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

INTERNAL CONTROLS, COMPLIANCE AND INTERNAL AUDIT STANDARDS

Table of Contents

INTRODUCTION

1. These Standards form part of the Internal Controls, Compliance and Internal Audit Regulation. All Banks are required to comply with these Standards, which expand on the Regulation. These Standards are mandatory and enforceable in the same manner as the Regulation.

2. The Board is in ultimate control of the Bank and accordingly ultimately responsible for the Bank's approach to internal controls, compliance and internal audit. 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 a comprehensive approach to internal controls, compliance and internal audit. Banks are encouraged to adopt leading practices that exceed the minimum requirements of the Regulation and Standards.[1]

3. 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 owned by another entity by more than 25% and less than 50% of its capital.

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

6. **Conflict of interest:** A situation of actual or perceived conflict between the duty and private or other interests of a person, which could improperly influence the performance of his or her duties and responsibilities.

7. **Control Functions:** Those functions that have a responsibility independent from management to provide objective assessment, reporting and/or assurance; this includes the risk management function, the compliance function and the internal audit function.

8. **Controlling Shareholder:** A shareholder who has the ability to directly or indirectly influence or control the appointment of the majority of the board of directors, or the decisions

[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.

made by the board or by the general assembly of the entity, through the ownership of a percentage of the shares or stocks or under an agreement or other arrangement providing for such influence.

9. **Compliance function:** An independent function that identifies, assesses, advises on, monitors and reports on the Bank's compliance risk.

10. **Compliance risk:** The risk of legal or regulatory sanctions, material financial loss, or loss to reputation a Bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities.

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

a. any Controlling Shareholder of the first entity;

b. any Subsidiary of the first entity or of any Controlling Shareholder of the first entity; and

c. any Affiliate.

12. **Internal Audit function:** An independent function that provides independent assurance to the Board of directors and Senior Management on the quality and effectiveness of a Bank's internal control, risk management and governance systems and processes, thereby helping the Board and Senior Management protect their organization and its reputation.

13. **Internal Control:** Consists of five interrelated elements, whose effective functioning is essential to achieving a Bank's performance, information, and compliance objectives:

a. management oversight and the control culture;

b. risk recognition and assessment;

c. control activities and segregation of duties;

d. information and communication; and

e. monitoring activities and correcting deficiencies.

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

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

16. **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.

17. **Subsidiary:** An entity, owned by another entity by more than 50% of its capital, or is under full control of that entity regarding the appointment of the board of directors.

ARTICLE (2): INTERNAL CONTROL FRAMEWORK

1. The Board or the Board audit committee must review, at least annually, the effectiveness of the Bank's internal control system and processes by means of:

a. periodic discussions with Senior Management concerning the effectiveness of the internal control system;

b. a timely review of evaluations of internal controls made by Senior Management, internal auditors, and external auditors;

c. periodic efforts to ensure that Senior Management has promptly followed up on recommendations and concerns expressed by internal auditors and external auditors and the Central Bank on internal control weaknesses, and

d. a periodic review of the appropriateness of the Bank's strategy and risk limits.

2. Banks' internal controls must, at a minimum, address:

a. Organizational structure: definitions of duties and responsibilities including clear delegation of authority, such as loan approval limits, decision-making policies and processes and separation of critical functions, including but not limited to business origination, payments, reconciliation, risk management, accounting, audit and compliance;

b. Accounting and financial reporting policies and processes: reconciliation of accounts, control lists, information for management;

c. Checks and balances (or "four-eyes" principle): segregation of duties, cross-checking, dual control of assets, double signatures; and

d. Safeguarding assets and investments: physical control and computer access, measures for the prevention and early detection and reporting of misuse, such as fraud, embezzlement, unauthorized trading and computer intrusion.

3. The relationship between a Bank's business units, the support and control functions and the internal audit function comprises the three lines of defence model:

a. The business units are the first line of defence. They undertake risks within assigned limits of risk exposure and are responsible and accountable for identifying, assessing and controlling the risks of their business.

b. The second line of defence includes the support and control functions, such as risk management, compliance, legal, human resources, finance, operations, and technology. Each of these functions, in close relationship with the business units, ensures that risks in the business units have been appropriately identified and managed. The business support and control functions work closely to help define strategy, implement Bank policies and procedures, and collect information to create a Bank-wide view of risks.

c. The third line of defence is the internal audit function that independently assesses the effectiveness of the processes created in the first and second lines of defence, and provides assurance on these processes.

4. The responsibility for internal control does not transfer from one line of defence to the next line.

Line of defence	Examples	Approach
First line	Front Office, any client-facing activity	Transaction-based, ongoing
Second line	Risk Management, Compliance, Legal, Human Resources, Finance, Operations, and Technology	Risk-based, ongoing or periodic
Third line	Internal Audit	Risk-based, periodic

ARTICLE (3): COMPLIANCE FUNCTION

1. Compliance must be part of the culture of the Bank, not just the responsibility of staff in the Bank's compliance function.

2. A Bank's Board-approved compliance policy must at a minimum address the following issues with respect to the compliance function:

a. The compliance function's standing within the Bank, its authority, its responsibilities and its relations with other control functions;

b. The purpose and scope of the compliance function and a description of its reporting lines to the chief executive officer, the Board and the Board risk committee/Board audit committee;

c. Its right to obtain access to information necessary to carry out its responsibilities, and the corresponding duty of Bank staff to co-operate in supplying this information;

d. Its right to conduct investigations of possible breaches of the compliance policy and to appoint external experts to perform this task if appropriate;

e. Its right to influence, and when necessary, challenge Senior Management decisions if compliance risks are identified;

f. The measures to ensure its independence; and

g. The process for timely escalation of breaches of the policy.

3. The compliance function must, at a minimum, undertake the following responsibilities and tasks in relation to anti-money laundering and countering the financing of terrorism:

a. Detection of money laundering/terrorist financing operations/organizations;

b. Examination of suspicious transactions and identification of those to be reported to the Central Bank's Financial Intelligence Department (FID);

c. Bi- annual assessment of the Banks' anti-money laundering & countering the financing of terrorism compliance framework and transmission of the assessment report to FID. Copies of such reports, along with Senior Management comments and decisions, must be sent to FID bi-annually;

d. Implementation, in coordination with FID as needed, of an on-going training programme on money laundering and terrorist financing; and

e. Any other cooperation with FID upon its request.

4. Compliance function staff must have a sound understanding of laws, regulations, rules and standards relevant to the Bank's business and keep abreast with their developments. The professional skills of compliance function staff must be maintained through regular and systematic education and training, including courses on real cases relating to money laundering and financing of terrorism.

5. The compliance function must have access to any member of staff and all records and data of the Bank, and if applicable the Bank's Subsidiaries and Affiliates, which is required to fulfil the mandate established by the Bank's compliance policy.

6. A consistent approach to compliance across the Group may be achieved through the establishment of a Group compliance function accountable to the Board of the Controlling Shareholder, or through compliance functions established in each entity (or branch) and accountable to those entities' Boards and also reporting to the Group's head of compliance.

7. In cases where compliance function staff are embedded in independent support or control units (e.g. legal, finance, financial crime or control, risk management), a separate reporting line from staff in these units to the head of compliance is necessary. These units must co-operate closely with the head of compliance to ensure that the head of compliance can perform his or her responsibilities effectively.

8. The head of compliance must not have direct business line responsibilities in the Bank. Compliance function staff must perform only compliance responsibilities. A close and co-operative working relationship between the compliance function and business units must be in place in order to identify and manage compliance risks at an early stage.

9. Banks must have processes for reporting, at least quarterly, on compliance risk to Senior Management and the Board. The compliance function's reports must at a minimum:

a. address compliance risk assessments that have taken place during the reporting period, including any changes in the compliance risk profile based on relevant measurements such as performance indicators;

b. summarize any identified breaches and/or deficiencies and the corrective measures recommended to address them; and

c. report on corrective measures already taken.

10. The Board, the Board audit committee or the Board risk committee must assess, at least annually, the performance of the compliance function. This must include an independent external quality assurance review of the compliance function at least once every five years.

11. Banks must ensure that any outsourcing arrangements do not impede effective supervision by the Central Bank. Specific tasks of the compliance function may be outsourced, but they must remain subject to appropriate oversight by the head of compliance. Regardless of the extent to which specific tasks of the compliance function are outsourced, the Board and Senior Management remain responsible for compliance by the Bank with all applicable laws, regulations, standards and the instructions of the Central Bank.

ARTICLE (4): INTERNAL AUDIT FUNCTION

1. The internal audit function must be accountable to the Board or the Board audit committee on all matters related to the performance of its mandate as described in the internal audit charter.

2. The internal audit function must independently evaluate the:

a. Effectiveness and efficiency of internal control, risk management, and compliance systems;

b. Reliability and integrity of management information systems and processes;

c. Compliance with laws, regulations, standards and the instructions of the Central Bank; and

d. Safeguarding of assets.

3. The Board and Senior Management must respect and promote the independence of the internal audit function by ensuring that internal audit reports are provided to the Board or the Board audit committee without management filtering, and that the internal audit function staff have direct access to the Board or the Board audit committee. The Central Bank may request to receive internal audit reports.

4. The internal audit reports must contain the auditee's response, clearly indicating the auditee's acceptance or non-acceptance of the internal audit finding. If accepted by the auditee, a justifiable reason for non-performance and the corresponding action plan must be provided, stating the completion time frame and responsible body for implementation. If not accepted by the auditee, a justifiable reason with supporting evidence must be provided for the finding's re-consideration during an escalation procedure.

5. The Board audit committee must ensure that the head of internal audit is a person of integrity and seniority in the Bank to credibly challenge the business units, support and other control functions of the Bank and, if applicable, Group. He/she must be a very well qualified person, academically or through a professional qualification, with a working experience of not less than 5 years in auditing of banking or financial business.

6. The head of internal audit and all internal audit function staff must avoid conflicts of interest. Internally recruited internal audit function staff must not engage in auditing activities for which they have had previous responsibility before a "cooling off" period of at least one full financial year has elapsed. Staff rotations within the internal audit function as well as to and from the

internal audit function must be governed by and conducted in accordance with a written policy. The policy should be designed to avoid conflicts of interest, including the observance of an appropriate "cooling-off" period following an individual's return to the internal audit staff, before that individual audits activities in the functional area of the bank where his/her rotation had been served.

7. The head of internal audit is responsible for acquiring human resources with sufficient qualifications and skills to effectively deliver on the mandate for professional competence, and to audit to the required level. The head of internal audit must ensure that the internal audit function staff acquires appropriate ongoing training in order to meet the growing technical complexity of Banks' activities, and the increasing diversity of tasks that need to be undertaken as a result of the introduction of new products and processes within Banks and other developments in the financial sector.

8. The internal audit function staff collectively must be competent to examine all areas in which the Bank operates. The competencies and expertise of the overall internal audit function staff (skill mix) must include accounting, compliance checking, treasury management, information technology and strategic thinking. The internal audit function staff must apply the care and skills expected of a reasonably prudent and competent professional and, in case of limited competence and experience in a particular area, must be supervised by more experienced internal audit function staff.

9. The internal audit function staff must respect the confidentiality of information acquired in the course of their duties.

10. Senior Management must inform the internal audit function of new developments, initiatives, projects, products and operational changes, and ensure that all associated risks, known and anticipated, are identified and communicated at an early stage.

11. On the basis of the audit plan, the internal audit function must be able to perform its assignments on its own initiative in all areas and functions of the Bank. The internal audit function must not be involved in designing, selecting, implementing or operating specific internal control measures. Senior Management may request advice from internal audit on matters related to risk and internal controls, nevertheless, the development and implementation of internal controls remains the responsibility of Senior Management.

12. The oversight function of the Board audit committee includes reviewing and approving the internal audit plan, its scope and the budget for the internal audit function. The plan must be based on a robust risk assessment (including input from Senior Management and the Board) and updated at least annually (or more frequently to enable an ongoing real-time assessment of where significant risks lie).

13. The Board or the Board audit committee must assess, at least annually, the performance of the internal audit function. This must include an independent external quality assurance review of the internal audit function at least once every five years.

14. The Bank's internal audit charter must be drawn up and reviewed at least every 3 years by the head of internal audit, and approved by the Board audit committee. The charter must be available both internally and publicly on the Bank's internet website.

15. Topics which must be addressed in the internal audit charter include, but are not limited to:

a. The internal audit function's standing within the Bank, its authority, its responsibilities and its relations with other control functions;

b. The purpose and scope of the internal audit function;

c. The responsibility and accountability of the head of internal audit;

d. The obligation to communicate the results of the internal audit functions' engagements and a description of its reporting line to the Board;

e. The terms and conditions under which the internal audit function can be called upon to provide consulting or advisory services, or carry out other special tasks;

f. The requirement to comply with the Institute of Internal Auditors' (IIA) International Standards for the Professional Practice of Internal Auditing, including the IIA's Code of Ethics; and

g. Procedures for the coordination of the internal audit function with the external auditor.

16. The scope of internal audit activities must include the evaluation of the effectiveness and efficiency of the internal control system, risk management and compliance functions, and governance systems and processes of the entire Bank, including the Bank's Subsidiaries and branches. In particular, the annual audit plan must adequately cover risk measurement and management processes and methodologies, including risk appetite framework elements such as risk limit breaches and internal models.

17. Every activity, including outsourced activities, and every entity controlled by the Bank, or if applicable Group, must fall within the scope of the internal audit function.

18. The scope must also ensure adequate coverage of matters of regulatory interest. Matters of regulatory interest that must receive particular attention in the internal audit plan include, but are not limited to, the internal capital and liquidity adequacy assessment processes, quality of risk reporting to the Board and Senior Management, regulatory compliance and reporting to the Central Bank. Within a banking Group, the annual audit plan must include the assessment of the alignment between the organization of control functions at Group level and the way that control functions operate at entity level.

19. Senior Management is responsible for implementing and maintaining an adequate and effective internal control system and processes. Therefore the internal audit function must inform Senior Management promptly of all significant findings so that timely corrective actions can be taken. Subsequently, the internal audit function must follow up with Senior Management on the outcome of these corrective actions. The head of internal audit must report to the Board audit committee the status of findings that have not (yet) been rectified by Senior Management.

20. The Board audit committee must review internal audit reports, including the response and follow-up by Senior Management, to ensure that timely and effective actions are taken to address internal audit findings, particularly control weaknesses or deficiencies in risk management and compliance.

21. A consistent approach to internal audit across the Group may be achieved through the establishment of a Group internal audit function accountable to the board of the Controlling

Shareholder, or through internal audit functions established in each entity (or branch) and accountable to those entities' boards of directors, and also reporting to the Group Head of Internal Audit.

22. It is recommended that Banks perform internal audit activities using their own staff. However, outsourcing of internal audit activities, but not the function, on a limited and targeted basis can be used to provide access to specialized expertise and knowledge for an internal audit engagement where the expertise is not available in house, or to resource constraints. The Board remains ultimate responsible for the internal audit function regardless of whether internal audit activities are outsourced.

23. The head of internal audit must preserve independence by ensuring that the supplier has not been previously engaged in a consulting engagement in the same area within the Bank, unless a reasonably long "cooling-off" period has elapsed (e.g. of at least one full financial year). In addition, Banks must not outsource internal audit activities to their external audit firm.

24. The head of internal audit at the level of the Controlling Shareholder must define the Group's internal audit strategy, determine the organization of the internal audit function both at the Controlling Shareholder and Subsidiary levels (in consultation with these entities' respective Boards and in accordance with local laws), and formulate the internal audit principles that include the audit methodology and quality assurance measures. The Group's internal audit function must determine the audit scope for the Bank. In doing so, it must comply with local legal and regulatory provisions, and incorporate local knowledge and experience.

ARTICLE (5): COMPENSATION

1. Staff in the compliance and internal audit functions must be compensated in a way that makes their incentives independent of the lines of business whose risk taking and incentive compensation they monitor and control. Instead, their performance measures and incentives must be based on achievement of their own objectives (e.g. adherence to internal controls) so as not to compromise their independence. This must apply also to the compliance function staff embedded in independent support or control units.

2. Staff in the compliance and internal audit functions must not be placed in a position where, for example, approving a transaction, making decisions or giving advice on risk and financial control matters could be directly linked to an increase or decrease in their performance-based compensation.

3. If staff in the compliance and internal audit functions receives variable compensation, its total compensation must be made up of a higher proportion of fixed relative to variable compensation.

ARTICLE (6): ISLAMIC BANKING

1. A Bank offering Islamic financial services must undertake a Shari'a compliance review at least annually, performed either by a separate internal Shari'a control department or as part of the existing internal and external audit functions, 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 provisions as per the fatwa, policies and procedures approved by the Bank's Shari'a control committee.

2. Tasks of the compliance function requiring specific expertise with respect to Islamic financial services may be outsourced, but they must remain subject to appropriate oversight by the head of compliance.

3. The Bank's internal Shari'a control committee is responsible for ensuring that the internal audit function provides independent assurance with respect to specific types of risk applicable to Islamic financial services.

4. The staff within the internal audit function must be competent and collectively have the relevant experience and sufficient authority within the Bank to assess whether Shari'a compliance processes are effective and appropriate, taking into account the business of the Bank, and to determine if the relevant policies and procedures are complied with.