders, a majority of the voting rights in the first entity;

    Or;

    d. If the first entity is a subsidiary of another entity that is itself a subsidiary of the second entity.

ARTICLE 2: OPERATIONAL RISK GOVERNANCE FRAMEWORK

1. The fundamental premise of sound risk management is that the Board and the management of a Bank understand the nature and complexity of the risks inherent in the portfolio of the Bank's products, services and activities. This is particularly important for operational risk.

2. A Bank must establish, implement and maintain an operational risk governance framework, which enables it to identify, assess, evaluate, monitor, mitigate and control operational risk. The operational risk governance framework consists of policies, processes, procedures, systems and controls.

3. The operational risk governance framework must be documented and approved by the Board of the Bank, must provide for a sound and well-defined framework to address the Bank's operational risk and must include definitions of operational risk and material operational loss.

4. A Board is responsible for establishing, maintaining and overseeing a robust operational risk governance framework that must take into account the risk profile, nature, size and complexity of the Bank's business and structure.

5. A Board must approve and subsequently review, at least annually, a risk appetite statement for operational risk that articulates the nature, types and levels of operational risk that the Bank is willing to assume and that sets appropriate limits and thresholds.

6. The operational risk governance framework must be fully integrated into the Bank's overall risk governance framework and risk management processes. This applies to all levels and areas of the Bank including to business lines and, if applicable, to Group levels, as well as new business initiatives, products, activities, processes and systems.

7. The operational risk governance framework must clearly:

    a. Identify the governance structures used to manage operational risk, including reporting lines, responsibilities and accountabilities;

    b. Establish operational risk reporting and management information systems;

    c. Provide for periodic independent review and assessment of operational risk; and

    d. Require policies to be reviewed and revised as appropriate, whenever a material change in the operational risk profile of the Bank occurs.

8. Larger or more complex Banks must have an Operational Risk Committee or other designated committee that addresses operational risk.

9. A Bank must measure operational risks for capital purposes using the approach most appropriate to the risk profile, nature, size and complexity of the Bank's business and structure. Holding capital against operational risks, however, is not a substitute for effective operational risk management.

10. A Bank must meet the following minimum criteria or demonstrate to the Central Bank that its framework meets the requirements for a comprehensive approach to operational risk management without the presence of all of the criteria enumerated below.

    a. A Bank must have an operational risk management system with clear responsibilities assigned to an operational risk management function. These responsibilities must include, but not be limited to, developing strategies to identify, assess, monitor and control or mitigate operational risk; codifying bank-level policies and procedures concerning operational risk management and controls; the design and implementation of the Bank's operational risk assessment methodology; and the design and implementation of a risk-reporting system for operational risk.

    b. A Bank must systematically track relevant operational risk data including material losses by business line. Its operational risk assessment system must be closely integrated into the risk management processes and procedures of the Bank. Its output must be an integral part of the process of and procedures for monitoring and controlling the Banks operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting and risk analysis. The Bank must have techniques for creating incentives to improve the management of operational risk throughout the Bank.

    c. There must be regular reporting of operational risk exposures, including material operational losses, to business unit management, Senior Management and to the Board. The Bank must have procedures for taking appropriate action according to the information within the management reports.

d. A Bank's operational risk management system must be well documented. A Bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which must include policies for the treatment of non-compliance issues.

e. A Bank's operational risk management processes and assessment system must be subject to regular internal audit review. These reviews must include both the activities of the business units and of the operational risk management function.

ARTICLE 3: BOARD OF DIRECTORS

1. The Board must establish and maintain a strong operational risk management culture, which has to be guided by strong operational risk management that supports and provides appropriate standards and incentives for professional and responsible behaviour. The Board must ensure that a strong control environment is established and maintained.

2. The Board must establish and maintain a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identifies acceptable business practices and prohibits conflicts of interest.

ARTICLE 4: SENIOR MANAGEMENT

1. Senior Management must consistently implement and maintain throughout the Bank (and, if applicable, Group) policies, processes and systems for managing operational risk in all material products, activities, processes and systems, consistent with the risk appetite statement.

2. Senior Management must clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability and to ensure that the necessary resources are available to manage operational risk in line with the Bank's risk appetite statement. The management oversight process for operational risk must be appropriate to the risks inherent in a business unit's activities.

3. Senior Management must ensure that the control environment provides for appropriate independence and segregation of duties. The approach to operational risk management must incorporate the "three lines of defence" approach:

   a. Business line management responsible for identification and control of risks;

   b. Control functions of risk management and compliance; and

   c. Internal audit to provide independent assurance.

4. Senior Management must implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms must be in place at the Board, senior management and business line levels that support proactive management of operational risk.

5. Senior Management must ensure that an appropriate level of operational risk training is available at all levels throughout the Bank. Training that is provided must reflect the seniority, role and responsibilities of the individuals for whom it is intended.

ARTICLE 5: IDENTIFICATION AND ASSESSMENT

1. A Bank must identify and assess the operational risk inherent in all material products, activities, processes and systems. Effective identification and assessment considers both internal and external factors. This must include any operational risk arising from common points of exposure, such as a single external service provider serving the Bank.[2]

2. A Bank's approach to assessment of operational risk at a minimum must address the following items:

   a. Determining which operational risk assessment tools will be employed by the Bank and how they are to be used;

   b. Establishing and monitoring thresholds or limits for inherent and residual risk exposure;

   c. Calibration of identified risks against operational risk appetite limits, as well as thresholds or limits for inherent and residual risk and approved risk mitigation strategies and instruments; and

   d. Providing for common operational risk terminology to ensure consistency of risk identification and assessment on a bank-wide or, if applicable, Group-wide basis.

3. A Bank must take into account its assessment of operational risk in its internal pricing and performance monitoring mechanisms.

ARTICLE 6: CONTROL AND MITIGATION

1. A Bank must have a strong control environment, including but not limited to, appropriate segregation of duties and dual control. Areas of potential conflicts of interest must be identified, minimized and be subject to careful independent monitoring[3] and review.

2. A Bank, in addition to segregation of duties and dual control, must ensure that other traditional internal controls are in place. Such controls include but are not limited to:

   a. Clearly established authorities and/or processes for approval;

   b. Close monitoring of adherence to assigned risk thresholds or limits;

   c. Safeguards for access to and use of, Bank assets and records;

   d. Appropriate staffing level and training to maintain expertise;

   e. Ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;

[2] Appendix 1 provides examples of tools that may be used for identifying and assessing operational risk.

[3] Independent monitoring may be done by the internal audit function or an external consultant, subject to the party having the appropriate skills to do so. The Central Bank will expect the Bank to explain and evidence its decision of how it chose an independent party and how their skills were assessed.

f. Regular verification and reconciliation of transactions and accounts; and

g. A vacation policy that requires officers and employees to take a minimum leave of absence as determined by the Bank.

3. Risk transfer and mitigation tools such as insurance are imperfect substitutes for sound controls and risk management so Banks must utilize risk transfer tools as complementary to, rather than a replacement for, internal operational risk control.

ARTICLE 7: DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT

1. Disaster recovery and business continuity planning must consider the whole of the Bank or Group, if applicable, to identify, assess and mitigate potential business continuity risks and ensure that the Bank is able to meet its financial and service obligations in the event of business disruptions.

2. A Bank's business continuity management (BCM) policy must be documented, set out its objectives and approach to BCM and be up-to-date. The BCM policy must clearly state the roles, responsibilities and authorities to act in relation to the BCM policy.

3. A Bank must conduct business impact analysis (BIA) and risk assessment on an ongoing basis. A BIA involves identifying all critical business functions and assessing the impact of a disruption on these.

4. Critical business functions are the business operations, resources and infrastructure that may, if disrupted, have a material impact on the Bank's business functions, reputation, profitability or customers.

5. When conducting the BIA, a Bank must consider at a minimum:

   a. Disruption scenarios over varying periods of time;

   b. The period of time for which the Bank could not operate without each of its critical business operations;

   c. The extent to which a disruption to the critical business operations might have a material impact on customers of the Bank; and

   d. The financial, legal, regulatory and reputational impact of a disruption to a Bank's critical business operations over varying periods.

6. A Bank must identify and document appropriate recovery objectives and implementation strategies based on the results of the BIA, taking into account the risk profile, nature, size and complexity of the Bank's business and structure. Recovery objectives are pre-defined goals for restoring critical business operations to a specified level of service (recovery level) within a defined period (recovery time) following a disruption.

7. A Bank must maintain at all times a documented business continuity plan (BCP) that meets the objectives of the BCM policy. The BCP must reflect the specific requirements of the Bank and must identify:

a. Critical business operations;

b. Recovery levels and time targets for each critical business operation;

c. Recovery strategies for each critical business operation;

d. Infrastructure and resources required to implement the BCP;

e. Roles, responsibilities and authorities to act in relation to the BCP; and

f. Communication plans with staff and external stakeholders.

8. A Bank must review and test its BCP at least annually or more frequently if there are material changes to business operations, to ensure that staff can effectively execute contingency plans and that recovery and resumption objectives and timeframes can be met. The results of the testing must be reported formally to the Board or to designated Senior Management in line with the BCM policy. The BCP must be updated if shortcomings are identified as a result of the review and testing.

ARTICLE 8: INFORMATION TECHNOLOGY

1. A Bank's effective use and sound implementation of technology can contribute to the control environment. However, use of technology-related products, activities, processes and delivery channels exposes a Bank to strategic, operational and reputational risks and the possibility of material financial loss. Automated processes introduce risks that must be addressed through technology governance and infrastructure risk management programmes, including an information security management system.

2. A Bank must have an integrated approach to identifying, measuring, monitoring and managing technology risk. Technology risk management includes but is not limited to:

a. Governance and oversight controls that ensure technology, including outsourcing arrangements, are aligned with and supportive of the Bank's business objectives;

b. Establishment and maintenance of appropriate information technology policies, procedures and processes to identify, assess, monitor and manage technology risks;

c. Establishment of a risk appetite statement and limits as well as performance expectations to assist in controlling and managing risk;

d. Implementation of an effective control environment;

e. Monitoring processes that test for compliance with policy thresholds or limits; and

f. Establishment and maintenance of appropriate and sound information technology infrastructure to meet the current and projected business requirements of the Bank under normal circumstances and in periods of stress and which ensures data and system integrity, security and availability.

ARTICLE 9: SYSTEMS AND INTERNAL REPORTING

1. A Bank must have information systems that enable accurate and timely monitoring of and reporting on operational risk. The level of sophistication of a Bank's operational risk information system must be calibrated to the risk profile, complexity and systemic importance of the Bank.

2. The processes for aggregating the necessary data and producing operational risk management reports must be fully documented. These must include standards, cut-off times and schedules for report production. The aggregation and reporting process must be subject to high standards of validation through periodic review by the internal audit function using staff with specific systems, data and reporting expertise, particularly where the process requires substantial manual intervention.

3. Operational risk reports to Senior Management and the Board must provide aggregate information as well as sufficient supporting detail to enable Senior Management and the Board to understand and assess the Bank's operational risk exposures.

ARTICLE 10: REPORTING REQUIREMENTS AND DISCLOSURE

1. A Bank must notify the Central Bank promptly and no later than 24 hours after experiencing an operational risk event that triggers, or is likely to trigger, disaster recovery or business continuity plans, or has, or is likely to have, a significant impact on the Bank's operations, profitability or capital. The Bank must explain to the Central Bank the nature of the event, actions being taken, the likely effect and the timeframe for returning to normal operations, where applicable. The Bank must notify the Central Bank when normal operations resume.

2. A Board-approved disclosure policy must provide for the Bank's publication of sufficient information on operational risk and controls to allow stakeholders to assess its approach to operational risk management and to determine whether the Bank identifies, assesses, evaluates, monitors and controls and mitigates operational risk effectively. In addition, a Bank must implement a process for assessing the appropriateness of its operational risk disclosures.

3. Branches and Subsidiaries of foreign Banks operating in the UAE may largely rely on the Group's disclosures, supplemented by disclosure, at least annually through their websites that are dedicated to their activities in the UAE, of a summary of the local branch or Subsidiary's operational risk management framework.

4. A Bank's public disclosures must be commensurate with the size, risk profile and complexity of a Bank's operations and evolving industry practice. A Bank's disclosures must be consistent with how Senior Management and the Board assess and manage the operational risk of the Bank.

ARTICLE 11: NEW BUSINESSES, PRODUCTS AND SYSTEMS

1. In general, a Bank's operational risk exposure is increased when a Bank engages in new activities, develops new products, enters unfamiliar markets, implements new business processes or technology systems and/or engages in businesses that are geographically distant from its head office. A Bank must ensure that its risk management control infrastructure is appropriate and that it keeps pace with the development of or changes to its products, activities, processes and systems.

2. A Bank must have policies and procedures that address the process for review and approval of new products, activities, processes and systems. The review and approval process must consider at a minimum:

   a. Inherent risks, including but not limited to legal risks, in the new product, service or activity;

   b. Changes to the Bank's risk profile and operational risk appetite, including the risk of existing products or activities;

   c. The necessary controls, risk management processes and risk mitigation strategies;

   d. Residual risk;

   e. Changes to relevant risk thresholds or limits;

   f. Procedures and metrics to measure, monitor and manage the risk of the new product or activity; and

   g. Whether appropriate investment has been made for human resources and technology infrastructure before new products are introduced.

3. A Bank must ensure that the implementation of new products, activities, processes and systems is monitored in order to identify any material differences to the expected operational risk profile and to manage any unexpected risks.

ARTICLE 12: ISLAMIC BANKING

1. A Bank offering Islamic financial services must have in place adequate systems and controls, including a Shari'a Control Committee, to ensure compliance with Shari'a provisions. This includes policies and procedures for the approval of Islamic products, contracts and activities.

2. A Bank offering Islamic financial services must keep track of income not recognized arising from Shari'a non-compliance and assess the probability of similar cases arising in the future. Based on historical reviews and potential areas of Shari'a non-compliance, the Bank must assess potential profits that cannot be recognized as eligible Islamic Banking profits.

3. A Bank offering Islamic financial services must undertake a Shari'a compliance review at least annually, performed either by a separate Shari'a Audit function or as part of the existing internal and external audit function by persons having the required knowledge and expertise. The objective must be to ensure that the nature of the Bank's financing and equity investment and its operations are executed in adherence to the applicable Shari'a rules and principles as per the fatwa, policies and procedures approved by the Shari'a Control Committee in accordance with the requirements set by the Central Bank and the Higher Shari'a Authority.

4. A Bank offering Islamic financial services must establish and implement a clear and formal policy for undertaking its different and potentially conflicting roles in respect of managing different types of investment accounts. The policy relating to safeguarding the interests of its investment account holders may include but is not limited to:

a. Identification of investing activities that contribute to investment returns and taking reasonable steps to carry on those activities in accordance with the Bank's fiduciary and agency duties and to treat all its fund providers appropriately and in accordance with the terms and conditions of its investment agreements;

b. Allocation of assets and profits between the Bank and its investment account holders must be managed and applied appropriately to investment account holders having funds invested over different investment periods;

c. Determination of appropriate reserves at levels that do not discriminate against the right for better returns of existing investment account holders; and

d. Limiting the risk transmission between current and investment accounts.

5. A Bank offering Islamic financial services must adequately disclose information on a timely basis to its investment account holders and the markets in order to provide a reliable basis for assessing its risk profile and investment performance.

6. A Bank offering Islamic financial services must maintain separate accounts in respect of the Bank's operations undertaken for restricted investment account holders and ensure proper maintenance of records for all transactions in investments.

APPENDIX 1: TOOLS FOR IDENTIFYING AND ASSESSING OPERATIONAL RISK

Examples of tools[4] that may be used for identifying and assessing operational risk include:

- **Internal loss data collection and analysis**: Internal operational loss data provides meaningful information for assessing a Bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic. Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses in order to obtain a more complete view of their operational risk exposure.
- **External data collection and analysis**: External data elements consist of gross operational loss amounts, dates, recoveries and relevant causal information for operational loss events occurring at organizations other than the Bank. External loss data can be compared with internal loss data, or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures.
- **Risk assessments:** In a risk assessment, often referred to as a risk self-assessment, a Bank assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact. A similar approach, risk control self-assessments (RCSA), typically evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment and residual risk (the risk exposure after controls) are considered. Scorecards built on RCSAs by weighting residual risks provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment.
- **Business process mapping:** Business process mappings identify the key steps in business processes, activities and organizational functions. They also identify the key risk points in the overall business process. Process maps can reveal individual risks, risk interdependencies and areas of control or risk management weakness. They also can help prioritize subsequent management action.
- **Risk and performance indicators**: Risk and performance indicators are risk metrics and/or statistics that provide insight into a Bank's risk exposure. Risk indicators, often referred to as Key Risk Indictors (KRIs), provide insight into the status of operational processes, which in turn may provide insight into operational weaknesses, failures and potential loss. Risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans.
- **Scenario analysis:** Scenario analysis is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome. Scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions. Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process.
- **Models**: Larger Banks may find it useful to quantify their exposure to operational risk by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure. The results of the model can be used in an economic capital process and can be allocated to business lines to link risk and return.

[4] Banks are encouraged to use a range of tools to gain an understanding of their operational risks, in a manner consistent and proportional with the size and complexity of the bank and the operational risks it faces.

- **Comparative analysis**: Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the Bank's operational risk profile. For example, comparison of the frequency and severity of internal data with RCSAs can help the Bank determine whether self-assessment processes are functioning effectively. Scenario data can be compared to internal and external data to gain a better understanding of the severity of the Bank's exposure to potential risk events.
- **Audit findings:** While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external factors. Banks must not solely rely on internal audit to identify operational risks.