Iraq

ENHANCED BANK INTERNAL AUDIT AND COMPLIANCE REGULATIONS

TECHNICAL ASSISTANCE REPORT

SEPTEMBER 30, 2018

Gerald A. Edwards, Jr.

CONTENTS

Acronyms and Abbreviations

BCBS	Basel Committee on Banking Supervision
CBI	Central Bank of Iraq
FSB	Financial Stability Board
GFC	Global Financial Crisis
IMF	International Monetary Fund
SOBs	State-Owned Banks

Preface

At the request of the Central Bank of Iraq (CBI), a technical assistance mission of the IMF Middle East Regional Technical Assistance Center was conducted for the CBI in Amman, Jordan during the period of September 9 – 13, 2018. The mission assisted a senior delegation from the CBI in drafting regulations on sound internal audit and compliance functions at banks. The mission was conducted by Mr. Gerald A. Edwards, Jr. (Jerry), external expert.

The mission has conducted a seminar that addressed key topics and international supervisory guidance developed by the Basel Committee on Banking Supervision (BCBS) and the Financial Stability Board (FSB) and involved discussions about international best practices with respect to banks' internal audit and compliance activities. As part of the seminar, Mr. Waleed Eidy, Advisor to the CBI Governor, who led the CBI delegation also gave a presentation on the Iraq banking system, key CBI regulations, and important Iraqi bank practices. In addition, the mission worked with the CBI delegation to develop draft CBI regulations for bank internal audit and compliance activities.

This report presents the recommendations provided by the mission to the CBI based on the supervisory guidance of the BCBS and FSB and extensive discussions with the CBI regarding its corporate governance rules and bank practices. The mission would like to thank the CBI for its cooperation, insights, and fruitful discussions.

EXECUTIVE SUMMARY

The mission was designed to support the Central Bank of Iraq (CBI) in improving its prudential regulations to further align them with International best practices, considering the appropriate Iraqi context. This included assisting a senior team of the CBI staff in drafting CBI regulations on bank internal audit and compliance functions. Due to the security situation in Iraq, the mission was held in Amman, Jordan.

The mission was attended by a CBI delegation of eight senior professionals, led by Mr. Waleed Eidy, the Adviser of the CBI Governor.[1] All the attendants were experienced in CBI banking supervision policies and activities, including various aspects of corporate governance. The delegation mentioned that while the CBI needed regulations on bank internal audit and compliance activities, it had recently updated its regulation on corporate governance and had submitted it to the World Bank for review a few months ago and the CBI had received commendation from the World Bank for the quality of that draft.

The mission has completed the following tasks:

1. **Conducted a seminar on subjects related to internal audit, compliance and corporate governance.** It included five presentations that addressed key policy foundations regarding sound corporate governance, risk governance, transparency and internal control as well as the latest international supervisory guidance of the Financial Stability Board (FSB) and the Basel Committee on Banking Supervision (BCBS) on internal audit and compliance functions.[2] The above guidance applies to both state-owned banks and private banks. The seminar presentations and related dialogue were subject to simultaneous translation. During this seminar, Mr. Waleed Eidy and his CBI colleagues also presented a brief overview of the banking system in Iraq and the CBI supervision framework. This mission seminar was conducted during the first 2.5 days of the mission and included extensive discussion, comments and questions from the CBI delegation.

2. **The mission presented a first draft of CBI regulations for internal audit and compliance functions based on the latest BCBS supervisory guidance.** This was translated and discussed extensively during the last two days of the mission with the CBI delegation. All the CBI's comments and suggestions were considered in the final draft versions, so that these draft regulations reflect unique aspects specific to the CBI's needs. In addition, due to the comprehensive approach used in the seminar slides, the CBI delegation members were provided

[1] Mr. Waleed Eidy, Adviser to the Governor of the CBI, led the CBI delegation, which was also comprised of managers, assistant managers, a legal consultant and superintendent.

[2] Due to translation needs, although the BCBS and FSB guidance typically refer to internal audit and compliance "functions", the word "activities" is used instead in the draft CBI regulations to improve understandability in Arabic.

with extensive information that it could use in any further supervisory guidance that they may wish to issue to their banks or supervisory inspectors.

At the mission's conclusion, Mr. Waleed Eidy and the other CBI members, said that they found the mission to be very helpful and they welcomed the draft CBI regulations on internal audit and compliance functions.

A recommendation was provided to the CBI to be implemented in the near term (<12 months). This report provides the following recommendation:

- **Implement the draft CBI regulations on bank internal audit and compliance functions.** These draft regulations are designed to reflect the latest BCBS and FSB guidance on internal audit activities and to reflect the Iraqi context. It also reflects all of the CBI delegations' comments and suggestions regarding internal audit activities during the mission. Both English and Arabic versions have been developed. *(near term)*

Capacity issues were carefully considered as these recommendations were developed and the two recommended draft regulations are addressed in Annexes I and II. The above recommendation is also summarized in Table 1.

Table 1. Key Recommendation to the CBI

Recommendations	Priority	Timeframe[3]
Recommendation 1 – Implement the draft CBI regulations on bank internal audit activities and compliance activities, which are designed to reflect the latest BCBS and FSB guidance on internal audit activities (para. 9.a.)	1	Near Term

[3] Near term: < 12 months.

I. INTRODUCTION

1. The mission seminar on bank internal audit and compliance functions was based on Basel Committee on Banking Supervision (BCBS) guidance on these functions and relevant guidance of the Financial Stability Board (FSB). The seminar was designed to provide key foundations as well as principles, explanatory text, and supervisory observations to assist the Central Bank of Iraq (CBI) with the development of regulations on internal audit and compliance functions. The BCBS guidance on these functions clearly states that the guidance applies to both state-owned banks (SOBs) and private banks, and this was emphasized during the presentations. The seminar covered the following presentations:

- **Introduction and prudential authorities' strong interest** in, and initiatives to address, sound i) corporate governance, ii) risk governance, and iii) transparency before, during and after the global financial crisis (GFC), and why these are very important to banking supervisors.

- **The BCBS corporate governance principles issued in 2015,** which incorporated many of the findings and recommendations of the FSB's thematic review of risk governance and guidance on risk appetite and risk culture issued during 2013-2014, and that reflected lessons learned from the GFC.

- **The CBI presentation on its banking system and CBI supervisory framework.** This presentation enabled a helpful discussion of the key challenges that the CBI had been facing with respect to its SOBs and private banks in areas related to the topics of this mission.

- **The BCBS bank internal control framework,** issued in 1998, is still current today and is cited in important BCBS guidance on governance, core principles, and audits, and therefore, was very relevant to this mission. This session also included a summary of an internal control framework issued in 2013, developed by U.S. and international organisations and used extensively by banks, that is consistent with the BCBS bank internal control framework and reflects current issues, such as the detection and mitigation of fraud risk.

- **The BCBS guidance on bank internal audit functions,** issued in 2012, along with its guidance on audit committees and outsourcing and the enhancements to guidance on internal audit and audit committees that were set forth in the 2015 BCBS corporate governance principles based on FSB risk governance recommendations. Therefore, this session reflected lessons learned from the GFC. The session also discussed the "three lines of defense", identified key audit standard setters, such as the International Auditing and Assurance Standards Board (external audit) and the Institute of Internal Auditors (internal audit), and summarized initiatives to enhance audit quality.

- **The BCBS guidance on bank compliance functions,** issued in 2005, as well as improved guidance set forth in the 2015 BCBS corporate governance principles. Thus, this session also reflected the lessons learned from the GFC.

2. The above seminar sessions included extensive discussion about best international practices and issues being faced by Iraqi banks and the CBI in these important areas. Also, these seminar sessions provided the basis for developing draft CBI regulations. The remaining sections of this report summarize key supervisory requirements reflected in the draft CBI regulations and the mission findings and recommendations.

II. MAIN FINDINGS

3. The mission seminar presented extensive information regarding the BCBS guidance on bank internal audit functions. This supervisory guidance was issued in 2012 and included guidance on audit committees and audit outsourcing. The session also addressed enhancements to the BCBS guidance on internal audit and audit committees that were set forth in the 2015 BCBS corporate governance principles based on FSB risk governance recommendations. The 16 key BCBS principles for bank internal audit functions are summarized in Table 2.[4]

4. In addition, the mission seminar presented extensive information with respect to the BCBS guidance on bank compliance functions. This supervisory guidance, issued in 2005, was enhanced by improved guidance set forth in the 2015 BCBS corporate governance principles, and therefore reflected lessons learned from the GFC. The key BCBS principles for bank compliance functions are summarized in Table 3.

5. During the mission the CBI members brought up challenging governance, internal control, audit and compliance issues that they had been facing, along with questions about best practices. The external expert was able to discuss international situations he had seen and their resolution, the thinking behind the FSB and BCBS guidance and initiatives, and related leading practices in a manner that addressed the CBI's questions during the mission. For example, the CBI noted that because SOBs have around 90% of bank deposits, provide

[4] The BCBS guidance on bank internal audit activities include four principles that *address guidance for supervisors and not for banks*, so they were discussed extensively during the mission seminar but were not included in Table 2 since they were not an appropriate basis for the draft CBI regulations on *bank* internal audit functions (but they could be included in a CBI risk-based supervision manual, for example). In summary, these four principles are: *Principle 17:* Bank supervisors should regularly assess whether the internal audit function has sufficient standing and authority within the bank and operates according to sound principles. *Principle 18:* Supervisors should formally report all weaknesses they identify in the internal audit function to the board of directors and require timely remedial actions. *Principle 19:* The supervisory authority should consider the impact of its assessment of the internal audit function on its evaluation of the bank's risk profile and on its own supervisory work. *Principle 20:* The supervisory authority should be prepared to take informal or formal supervisory actions requiring the board and senior management to remedy any identified deficiencies related to the internal audit function within a specified timeframe and to provide the supervisor with periodic written progress reports.

approximately 85% of bank credit, and own nearly 50% of the total number of bank branches in Iraq, SOBs have an elevated stature in the Iraqi banking system and they often have not embraced sound corporate governance, including sound internal audit and compliance policies. Also, some private banks have not taken steps to enhance the independence, stature, resources and role of the heads of internal audit and compliance functions as set forth in FSB and BCBS guidance and may exert undue pressure so that deficiencies will not be fully reported to the board of directors or its audit committee. Some banks' chief executives sought to override or re-write internal auditors' reports before their presentation to the audit committee. These practices at some SOBs and private banks result in increased bank risks and compliance problems that are not subject to timely resolution by the board of directors and senior management.

Table 2: Overview of key BCBS principles for bank internal audit activities

Principle 1: An effective internal audit function 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 organisation and its reputation.

Principle 2: The bank's internal audit function must be independent of the audited activities, which requires the internal audit function to have sufficient standing and authority within the bank, thereby enabling internal auditors to carry out their assignments with objectivity.

Principle 3: Professional competence, including the knowledge and experience of each internal auditor and of internal auditors collectively, is essential to the effectiveness of the bank's internal audit function.

Principle 4: Internal auditors must act with integrity.

Principle 5: Each bank should have an internal audit charter that articulates the purpose, standing and authority of the internal audit function within the bank in a manner that promotes an effective internal audit function (Principle 1).

Principle 6: Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the internal audit function.

Principle 7: The scope of the internal audit function's activities should ensure adequate coverage of matters of regulatory interest within the audit plan.

Principle 8: Each bank should have a permanent internal audit function, which should be structured consistent with Principle 14 when the bank is within a banking group or holding company.

Principle 9: The bank's board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate, effective and efficient internal control system and, accordingly, the board should support the internal audit function in discharging its duties effectively.

Principle 10: The audit committee, or its equivalent, should oversee the bank's internal audit function.

Principle 11: The head of the internal audit department should be responsible for ensuring that the department complies with sound internal auditing standards and with a relevant code of ethics.

Principle 12: The internal audit function should be accountable to the board, or its audit committee, on all matters related to the performance of its mandate as described in the internal audit charter.

Principle 13: The internal audit function should independently assess the effectiveness and efficiency of the internal control; risk management and governance systems and processes created by the business units and support functions and provide assurance on these systems and processes.

Principle 14: To facilitate a consistent approach to internal audit across all the banks within a banking organisation, the board of directors of each bank within a banking group or holding company structure should ensure that either: (i) the bank has its own internal audit function, which should be accountable to the bank's board and should report to the banking group or holding company's head of internal audit; or (ii) the banking group or holding company's internal audit function performs internal audit activities of sufficient scope at the bank to enable the board to satisfy its fiduciary and legal responsibilities.

Principle 15: Regardless of whether internal audit activities are outsourced, the board of directors remains ultimately responsible for the internal audit function.

Principle 16: Supervisors should have regular communication with the bank's internal auditors to (i) discuss the risk areas identified by both parties, (ii) understand the risk mitigation measures taken by the bank, and (iii) understand weaknesses identified and monitor the bank's responses to these weaknesses.

Table 3: Overview of BCBS principles for bank compliance activities
Responsibilities of the board of directors for compliance **Principle 1:** The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board should approve the bank's compliance policy, including a formal document establishing a permanent and effective compliance function. At least once a year, the board or a committee of the board should assess the extent to which the bank is managing its compliance risk effectively. **Responsibilities of senior management for compliance** **Principle 2:** The bank's senior management is responsible for the effective management of the bank's compliance risk. **Principle 3:** The bank's senior management is responsible for establishing and communicating a compliance policy, for ensuring that it is observed, and for reporting to the board of directors on the management of the bank's compliance risk. **Principle 4:** The bank's senior management is responsible for establishing a permanent and effective compliance function within the bank as part of the bank's compliance policy. **Compliance function principles** **Principle 5: Independence.** The bank's compliance function should be independent. **Principle 6: Resources.** The bank's compliance function should have the resources to carry out its responsibilities effectively. **Principle 7: Compliance function responsibilities.** The responsibilities of the bank's compliance function should be to assist senior management in managing effectively the compliance risks faced by the bank. Its specific responsibilities are set out below. If some of these responsibilities are carried out by staff in different departments, the allocation of responsibilities to each department should be clear. **Principle 8: Relationship with Internal Audit.** The scope and breadth of the activities of the compliance function should be subject to periodic review by the internal audit function. **Other matters** **Principle 9: Cross-border issues.** Banks should comply with applicable laws and regulations in all jurisdictions in which they conduct business, and the organisation and structure of the compliance function and its responsibilities should be consistent with local legal and regulatory requirements. **Principle 10: Outsourcing.** Compliance should be regarded as a core risk management activity within the bank. Specific tasks of the compliance function may be outsourced, but they must remain subject to appropriate oversight by the head of compliance.

6. **The BCBS principles for bank internal audit and compliance activities summarized in Tables 2 and 3 set forth supervisory expectations for international best practices and therefore, provide an important basis for the requirements in the draft CBI regulations that are discussed in the next section.** The mission seminar sessions also incorporate the FSB review and guidance on risk governance that made significant contributions which:

- Improved the BCBS corporate governance principles, as shown in its 2015 enhanced version, including addressing boards' risk and audit committees;

- Elevated the stature and independence of the Chief Risk Officer and internal audit functions;
- Elevated the role of internal audit in reviewing the risk management and Chief Risk Officer functions; and
- Encouraged supervisors to strengthen their reviews and supervisory practices in order to better reinforce both sound corporate governance and risk governance.

7. While Tables 2 and 3 present the "bold principles" only, the BCBS guidance also provides extensive explanatory text which along with the presentation slides could be useful to the CBI in developing supervisory guidance on these important topics. The mission provided the CBI members with the presentation slides and original BCBS policy guidance to assist them in this respect.

III. MISSION RECOMMENDATIONS

8. The CBI delegation members discussed the approach that they would prefer with respect to the draft regulations on bank internal audit and compliance activities. The CBI delegation preferred an approach that is summary in nature and that would be clearly tied to the BCBS guidance, as they felt that this approach would strengthen their ability to change poor governance, audit and compliance practices at the SOBs and private banks, since the CBI would be able to easily show that the CBI regulations' requirements were based on the BCBS principles reflecting the best international supervisory guidance. Therefore, the mission developed the draft regulations with an introduction and requirements that were directly linked to the introduction and principles of the BCBS supervisory guidance on internal audit and compliance functions. The CBI delegation then reviewed those with the assistance of the translators, suggested additions or refinements based on the CBI's needs,[5] and the external expert also offered suggestions to address key issues raised by the CBI delegation. The draft regulations, that reflect all CBI inputs, are set forth in Annex I and II, in both English and Arabic versions.

9. In view of the above findings and discussions with the CBI delegation, this report makes the following recommendation:

a. **Implement the draft CBI regulation on bank internal audit activities and the draft regulation on bank compliance activities.** These draft regulations are designed to reflect the latest BCBS and FSB guidance on internal audit activities and compliance activities and to reflect the Iraqi context. They also reflect all of the CBI delegations'

[5] For example, the CBI's new corporate governance regulations, discussed with the World Bank, specify that the head of a bank's compliance function should report to the bank board's audit committee, instead of to an "ethics and compliance committee" of the board of directors as recommended by the 2015 BCBS corporate governance principles. Therefore, the draft CBI regulations use an approach consistent with the CBI corporate governance rules in this respect.

comments and suggestions regarding drafts during the mission. Both English and Arabic versions have been developed and are presented in Annex I and II. *(near term)*

- **The draft CBI regulation on bank internal audit activities provides an introduction and then presents regulatory requirements which correspond to the BCBS principles summarized in Table 2, with enhancements to reflect the unique Iraqi context and needs.** The requirements address key topics such as the governance of the internal audit function and its accountability to the audit committee; the independence, stature, competence and integrity of those performing internal audit activities; audit outsourcing; and the important dialogue between internal auditors and CBI supervisors,

- **The draft CBI regulation on bank compliance functions provides an introduction and then presents regulatory requirements which correspond to the BCBS principles summarized in Table 3, along with refinements to address the CBI's objectives and corporate governance requirements.[6]** The requirements address key topics such as the responsibilities of the board of directors and senior management for the compliance function; compliance function principles, including the relationship with the internal audit function; cross-border issues; and outsourcing matters.

Implementation of this recommendation should enhance the stature, independence, resources, and effectiveness of Iraqi banks' internal audit and compliance activities in a manner consistent with BCBS guidance and international best practices. Capacity issues were carefully considered as these recommendations were developed.

10. The mission encourages the CBI to overcome any significant challenges it may face from the banking industry in implementing the proposed regulations on internal audit and compliance activities. The draft CBI regulations are designed to enable the CBI to require Iraq's SOBs and private banks to significantly improve their governance, audit and compliance activities in line with international best practices. However, there is a risk that the CBI may face significant challenges from some SOBs and certain private banks as it seeks to implement sound corporate governance regulations and the recommended regulations on sound internal audit and compliance functions developed during this mission. It will be important for the CBI to overcome these potential challenges, implement sound regulations in the above important areas, effectively train its supervisory teams, and ensure appropriate implementation by Iraqi banks

[6] For example, the CBI's new corporate governance regulations, discussed with the World Bank, specify that the head of a bank's compliance function should report to the bank board's audit committee, instead of to an "ethics and compliance committee" of the board of directors as recommended by the 2015 BCBS corporate governance principles. Therefore, the draft CBI regulations use an approach consistent with the CBI corporate governance rules in this respect.

Annex I. Draft CBI Regulation on Bank Internal Audit Activities

Based on the BCBS Internal Audit Guidance (2012) and

Corporate Governance Principles (2015)

I. CBI Introduction – The importance of Internal Audit[1]

1. The CBI is issuing this supervisory regulation for assessing the effectiveness of the internal audit activity in banks, which forms part of the CBI's ongoing efforts to address bank supervisory issues and enhance supervision through regulations and guidance that encourages sound practices within banks. It takes into account developments in international supervisory practices and in banking organisations and incorporates lessons drawn from the global financial crisis. Legal basis – pursuant to the provisions of Article 54 regarding the Instructions for Implementation of the Banking Law No. 4 of 2010, and to ensure the soundness of the operation of a bank's activities, each bank should establish an internal audit section within its organisation (which is also called an "internal audit activity"). This internal audit section should be commensurate with the size, complexity, and nature of the bank's operations and be staffed with a sufficient number of qualified and experienced professionals and have appropriate resources so that they can perform their obligations properly. The internal audit activity should be part of the consolidated supervision framework of the bank and primarily report to the audit committee of the board of directors.

2. Annually, the head of the internal audit section devises an updated risk-focused action plan and procedures to be approved by the board of directors or its audit committee at the beginning of the year. This updated plan will include a requirement that the internal audit section should visit each of the bank's branches each quarter at a minimum. The updated action plan and procedures should be implemented in a given year and should be monitored by the audit committee of the board of directors.

3. The CBI requires that banks should have an internal audit section with sufficient authority, stature, independence, resources and access to the board of directors and its audit committee. Independent, competent and qualified internal auditors with integrity are vital to sound corporate governance.

4. A strong internal control system, including an independent and effective internal audit section and activity, is part of sound corporate governance. CBI supervisors must be

[1] This regulation draws on the BCBS's principles with respect to internal audit (2012) and corporate governance (2015), as well as international best practices.

satisfied as to the effectiveness of a bank's internal audit section, that policies and practices are followed, and that management takes appropriate and timely corrective action in response to internal control weaknesses identified by internal auditors. An internal audit section provides vital assurance to a bank's board of directors and senior management, and the CBI, as to the quality of the bank's internal control system. In doing so, the function helps reduce the risk of loss and reputational damage to the bank.

5. The CBI requires bank internal auditors to comply with and to contribute to the development of national and international professional standards, such as those issued by The Institute of Internal Auditors, and it promotes due consideration of prudential issues in the development of internal audit standards and practices.

6. For large banks and internationally active banks, an audit committee is responsible for providing oversight of the bank's internal auditors. Such a committee is established within the board of directors. Annex 1 of this regulation provides more details about the responsibilities of bank audit committees. Other banks are also expected to establish such a committee.

7. This regulation applies to all banks, including state owned banks, private banks and those within a banking group, as well as foreign bank branches in Iraq, and to those holding companies subject to prudential supervision whose subsidiaries are predominantly banks. All of these structures are referred to as banks, banking organisations, or banking groups in this regulation. The application of this regulation should be commensurate with the significance, complexity and international presence of the bank.

II. CBI Requirements

1. An effective internal audit activity provides independent assurance to the board of directors and senior management on the quality and effectiveness of a *bank's risk management, governance (including compliance activity), and internal control systems and processes*, thereby helping the board and senior management protect their organisation and its reputation. The head of internal audit reports *<u>primarily to the board's audit committee.</u>*

2. The bank's internal audit activity must be independent of the audited activities, which requires the internal audit activity to have sufficient standing and authority within the bank, thereby enabling internal auditors to carry out their assignments with objectivity.

3. Professional competence, including the knowledge and experience of each internal auditor and of internal auditors collectively, is essential to the effectiveness of the bank's internal audit activity. The bank's senior management will seek to develop and enhance the skills of the internal audit staff through conducting training courses inside and outside Iraq, as needed, and such courses are important and will be monitored by the

CBI. The responsibilities of the internal audit section include the auditing of spending financial transactions before and after their disbursement.

4. Internal auditors must act with integrity.

5. Each bank should have an internal audit charter that articulates the purpose, standing and authority of the internal audit activity within the bank in a manner that promotes an effective internal audit activity as described in Requirement 1.

6. Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the internal audit activity.

7. The scope of the internal audit activities should ensure adequate coverage of matters of regulatory interest within the audit plan. Each bank should have a permanent internal audit activity, which should be structured consistent with Requirement 14 when the bank is within a banking group or holding company.

8. The bank's board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate, effective and efficient internal control system and, accordingly, the board should support the internal audit activity in discharging its duties effectively. *Internal audit reports should be provided directly to the board or its audit committee and the internal auditors should have direct access to the board or the board's audit committee.*

9. The audit committee, or its equivalent, should oversee the bank's internal audit activity (also see Annex 1). The head of the internal audit activity's primary reporting line is to the board or its audit committee, which is also responsible for the nomination, oversight of the performance and, if necessary, proposed dismissal of the head of the internal audit activity, which is subject to the approval of the CBI. If the head of internal audit is removed from his or her position, this should be disclosed publicly to financial institutions, investors and to customers, because it may indicate potential problems with the quality of the bank's internal controls.

10. The bank should also discuss the reasons for its proposal for such removal with the relevant departments within the CBI.

11. The head of the internal audit department should be responsible for ensuring that the department complies with sound internal auditing standards and with a relevant code of ethics.

12. The internal audit activity should be accountable to the board, or its audit committee, on all matters related to the performance of its mandate as described in the internal audit charter.

13. The internal audit activity should independently perform a risk-based assessment of the effectiveness and efficiency of the internal control, risk management, and governance systems and processes created by the business units and support activities and provide assurance on these systems and processes. *This includes considering whether the risk management activity gives timely and appropriate consideration to the emerging risks facing the bank and reports on these to the board and senior management.*

14. To facilitate a consistent approach to internal audit across all the banks within a banking organisation, the board of directors of each bank within a banking group or holding company structure should ensure that either:

(i) the bank has its own internal audit activity, which should be accountable to the bank's board and should report to the banking group or holding company's head of internal audit; or

(ii) the banking group or holding company's internal audit activity performs internal audit activities of sufficient scope at the bank to enable the board to satisfy its fiduciary and legal responsibilities.

15. Regardless of whether certain internal audit activities are outsourced, the board of directors or its audit committee remains ultimately responsible for the *quality of* internal audit activities and must monitor the quality of any outsourced internal audit activities. The head of the bank's internal audit section should assist the audit committee in assessing the quality of any outsourced audit activities. Both the bank and the audit company or other firm providing the outsourced service will be accountable to the CBI.

16. The bank's internal auditors should have regular communication with CBI supervisors to (i) discuss the risk areas identified by both parties, (ii) understand the risk mitigation measures taken by the bank, and (iii) understand weaknesses identified and monitor the bank's responses to these weaknesses.

ANNEX 1: The role of the audit committee, in particular with respect to the internal audit activity

An audit committee is required for state owned and private systemically important banks and for other banks based on an organisation's size, risk profile or complexity; and should:

- be distinct from other committees;
- have a chair who is independent and is not the chair of the board or of any other committee;
- be made up entirely of independent or non-executive board members; and
- include members who have experience in audit practices, financial reporting and accounting.
- The audit committee is, in particular, responsible for:
- framing policy on internal audit and financial reporting, among other things;
- overseeing the financial reporting process;

- providing oversight of and interacting with the bank's internal and external auditors and the bank's compliance activity; and requiring all external audit work to be performed in a manner consistent with international accounting and auditing standards (including on quality control) and relevant instructions adopted by the CBI;2
- recommending to the board or shareholders for their approval, the appointment, remuneration and dismissal of external auditors, subject to CBI approval;
- reviewing and approving the audit scope and frequency; and the tenure of external auditors (4 - 5 years);
- receiving key internal and external audit reports and compliance reports and ensuring that senior management is taking necessary corrective actions in a timely manner to address control weaknesses, non-compliance with policies, laws and regulations, and other problems identified by auditors, the compliance activity and other control activities;
- overseeing the establishment of accounting policies and practices by the bank; and
- reviewing the third-party opinions on the design and effectiveness of the overall risk governance framework and internal control system.

At a minimum, the audit committee as a whole should possess a collective balance of skills and expert knowledge – commensurate with the complexity of the banking organisation and the duties to be performed – and should have relevant experience in financial reporting, accounting and auditing. Where needed, the audit committee must have access to external expert advice.

[2] It is essential that the annual report of the bank and external auditor's report be fully accurate and timely (issued within the required deadline) and not mislead with respect to any substantive information, and be consistent with international accounting and auditing standards, as well as national professional standards and instructions of the CBI.

Annex II. Draft CBI Regulation on Bank Compliance Activities

Based on BCBS guidance on Corporate Governance (2015) and Compliance Activities (2005)

I. CBI Introduction on the importance of bank compliance activities (drawing from BCBS corporate governance and compliance activity guidance)

[Legal -- Based on Paragraph 3, Article 18, of Bank Law No. 94 of 2004, and Article 71 of the Instructions for the Facilitation of the Implementation of Bank Law No. 94]

1. As part of its ongoing efforts to address bank supervisory issues and enhance sound practices in banks, the CBI is issuing this regulation on compliance risk and the compliance activity in banks. CBI banking supervisors must be satisfied that effective compliance policies and procedures are followed and that management takes appropriate corrective action when compliance failures are identified. (The expression "bank" is used in this regulation to refer generally to banks, banking groups, and to holding companies whose subsidiaries are predominantly banks.)
2. Compliance starts at the top. It will be most effective in a corporate culture that emphasizes standards of honesty and integrity and in which the board of directors and senior management lead by example to safeguard the assets of the bank and the deposits of customers. It concerns everyone within the bank and should be viewed as an integral part of the bank's business activities. A bank should hold itself to high standards when carrying on business, and at all times strive to observe the spirit as well as the letter of the law. Failure to consider the impact of its actions on its shareholders, customers, employees and the markets may result in significant adverse publicity and reputational damage, even if no law has been broken.
3. Each bank (including state owned and private banks and banking groups) must establish a compliance section (also called the "compliance activity") and set out an annual policy and procedures to be presented to the board of directors for approval by the audit committee. The number of the staff working for this section and the section's resources should be commensurate to the size and diversity of the activities and branches of the bank. The compliance section will perform an evaluation of the bank's compliance in conducting its operations in accordance with the respective legal requirements. This section will confirm the correctness of such policies and procedures and seek to avoid mistakes and violations of applicable laws, instructions and codes of professional conduct that would expose the bank to various risks, in cooperation with all of the sections and units of the bank.
4. The expression "compliance risk" is defined in this regulation as 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, instructions, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities (together, "compliance laws, rules and standards").
5. Compliance laws, rules and standards generally cover matters such as observing proper standards of market conduct, avoiding and managing conflicts of interest, treating customers fairly, and ensuring the suitability of advice to customers. They include specific areas such as

the prevention of money laundering and terrorist financing and extend to tax laws that are relevant to the structuring of banking products or customer advice. For example, foreign currency obtained from the CBI for customers should be used in accordance with the customers' requirements, subject to applicable laws, regulations and instructions. A bank that knowingly participates in transactions intended to be used by customers to avoid regulatory or financial reporting requirements, evade tax liabilities or facilitate illegal conduct will be exposing itself to significant compliance risk.

6. Compliance laws, rules and standards have various sources, including primary legislation, rules and standards issued by legislators and regulations and instructions of the CBI, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to the staff members of the bank. For the reasons mentioned above, these are likely to go beyond what is legally binding and embrace broader standards of integrity and ethical conduct.
7. Compliance should be part of the culture of the bank; it is not just the responsibility of specialist compliance staff. Nevertheless, a bank will be able to manage its compliance risk more effectively if it has a compliance activity in place that is consistent with the "compliance activity requirements" set forth below. The expression "compliance activity" and "compliance section" are used in this regulation to describe staff carrying out compliance responsibilities.
8. There may be some differences between banks regarding the organisation of the compliance activity. In larger banks, compliance staff may be located within operating business lines, and internationally active banks may also have group and local compliance officers. In smaller banks, compliance activity staff may be located in one unit. Separate units have been established in most banks for specialist areas such as data protection and the prevention of money laundering and terrorist financing.
9. Regardless of how the compliance activity is organized within a bank, it should be independent and sufficiently resourced, its responsibilities should be clearly specified, and its activities should be subject to periodic and independent review by the internal audit activity. Requirements 5 to 8 below set forth these CBI expectations. The requirements are applicable to all banks, including state owned banks, private banks, banking groups and branches of foreign banks. The way in which the requirements are implemented should depend on factors such as the bank's size, the nature, complexity and geographical extent of its business, and the legal and regulatory framework within which it operates within Iraq and other applicable countries.

II. CBI requirements for bank compliance activities

Responsibilities of the board of directors for compliance

1. The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board should approve the bank's compliance policy, including a formal document establishing a permanent and effective compliance activity, *and the appointment and remuneration of the section head of compliance.* At least once a year, the board or its audit committee of the board should assess the extent to which the bank is managing its compliance risk effectively.

   Responsibilities of senior management for compliance

2. The bank's senior management is responsible for the effective management of the bank's compliance risk.
3. The bank's senior management is responsible for establishing and communicating a compliance policy (developed by the head of the compliance section) for ensuring that it is observed, and for reporting to the audit committee of the board of directors at least quarterly on the assessment and management of the bank's compliance risk, and more frequently in case of urgent emerging risks. *The duty of senior management to ensure that the compliance policy is observed entails responsibility for ensuring that appropriate remedial or disciplinary action is taken if breaches are identified. The head of the compliance section, must report promptly to the board of directors or the audit committee of the board on any material compliance failures (e.g., failures that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation). The reports by the head of the compliance section must be accurate, timely, and comprehensive in addressing both the strengths and weaknesses in the bank's compliance practices, and in particular, should portray accurately any significant compliance risks, financial violations, and other violations that expose the bank to significant compliance risk.*

4. The bank's senior management is responsible for establishing a permanent and effective compliance activity within the bank as part of the bank's compliance policy.

Compliance activity requirements

5. The bank's compliance activity should be independent. The concept of independence involves four related elements, each of which is considered in more detail below.

- The compliance activity should have a formal status within the bank.
- There should be a group compliance officer or head of compliance with overall responsibility for coordinating the management of the bank's compliance risk.
- Compliance activity staff, and in particular, the head of compliance, should not be placed in a position where there is a possible conflict of interest between their compliance responsibilities and any other responsibilities they may have.
- Compliance activity staff should have access to the information and personnel necessary to carry out their responsibilities.

The CBI supervisor of the bank and the board of directors should be informed by the bank when the head of compliance takes up or leaves that position and, if the head of compliance is leaving the position, the reasons for his or her departure. For internationally active banks with local compliance officers, the CBI as the host country supervisor should be similarly informed of the arrival or departure of the local head of compliance.

6. The bank's compliance activity should have the resources to carry out its responsibilities effectively. The resources to be provided for the compliance activity should be both sufficient and appropriate to ensure that compliance risk within the bank is managed effectively. In particular, compliance activity staff should have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their specific duties.

Compliance activity staff should have a sound understanding of compliance laws, rules and standards and their practical impact on the bank's operations. The professional skills of compliance activity staff, especially with respect to keeping up-to-date with developments in compliance laws, rules and standards, should be maintained through regular and systematic education and training.

7. The responsibilities of the bank's compliance activity should be to assist senior management in managing effectively the compliance risks faced by the bank. Its specific responsibilities are set out below. If some of these responsibilities are carried out by staff in different departments, the allocation of responsibilities to each department should be clear. Responsibilities include:

- *Advice*
- *Guidance and education*
- *Proactive identification, measurement and assessment of compliance risk*
- *Monitoring, testing and reporting*
- *Statutory responsibilities and liaison* -- It may liaise with relevant external bodies, including regulators, standard setters and external experts.
- *Fulfilling responsibilities set forth in the bank's compliance program*

8. The scope and breadth of the activities of the compliance activity should be subject to periodic review by the internal audit activity.

9. The bank's senior management should engage the compliance section staff in annual professional development courses in order to keep pace with recent developments in the compliance area. When evaluating the compliance section, the CBI will consider that such training courses will constitute an important part of the bank's management of compliance risk.

10. The compliance section should have dialogue, and cooperate with respect to relevant information, with the internal audit section in the areas related to the evaluation of a bank's performance.

11. *Cross-border issues.* Banks should comply with applicable laws and regulations in all jurisdictions in which they conduct business, and the organisation and structure of the compliance activity and its responsibilities should be consistent with local legal and regulatory requirements.

12. *Outsourcing.* Compliance should be regarded as a core risk management activity within the bank. Specific tasks of the compliance activity may be outsourced, but they must remain subject to appropriate oversight by the head of compliance.