CBI Detailed Assessment Guidelines for the 2025 Standards

Intended for Private Banks (Commercial and Islamic)

This document is provided for reference purposes only and is not intended for official use, for formal reference please consult the previously published Arabic version of the document.

Contents

1. Introduction

The Central Bank of Iraq (CBI) has launched a binding, multi-year banking reform initiative to modernize Iraq's financial sector, enforce rigorous standards, and align with international best practices. Effective August 2025, the program mandates strict compliance in governance, financial soundness, and risk management, introducing clear regulatory pathways—Stay, Merge, or Exit—for all licensed banks. This initiative aims to enhance stability, safeguard depositor interests, and foster a resilient, transparent, and globally credible banking environment, supporting sustainable economic growth and ensuring that all private banks operate under robust, enforceable standards and close CBI supervision.

This circular establishes the fundamental regulatory requirements and procedures applicable to private banks. It aims to provide clarity and guidance to banks in their pursuit of full compliance within the specified timelines. The regulatory requirements and procedures outlined herein are mandatory, and CBI shall closely monitor their adherence and implementation.

The Assessment Guidelines are structured identically for each standard, comprising:

A. **Standard Summary**: A concise overview of the standard's scope, objectives, and key compliance elements;

B. **Assessment Guidelines**: A detailed description of the CBI's expectations for implementation, including specific governance, procedural, financial, and operational details; and

C. **Assessment Process**: A clear description of the CBI's supervisory methodology, including required documentation, metrics, review tools, and timelines.

This document is designed to be read in conjunction with the Standards Booklet and the Pathways Circular, which together provide a fuller picture of the reform program. The requirements provided herein shall surpass and take precedence over any conflicting requirements, except for any requirements and regulations required by applicable laws.

The standards set forth in this document are designed to address the underlying root causes of the international foreign currency restrictions imposed on numerous banks in Iraq and have been developed in coordination with the international entities responsible for such measures. Adherence in full to the letter and spirit of these standards, as confirmed by globally reputable and recognized 3rd party organizations, will facilitate the removal of existing foreign currency restrictions that currently hinder the integration of affected banks into the global financial system, except in cases where other restrictions arise on grounds outside the scope of these standards such as an OFAC designation. Access to foreign currency is further subject to the acquisition of direct tier-one correspondent banking relations with foreign banks following the affected banks' full compliance with reform standards.

The CBI will oversee the precise and comprehensive enforcement of these standards. All private banks (both commercial and Islamic) are required to familiarize themselves with every provision of this document and to implement the necessary changes without delay. Non-compliance will result in immediate administrative action, up to and including the imposition of sanctions, remedial measures pursuant to article (56) of the Banking Law No. 94 of 2004, or the revocation of banking licenses pursuant to article (13) of the same law. The CBI will not tolerate ambiguity, delay, or partial compliance. The requirements contained within this circular are mandatory, and all private banks (commercial and Islamic) are expected to treat them as such.

The circular will enter into force as of the date of its publication and shall apply exclusively to all private banks (both commercial and Islamic).

2. Ownership and Governance

A.1 Ownership Structure

Standard A1.1

A. Standard Summary

1. Shareholding of a bank by any individual or corporation (including shareholdings of connected parties) shall not exceed the threshold of 10% (ten percent) without express written approval from CBI.
    a. CBI shall have the authority to allow banks to exceed the aforementioned threshold based on specific criteria but shall not allow shareholdings to exceed 40% (forty percent) for individuals and corporations.
    b. Corporations classified as "qualified institutional investors" – as defined below in Standard A1.2 – shall be allowed to own a shareholding of up to 60% (sixty percent) depending on the type of the "qualified institutional investor" and after obtaining approval from CBI.
    c. The term "shareholding of a bank" shall be interpreted to include shareholding of any holding company that owns the bank. When a bank is owned by a holding company or a group of companies, the shareholding limitations shall apply exclusively to the holding company and not to the bank itself.

B. Assessment Guidelines

1. The equity holdings of all connected parties in a bank shall be considered on an aggregate basis and not on an individual basis, to avoid possible circumventing of the defined thresholds.
2. The term "connected parties" refers to any individuals, or legal entities belonging to individuals, that are directly related by familial, business, and/or political links, as defined in the following way:
    a. Familial links: the individuals are linked by blood, marriage or kinship up to the fourth degree, i.e. including
        i. First degree: mother, father, daughter, son
        ii. Second degree: sister, brother, grandmother, grandfather, granddaughter, grandson
        iii. Third degree: aunt, uncle
        iv. Fourth degree: first cousins (children of aunts / uncles)
    b. Business links: the individuals (or entities) are currently in a business partnership, hold shares in the same institution, serve together on the Board of Directors of the same institution, or one individual is employed by a company owned or controlled by the other
    c. Political links: the individuals (or entities) have either familial or business links to, or are under influence or control of, the same politically exposed person (PEP) or other party of influence
3. All new applicants seeking to acquire an equity stake in a licensed bank that may result in total direct or indirect shareholding (including connected parties) exceeding the threshold must obtain prior written approval from CBI. This approval shall only be granted upon successful submission of all required shareholding information as detailed below:
    a. A bank's written request to receive approval for exceeding the 10% (ten percent) shareholding limit must demonstrate that the bank meets both of the following criteria:
        i. The bank has, at the time of the request, met all standards contained in this document, except the 10% shareholding limit

ii. No investor, either alone or through connected parties, exceeds a 40% shareholding at the time of the request

b. A bank's written request to receive approval for exceeding a 20% (twenty percent) shareholding must demonstrate that the bank meets both of the following criteria:

i. One of the bank's shareholders, at the time of the request, is a shareholder that is classified as a "qualified institutional investor" – as defined below in Standard A1.2 – and holds shares of the bank exceeding the shares of the shareholders requesting the exception, including shares of connected parties.

c. CBI retains the authority to deny, at its sole discretion, a request to any bank

4. Banks shall notify CBI of any change in shareholding that constitutes an increase of at least 5 (five) percentage points, and any change in shareholding that results in shareholder(s) exceeding the threshold of 10% (ten percent).

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI, based on inputs from shareholder diligence and EDD reports provided by third-party specialist firms.

2. CBI shall conduct the following activities, including but not limited to the following:

a. Compile an up-to-date list of bank's shareholders with inputs from banks, considering connected parties as a single entity

b. Confirm the bank meets the criteria defined above (Standard A1.1, paragraph A of this document), and accordingly decide on their request for shareholding increase

c. Create a table comparing the bank's shareholders current holdings to the current limit based on all above factors (type of shareholder, any exceptions granted, any interim, CBI-defined limit)

d. Flag any shareholding that exceeds the corresponding limit

3. Each bank shall submit, on at least a quarterly basis and upon any material change in shareholding, a comprehensive shareholding disclosure report. This report shall include full details on all direct and indirect shareholders, identification of connected parties as defined earlier and the aggregate percentage of shareholding held by each shareholder cluster, including connected parties. A one-time shareholder diligence/ EDD report by a third-party specialist firm shall be generated for each new owner/ shareholder within the bank.

4. Additionally, any material changes in shareholdings should be reported to CBI – with at least 30 (thirty) days prior notice, or once the bank becomes aware of such proposal, whichever is earlier – and approved by CBI.

5. In general, shareholders acting in concert will be considered to be connected parties.

Standard A1.2

A. Standard Summary

1. A bank shall have at least one shareholder who is a qualified institutional investor (QII) and who also holds an equity stake in the bank of not less than 5% (five percent).

B. Assessment Guidelines

The term "qualified institutional investors" refers to corporate entities that are either one of the following:

1) A bank fulfilling all of the following conditions:

a. Is licensed and supervised by a financial regulatory authority;
b. Has been operating as a licensed bank for at least five (5) consecutive years;
c. Holds assets of not less than four trillion Iraqi dinars (IQD);
d. Maintains an active correspondent banking relationship in each of three currencies: USD, EUR, and CNY

The Ownership Cap for this type of QII shall be up to 60% (sixty percent) of the bank's shareholding.

2) A regulated non-bank institutional investor (e.g. Asset Manager) that fulfills all of the following conditions:
   a. Is licensed and supervised by a financial market regulator in a jurisdiction not appearing on the Financial Action Task Force (FATF) Grey List or Black List;
   b. Has assets under management (AUM) with an aggregate value of not less than four trillion Iraqi dinars (IQD), or the equivalent thereof in a foreign currency;
   c. Has a track record of at least 5 (five) years of holding controlling stakes in the banking sector

   The Ownership Cap for this type of QII shall be up to 10% (ten percent) of the bank's shareholding as per the Iraqi Corporate Law

3) A sovereign wealth fund (SWF) or a multilateral development bank (MDB)

   a. A SWF established by a national government and fulfilling the following criteria:
      i. Is licensed and supervised by a financial market regulator in a jurisdiction not appearing on the Financial Action Task Force (FATF) Grey List or Black List;
      ii. Has not less than 5 (five) years of experience in asset management or investments in the financial sector;
      iii. Has a total committed capital of not less than four trillion Iraqi dinars (IQD).

   b. An MDB that has not less than 5 (five) years of experience in asset management or investments in the financial sector.

   The Ownership Cap for this type of QII shall be up to 10% (ten percent) of the bank's shareholding as per the Iraqi Corporate Law.

4) An investment fund that fulfills all the following conditions:
   a. Is managed by a fund manager approved by the CBI on the basis of fit-and-proper criteria;
      (i) Fit-and-proper criteria shall include, but not necessarily be limited to, credible evidence that the fund manager is capable of successfully managing equity investments in banks
   b. Has a governance structure that has been approved by the CBI;
   c. Has a capital of not less than one hundred billion Iraqi dinars (IQD);
   d. Has a majority of its capital sourced from Iraqi institutional investors

   The Ownership Cap for this type of QII shall depend on the legal structure of the QII itself, pursuant to Iraqi Corporate Law and all relevant Iraqi laws.

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.
2. CBI shall conduct the following activities, including but not limited to the following:
    a. Review the bank's shareholders' agreement to determine which shareholder(s) have been classified by the bank as a QII, and shall confirm that their shareholding falls between the stipulated minimum and maximum
    b. Confirm that each shareholder classified by the bank as a QII meets all the relevant requirements to be classified as such, through review of relevant documentation provided by the QII itself. Relevant documentation may include, but is not limited to, audited financial statements, regulatory licenses, written confirmation from the SWIFT network indicating the existence of a correspondent banking relationship, board composition, portfolio history, organizational structure, and internal governance reports
3. Assessment shall be conducted annually or whenever a new QII becomes a shareholder of the bank. As described above, each bank shall submit a shareholding disclosure report upon any material change in shareholdings – defined as any change in shareholdings of at least 5 (five) percentage points – that will facilitate CBI's ability to conduct an assessment at the proper time.

Standard A1.3

A. Standard Summary

1. A bank shall embed into its shareholders' agreement specific measures that discourage concealed arrangements or transactions (e.g., nominee agreements), as defined by CBI.

B. Assessment Guidelines

1. The term "shareholders' agreement" refers to a legally binding contract among all the bank's shareholders that details the rights and obligations of the shareholders. Although there is no obligation for a bank to make the document public (as in the case of a bank's bylaws or articles of incorporation), provisions of the shareholders' agreement must be submitted for review upon request of CBI.
2. A bank's shareholders' agreement shall include provisions that prohibit concealed arrangements on penalty of share forfeiture, i.e. any shares found to be linked to concealed arrangements shall be subject to forfeiture of the shares in question to the bank's Treasury. The concealed arrangements that shall be penalized shall include, but not necessarily be limited to, the following:
    a. Undisclosed nominee arrangements: any arrangement whereby a shareholder appoints another party, who may or may not be a fellow shareholder of the bank, to hold shares on their behalf without disclosing the true shareholding to the company or other shareholders
    b. Encumbrance of shares: any arrangement whereby a shareholder grants a third party, who may or may not be a fellow shareholder of the bank, a right or claim over their shares which may restrict the shareholder's ability to sell or transfer those shares. Common instances of encumbrances include pledges of collateral, lock-up agreements, and share mortgages
3. A bank's shareholders agreement shall include specific shareholder rights designed to protect shareholders' interests in the context of share sales or transfers. Specific shareholder rights shall include, but not necessarily be limited to the following:
    a. Tag-along rights: when a shareholder decides to sell their shares, other existing shareholders are guaranteed the opportunity to participate pro-rata in the sale – to the same buyer – at the same time and for the same price per share as initially proposed by the selling shareholder

b. Right of first refusal: when a shareholder decides to sell their shares, other existing shareholders are guaranteed the opportunity to purchase those shares before they are offered to any outside parties, at the same time and for the same price per share as initially proposed by the selling shareholder

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.
2. CBI shall review the bank's shareholders' agreement to determine whether:
   a. It contains the minimum required provisions that appropriately penalize undisclosed nominee arrangements and encumbrances of shares, or not
   b. It contains the minimum required provisions that protect tag-along rights and right of first refusal, as outlined above, or not
   c. All current shareholders have signed the agreement, or not
3. The assessment shall be conducted annually.

A.2 Owner Due Diligence

Standard A2.1

A. Standard Summary

1. All shareholders of a bank, holding shares either directly or through connected parties, shall undergo shareholder diligence and ID verification.

B. Assessment Guidelines

1. The term "connected parties" is defined as per the definition contained in the Assessment Guidelines of Standard A1.1.
2. "Shareholder diligence and ID verification" is an exercise that shall include, but not necessarily be limited to, the following elements:
   a. Identity verification, to confirm that the person is who they claim to be
   b. Background checks, including criminal records checks, to ascertain whether the individual may pose a risk to the bank
   c. Screening of names against public and proprietary sanctions lists to ensure compliance with regulatory requirements and to avoid doing business with individuals or entities involved in illegal activities
   d. Evaluation of risk profiles of individuals, to evaluate the risk associated with each ultimate beneficial owner and shareholder based on various factors
   e. Identifying whether an individual is connected to another shareholder of the bank, by familial, business, or political links as defined above
3. The requirement to undergo shareholder diligence and ID verification applies to all shareholders, including those who already underwent similar verification during a past license application, and/or who were in the past granted a license, as well as those who have never undergone any such verification or have never been granted a license.

C. Assessment Process

1. Shareholder diligence and ID verification shall be conducted by a third-party specialist firm from a list of CBI-approved firms.
2. The third-party specialist firm shall:
    a. Identify and generate exhaustive list of all the bank's shareholders, i.e., both direct individual shareholders or ultimate beneficial owner in the case of corporate entities holding shares
    b. Conduct the testing that includes the checks listed above
    c. Produce a substantiated report that presents the comprehensive findings of the tests, including all red flags
3. This test is to be done for shareholders once during the reform period, new shareholders must submit to shareholder diligence and ID verification within one month of the date they acquire such an equity stake.
4. The decision on whether the shareholder passes the due diligence test shall be made by the CBI team based on the substantiated report produced by the third-party specialist firm and after further validation on its contents.

Standard A2.2

A. Standard Summary

1. All shareholders of a bank that hold an equity stake – either directly or through connected parties – of at least 1% (one percent), or who are politically exposed persons (PEPs), shall undergo enhanced due diligence tests.

B. Assessment Guidelines

1. The term "politically exposed persons (PEPs)" is defined in alignment with the Due Diligence Guidelines Toward Holders of Senior Positions (CBI Regulation No. 2 of 2023) as any individual who holds or has held a prominent public function, whether domestically or internationally, including but not limited to:
    a. Heads of state, heads of government, ministers, and their deputies or advisors
    b. Members of parliament or similar legislative bodies
    c. Senior judicial officials and members of high courts
    d. Senior military officers and commanding personnel in security agencies
    e. Ambassadors, high-ranking diplomats, and similar representatives
    f. Senior executives of state-owned enterprises and members of their boards
    g. Senior party officials of political parties
    h. Directors, deputy directors, and board members of international organizations
    i. Any individual linked by blood, marriage, or kinship up to the second degree to an individual that meets any of the above criteria
2. An enhanced due diligence test is a rigorous exercise that shall include, at a minimum, the following checks:
    a. A thorough shareholding and influence mapping, including shareholders' connections to PEPs up to the fourth degree (as defined above under the Assessment Guidelines of Standard A1.1), connections to other shareholders, including both natural persons (through familial, business or political links) and corporations (through ultimate beneficial ownership)

b. An assessment of the individual's reputation and integrity, including follow-up on allegations of fraud and links to money laundering

c. An assessment of the individual's source of wealth to identify any adverse information

3. In the case of corporate shareholders holding equity stakes above the aforementioned minimum level, the enhanced due diligence tests shall be conducted on the ultimate beneficial owner(s) of the corporate entity, and a corporate due diligence test will be conducted on the entity itself. The corporate due diligence test is an assessment that shall cover the following areas:

   a. Sources of funds and financial standing – including audited financial statements for the preceding three fiscal years, verification of the lawful origin of funds intended for investment, and evidence of financial capacity to sustain the shareholding

   b. Corporate governance and control mechanisms – including the entity's board composition, internal governance procedures, and existence of independent audit or compliance functions

   c. Business activities and sectoral risk – including a description of the entity's core business operations, sectoral affiliations, geographic presence, and any exposure to high-risk industries or jurisdictions

   d. Legal and regulatory compliance history – including any prior or ongoing investigations, administrative penalties, sanctions, or court proceedings

   e. History of financial distress – including any declarations of bankruptcy, restructuring proceedings, debt defaults, or other indicators of financial instability within the last ten years; and

   f. Tax compliance – including verification of tax filings and payment status in all jurisdictions of operation, and absence of material unpaid tax liabilities or unresolved tax disputes

4. The requirement to undergo EDD testing applies to all shareholders meeting the specified criteria, including those who already underwent similar testing during a past license application, and/or who were in the past granted a license, as well as those who have never undergone any such testing or have never been granted a license.

5. Those individuals flagged / presented as connected parties will undergo a single, consolidated EDD test rather than one test per individual.

6. Any bank becoming aware of a proposed acquisition of a qualifying holding in the bank or of a proposed increase in an existing qualifying holding in the bank shall give at least 30 (thirty) days prior notice to the CBI, or once it becomes aware of such proposal, whichever is earlier.

7. New shareholders must undergo EDD testing within 3 (three) months of the date they acquire such an equity stake.

C. Assessment Process

1. The enhanced due diligence tests shall be conducted by a third-party specialist firm from a list of CBI-approved firms.

2. The third-party specialist firm shall:

   a. Generate an exhaustive list of all the bank's shareholders holding an equity stake of at least 1% (either directly or through connected parties), duly verified by cross-checking against filings held by Iraq Ministry of Trade, the Iraqi Stock Exchange and publications by the CBI

   b. Conduct the enhanced due diligence test that includes the checks listed above

c. Produce a substantiated report that identifies any of the bank's shareholders whose shareholding in the bank risks compromising the bank's financial stability and/or poses reputational risk to the banking sector at large

3. New shareholders meeting the criteria mentioned in the Standard Summary must undergo EDD tests within one month of the date they acquire such an equity stake.

4. The decision on whether the shareholder passes the EDD test shall be made by the CBI team based on the substantiated report produced by the third-party specialist firm and after further validation on its contents.

5. It is the bank's responsibility to ensure that no individual who fails to pass the EDD test continues to hold a shareholding beyond six months from the notification of the failure to pass, without correcting the cause of the failure.

A.3 Board Governance

Standard A3.1

A. Standard Summary

1. A bank's Board of Directors shall meet the following criteria:

   a. The Board shall consist of exactly 9 (nine) members

   b. All members of the Board shall be non-executive members except for the Chief Executive Officer (CEO)

   c. Exactly two-thirds of the Board shall be independent Board members, and at least half of the independent Board members must be nominated by the QII

   d. If the chairman of a bank's Board of Directors is not an independent Board member, they shall not be allowed membership of any of the board committees.

B. Assessment Guidelines

1. The term "non-executive member" means a Board member that does not work full-time for the bank, nor part-time in any position beyond that of Board member.

2. An individual shall be considered an "independent Board member" unless it is proven that they:

   a. Have a direct or indirect material relationship with the bank other than membership on the Board and/ or a minor ownership of less than 2% (two percent)

   b. Have, now or at any point in the 5 (five) years prior to their appointment been employed by the bank or its affiliates

   c. Have, or have had in the 5 (five) years prior to their appointment, a business relationship with the bank or its affiliates

   d. Are a controlling shareholder, employee, advisor, or Board member of a qualified institutional investor holding shares in the bank

   e. Are affiliated with any non-profit organization that receives significant funding from the bank or its affiliates

   f. Receive, or have received in the 5 (five) years prior to their appointment, any additional remuneration from the bank or its affiliates besides their director's fee

g. Participate in any pension plan of the bank or its affiliates

h. Are employed as an executive officer of another company where any of the bank's executives serve on that company's Board of Directors

i. Are, or have been at any time during the 5 (five) years prior to their appointment, affiliated with or employed by a present or former auditor of the bank or its affiliates

j. Have served on the Board of the bank for more than 10 (ten) years in their lifetime

k. Holds any credit facility with the bank – however, the CBI may, at its sole discretion, grant exceptions to this requirement in specific cases of, especially in cases of small credit facilities

l. Are a member of family (up to the 4th degree) of any individual who would fail any of the above tests

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.
2. CBI shall conduct the following activities, including but not limited to the following:
   a. Review Board charter and any other relevant governance documents to determine that the bank has embedded these practices into their organization
   b. Receive declarations from banks regarding the makeup of their Board, the names of the individuals and an assessment – conducted by the bank's Nomination and Remuneration Committee – of whether each member can be classified as an "independent board member" in accordance with the criteria specified
   c. Check the bank's publicly-accessible website and annual report to determine whether the Board makeup and designation of independents is reflected and meets the criteria set out in the standard
   d. Review minutes of Board meetings and discuss with CBI-appointed observer attending the bank's Board meetings, as proof that the ratios are being adhered to
   e. Receive QII attestation that three of the independent board members were nominated by the QII
3. Assessment shall be conducted annually.

Standard A3.2

A. Standard Summary

1. All members of the Board of Directors of a bank shall be appointed at the Annual General Meeting of shareholders, for a period of no more than 4 (four) years. Board members may be reappointed for only one subsequent period of equal length, for a maximum total of 2 (two) full terms and a maximum total of 8 (eight) years.

B. Assessment Guidelines

1. An Annual General Meeting (AGM) is a formal gathering of the bank's shareholders and management, typically held once a year.
2. For current Board members, their reelection shall only be allowed if they have served on the Board of the bank for no more than four years in their lifetime at time they are put up for reelection.

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.
2. CBI shall review Board charter and any other relevant governance documents to determine that the bank has embedded these practices into their organization.
3. Assessment shall be conducted annually.

Standard A3.3

A. Standard Summary

1. The Board of Directors of a bank shall conduct at least 6 (six) meetings per calendar year.

B. Assessment Guidelines

1. A gathering of Board members shall only count towards the six-meeting minimum if both of the following conditions are met:
    a. A quorum of Board members – defined as a minimum of 50% (fifty percent) of members that includes at least three independent members – are present
    b. A CBI-appointed observer is invited to attend (invitation shall be extended at least 4 (four) weeks prior to the meeting) and the observer shall obtain a copy of the Board-approved minutes of the meeting as well as the audio-visual recordings of the meeting from the board secretary.

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.
2. CBI shall conduct the following activities, including but not limited to the following:
    a. Review the Board charter and any other relevant governance documents to determine that the bank has embedded these practices into their organization
    b. Review minutes of Board meetings and hold discussions with the CBI-appointed observer to confirm that sufficient Board meetings are taking place.
3. Assessment shall be conducted annually.

Standard A3.4

A. Standard Summary

1. Certain Board decisions shall require super-majority approval to pass, including decisions related to the following:
    a. Dismissal of a board member
    b. Appointment or removal of CEO, CTO, CFO, CRO, Head of Compliance / Head of Sharia Compliance for Islamic Banks and Anti-Money Laundering Officer (MLRO); CBI approval is required for the relevant appointments as mentioned in Standard A6.1.
    c. Approval of major mergers, purchases or sales above a certain threshold
    d. Changes to articles of association or corporate bylaws, issuance of new shares

e. Capital restructuring, or any other actions that dilute existing shareholdings

f. Approval of related party transactions as detailed in standard D1 which is relevant for related parties and conflicts of interest

B. Assessment Guidelines

1. "Super-majority approval" is defined as approval by a share of votes that equals or exceeds two-thirds of valid votes (i.e., not counting abstentions or absences) and it applies only on the specific decisions detailed above and not on all normal decisions that requires 50%-plus-one for approval.
2. A minimum quorum is required for a supermajority decision to be valid, this minimum quorum is the one defined by CBI specified in Standard A3.3 above.
3. The threshold for value of mergers, purchases, or sales – above which super-majority approval is needed – shall be 20% (twenty percent) of the equity of the bank and its subsidiaries on a consolidated basis.
4. Any transaction or cumulative set of transactions involving selling or purchase of equity amounting to 20% (twenty percent) of the assets of the bank and its subsidiaries on a consolidated basis whether conducted directly or indirectly, in a single deal or via multiple related contracts—shall be subject to the following:
   a. Super majority approval from the board;
   b. Prior written notification to CBI and submission of detailed transaction documentation.
5. "Cumulative set of transactions" is defined as multiple transactions conducted with the same party within two consecutive calendar years.

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.
2. CBI shall conduct the following activities, including but not limited to the following:
   a. Review Board charter and any other relevant governance documents to determine whether the bank has embedded these practices into their organization
   b. Review minutes of Board meetings and hold discussions with the CBI-appointed observer to confirm that sufficient Board meetings are taking place.
3. Assessment shall be conducted annually.

A.4 Board fit and proper testing

Standard A4.1

A. Standard Summary

1. All members of the Board of Directors of a bank as well as members of the Sharia Supervisory Board for Islamic Banks shall undergo "fit and proper" tests.

B. Assessment Guidelines

1. The "fit and proper" test is a thorough evaluation of an individual that shall include, but not necessarily be limited to, assessments of their:

a. Past criminal record and history of disciplinary actions

b. Character and integrity, including evaluation of their personal and professional conduct, reputation, ethical behavior, and transparency in prior roles

c. As provided by Article 17 of the 2004 Banking Law, a Board member must be at least 30 years old upon their ascension to the Board

d. Absence of conflicts of interest that could cause management integrity issues or any risks to separation of shareholders and management

e. Academic credentials, including verification of the Board member's academic qualifications to ensure all board members hold at least a university degree, in line with CBI regulations

f. Professional experience, including verification of employment history, and verification of professional certifications, in line with CBI regulations

   i. Specifically, the Board member must have at least 10 (ten) years of leadership or management experience in relevant areas including but not limited to finance, law, accounting, and technology, ideally within companies of similar size and complexity

g. Financial soundness, including evaluation of the Board member's personal financial position, history of insolvency or bankruptcy, and record of compliance with tax and debt obligations in Iraq or abroad

h. Regulatory and legal compliance, including review of criminal history, past and present involvement in any legal proceedings, regulatory violations, penalties, or sanctions whether in Iraq or abroad

i. Time commitment and independence, including analysis of the Board member's existing roles and responsibilities across other institutions to determine their ability to dedicate sufficient time and avoid conflicts of interest

j. For the members of the Sharia Supervisory Board of Islamic banks, the assessment must ensure compliance with the specific requirements for board members as detailed in the following circular: 'Requirements for Candidates for Leadership Positions in Banks Operating in Iraq'

2. Both existing and future Board members shall undergo "fit and proper" tests. Existing Board members must undergo the testing before a specific deadline defined by CBI, even if they have undergone similar tests in the past for any reason and for any position as part of a licensing process or any other approval process. Future Board members will be required to pass a "fit and proper" test before they are officially appointed.

3. Individuals with existing or past affiliations (as per the definition of connected parties mentioned earlier) with politically exposed persons (PEPs) or entities under sanctions shall be subject to enhanced due diligence procedures, including a full disclosure of the nature and timeline of the affiliation, and a CBI determination of its acceptability.

C. Assessment Process

1. The "fit and proper" tests of a bank's Board members shall be conducted by a third-party specialist firm from a list of CBI-approved firms.

2. The third-party specialist firm shall conduct the "fit and proper" tests incorporating the required elements listed above.

3. Wherever possible, documentation supporting all the above points shall be submitted in full (e.g., including CV, degree certificates, proof of employment, financial statements, legal clearances, and reference letters).

4. Banks must have conducted these tests on all individuals who are members of the Board by a specific date defined by CBI. All new board members will need to be cleared through this test before being formally appointed. Board members shall also be required to undergo “fit and proper” testing upon winning re-election.

A.5 Governance Structure

Standard A5.1

A. Standard Summary

1. A bank shall have a clear governance structure with well-defined roles and responsibilities, and clear delineation between shareholders, Board (including committees), and leadership team.

B. Assessment Guidelines

1. Clear delineation means a state of affairs wherein banks’ stakeholder groups (shareholders, Board, leadership team) have well-defined, non-overlapping spans of control, governance policies and decision-making processes, and accountability mechanisms that ensure that no stakeholder group is given the responsibility to assess their own performance, and there is no undue influence of any one stakeholder group on another.

C. Assessment Process

1. Assessment against this standard shall be conducted by a third-party specialist firm from a list of CBI-approved firms.
2. As part of its assessment, the third-party specialist firm shall:
    a. Review all relevant governance documents (including organizational charts and descriptions of roles and responsibilities, to determine that the bank has embedded this delineation into its organization
    b. Review on-site inspection reports
    c. Review reports from CBI-appointed observers
3. Assessment shall be conducted annually.

Standard A5.2

A. Standard Summary

1. A bank shall have an Audit Committee; Risk Committee; Technology and IT Governance Committee, Environmental Standards, Social Standards, Sustainability, and Governance Committee and a Nomination and Remuneration Committee (NRC) which is detailed below. All the aforementioned committees must be established and governed in accordance with the CBI Governance Manual, and the chairman of each of these committees shall be an independent Board member.

B. Assessment Guidelines

1. Each board committee shall have its own set of clearly delineated responsibilities:
    a. The Audit Committee shall oversee the integrity of financial reporting, monitor compliance with applicable laws and regulations, and supervise the internal audit function. This committee is also responsible for ensuring that external audits are conducted in accordance with CBI standards, and that the bank has appropriate systems in place to manage financial risk

b. The Risk Committee shall be responsible for identifying, assessing, and mitigating risk throughout the organization. This includes overseeing the implementation of risk management policies and procedures necessary to safeguard the bank's assets and maintain its financial stability

c. The Technology and IT Committee shall be responsible for guiding a bank's technological direction, ensuring that it leverages technology effectively while managing risks and complying with regulations

d. The Environmental Standards, Social Standards, Sustainability, and Governance Committee is responsible for overseeing the bank's commitment to sustainable practices, ensuring compliance with environmental and social regulations, promoting corporate social responsibility initiatives, and integrating sustainability into the bank's strategic decision-making processes.

2. The term "independent Board member" is defined as per the definition contained in the Assessment Guidelines of Standard A3.1.

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.

2. CBI shall conduct the following activities, including but not limited to the following:

a. Review relevant committee charters and minutes of committee meetings, to verify that the committees exist, meet regularly, and address topics relevant to their responsibilities

b. Verify that the individual designated as chairman of each committee is actually independent, as per the results of assessment against Standard A3.1

3. Assessment shall be conducted annually.

Standard A5.3

A. Standard Summary

1. A bank shall have a Nomination and Remuneration Committee (NRC), which shall be responsible for nominating and approving new members of the leadership team except for Internal Audit and Sharia Internal Audit, for vetting all nominees to the Board, and for nominating and overseeing the approval process of new independent Board members.

a. The NRC shall be made up of at least 3 (three) members

b. All members of the NRC shall be independent Board members

c. All decisions taken by the NRC regarding confirmation of Board members must be unanimous

B. Assessment Guidelines

1. The term "independent Board member" is defined as per the definition contained in the Assessment Guidelines of Standard A3.1.

2. Unanimity, for the purposes of this standard, shall be defined as a vote of 3 (three) votes to zero. Votes resulting in fewer than 3 (three) votes (due to objection, abstention, or absence of one or more committee members) are not valid.

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.

2. CBI shall conduct the following activities, including but not limited to the following:
    a. Review NRC charter to ensure that these practices are embedded into the committee's governance rules
    b. Confirm that the individual(s) designated as independent member(s) of the committee are actually independent, as per the results of assessment against Standard A3.1
    c. Review minutes of the committee's meetings to verify unanimity rule is being observed
3. Assessment shall be conducted annually.

Standard A5.4

A. Standard Summary

1. Islamic banks shall establish a Sharia Supervisory Board (SSB), which shall be an independent body reporting directly to the Board of Directors. The SSB shall have full autonomy in overseeing the Sharia compliance of all operations, products, services, and contracts of the bank. The SSB shall be governed in accordance with CBI regulations and shall operate similarly to a Board Committee, while maintaining complete independence from management and the Board and being appointed directly by the general assembly.

B. Assessment Guidelines

1. The Sharia Supervisory Board must consist of at least five members, three of whom must hold at least a bachelor's degree in Islamic jurisprudence and two with expertise in banking, finance, or law.

2. All members must be independent – none may be shareholders, Board members, employees, or executives of the bank or any of its subsidiaries, nor may they have held such positions in the two years preceding their appointment.

3. No member may be affiliated with another Sharia Board of any other Islamic bank operating in Iraq.

4. The Chairman of the SSB must hold at least a Master's degree from a recognized university in Islamic sciences (including Islamic commercial jurisprudence), and have not less than three years of experience issuing fatwas or conducting academic research in Islamic finance.

5. The SSB shall hold regular meetings and submit reports to the Board of Directors.

6. The Board of Directors and the Chairman of the SSB are jointly responsible for notifying the CBI of any potential or actual conflicts of interest.

C. Assessment Process

1. The CBI shall assess compliance with this standard annually.
2. The CBI shall conduct the following activities, including but not limited to the following:
    a. Review the SSB charter and meeting minutes to confirm regularity of meetings, independence, and Sharia oversight.
    b. Verify the qualifications of all SSB members, in line with regulatory criteria.
    c. Ensure that no SSB member is currently or was recently involved in any executive or governance capacity within the bank or its affiliates.

d. Confirm that no dual appointments exist across multiple banks.

A.6 Leadership Team Fit and Proper Testing

Standard A6.1

A. Standard Summary

1. All individuals employed by a bank as part of its leadership team shall undergo "fit and proper" tests.

B. Assessment Guidelines

1. For the purposes of this standard, a bank's leadership team refers to the following roles or their effective equivalents:
   a. Chief Executive Officer (CEO)
   b. Chief Technology Officer (CTO)
   c. Chief Financial Officer (CFO)
   d. Chief Risk Officer (CRO)
   e. Chief Internal Audit Officer or Chief of Internal Sharia Audit for Islamic Banks
   f. Head of Compliance or Head of Sharia Compliance for Islamic Banks
   g. Anti-Money Laundering Officer (MLRO)
   h. All heads of business lines (e.g., Head of Retail Banking, Head of Commercial Banking)
   i. Anyone else who reports directly to the CEO or the Board of Directors
   j. Anyone exerting significant influence on the bank's management while being an employee or an officer of the bank's parent or affiliate (e.g., Group Head of Risk in the holding company that owns or controls the bank)
2. A "fit and proper" test is an evaluation of an individual's suitability for a particular leadership position. General "fit and proper" requirements for different executive roles, found in the CBI Governance Manual 2024, include the following:
   a. The individual shall not be a member of the Board of another bank, unless such other bank is affiliated (through an owner / parent or subsidiary relationship) with the bank in question
   b. The individual is fully dedicated to the management of bank business and shall have no other employment role with any other institution
   c. The individual must at least have a university degree and qualifications that are relevant to their specific role within the bank, specifically:
      i. The Chief Executive Officer (CEO) must be at least 30 (thirty) years old and hold a university degree in one of the following disciplines: economics, law, public administration, business administration, accounting, financial and banking sciences, statistics, banking management, investment and resource management, financial and accounting control, or any other relevant specialization. They must have not

less than 10 years of cumulative experience, including at least 5 (five) years in executive management within a bank.

ii. The Chief Technology Officer (CTO) must be at least 30 (thirty) years old and hold a university degree in a field related to information technology, such as computer engineering, computer science, or information technology. They must have not less than 10 (ten) years of relevant experience in IT and systems management, including 3 (three) years in a leadership position. The candidate must also have strong knowledge of project management and cybersecurity, demonstrate good proficiency in English, and must hold one of the following professional certifications: COBIT 2019 or ITIL 4

iii. The Chief Financial Officer (CFO) be at least 30 (thirty) years old and hold a university degree in accounting, finance, banking, business administration, or financial and accounting control. They must have at least 10 (ten) years of experience in banking, accounting, or financial management. The CFO must also be a member of a recognized professional accounting or auditing association.

iv. The Chief Risk Officer (CRO) must be at least 28 (twenty-eight) years old and hold a university degree in economics, public administration, financial management, accounting, banking and financial sciences, statistics, quality management, investment and resource management, financial and accounting control, or any other relevant specialization. They must have at least 7 (seven) years of experience in banking risk management, financial risk management, and regulatory affairs, including a minimum of 3 (three) years in a senior risk role. The CRO must be trained in risk governance and regulatory compliance and must hold the Certified Islamic Specialist in Risk Management certificate.

v. The Chief Internal Audit Officer or Chief Internal Sharia Audit Officer for Islamic Banks must be at least 30 years old and hold a university degree in accounting, banking management, public administration, business administration, financial management, financial and banking sciences, statistics, investment and resource management, or financial and accounting control. They must have at least 7 (seven) years of experience, including 5 (five) years in senior auditing roles within banks, and must be a member of a recognized professional auditing or accounting association.

   For the Chief Internal Sharia Audit Officer, the candidate must also be a member of a recognized professional Islamic auditing association with proven expertise and must hold one of the following certifications: Certified Sharia Auditor (CSA) or Certified Sharia Adviser and Auditor (CSAA).

vi. The Head of Compliance or Head of Sharia Compliance for Islamic banks must be at least 30 (thirty) years old and hold a university degree in law, public administration, financial management, accounting, financial and banking sciences, statistics, banking management, quality management, investment and resource management, or financial and accounting control. They must have at least 5 (five) years of experience in regulatory compliance or financial supervision, not less than 75 (seventy-five) hours of formal training in compliance practices, and must demonstrate good command of English. They must also hold one of the following certifications:

   (a) Certified Compliance Manager (GCI Certified Compliance Manager)

   (b) International Advanced Certificate in Compliance

   In the case of the Head of Sharia Compliance, the candidate must also hold the Certified Islamic Specialist in Governance and Compliance (CISGC) Certification.

vii. The Anti-Money Laundering Reporting Officer must be at least 30 (thirty) years old, must be an Iraqi national, and must hold a university degree in law, public administration, financial management, accounting, financial and banking sciences, statistics, banking management, quality management, investment and resource management, or financial and accounting control. The candidate must have not less than 5 (five) years of experience in banking, finance, or regulatory roles and must have

completed at least 75 (seventy-five) hours of formal training in AML/CFT practices. They must demonstrate good command of English and must hold one of the following certifications:

(a) Certified Anti-Money Laundering Specialist (CAMS)

(b) Certified Global Sanctions Specialist (CGSS)

viii. The Head of Retail Banking must hold a degree in economics, business, or financial management and have at least 7 (seven) years of banking experience including 3 (three) years in retail banking leadership.

ix. The Head of Commercial Banking must hold a degree in economics, law, or banking sciences and demonstrate at least 7 (seven) years of banking experience in corporate lending, credit, investment banking or SME finance.

d. The individual must have experience in banking or related businesses

3. In addition to the above requirements and those mentioned in the CBI Governance Manual 2024, the individual must also undergo a full background check that includes checks of criminal records and past disciplinary actions.

4. Whether for current leadership team members, or future hires, individuals must undergo "fit and proper" testing even if they underwent such testing as part of an earlier process with any institution.

5. It is permitted to have a gap in leadership roles for a period of no longer than 12 (twelve) weeks in cases of sudden resignations, dismissals or position vacancies. This shall not apply for the CEO position, which requires the board to immediately appoint an Interim CEO until a permanent CEO is appointed in the allowed period of 12 (twelve) weeks.

C. Assessment Process

1. Leadership team "fit and proper" tests shall be conducted by a third-party specialist firm from a list of CBI-approved firms.

2. The third-party specialist firm shall:

   a. Generate list of individuals at the bank requiring testing, including any "equivalent" roles that may have different names from those listed above

   b. Apply the "fit and proper" tests to the individuals within scope

   c. Request and receive from candidates complete sets of relevant documentation in support of the assessment, including but not limited to: an up-to-date curriculum vitae, certified copies of academic and professional credentials, employment contracts or appointment letters, financial disclosures, police clearance certificates, and reference letters from prior employers or regulators

   d. Flag any individuals who fail the "fit and proper" test, reporting results to the bank and CBI

3. All individuals who are members of the bank's leadership team must have undergone "fit and proper" testing by a specific deadline defined by CBI. Going forward, the process is only conducted when a bank hires a new member of the leadership team.

4. In addition to the tests mentioned above, the CBI shall conduct a final interview for the CEO, the CFO the CRO, the Head of Compliance / Head of Sharia Compliance for Islamic Banks, the Chief Internal Audit Officer/ Chief Internal Sharia Audit Officer for Islamic Banks and the MLRO prior to final approval of appointment.

3. Business Model Sustainability

B.1 Detailed Business Plan

Standard B1.1

A. Standard Summary

1. Each bank shall submit a new business plan detailing its 5-year strategy, key products and services, relevant pricing, target customer demographics and investment.
    a. Key products and services detailed in the business plan shall include loans, cards, deposits, and payments

B. Assessment Guidelines

1. The business plan shall include:
    a. A thorough analysis of the market, including:
        i. A competitor benchmarking section comparing pricing, service models, and customer experience against at least three licensed Iraqi banks, and planned differentiation strategies
        ii. A customer segmentation model that includes profiling of retail customers (e.g., by income level) and corporate/SME customers (e.g., by revenue, by sector), and link acquisition strategies to product design and pricing
        iii. A complete pricing matrix, covering all customer-facing charges such as lending rates, deposit yields, card fees, and payment processing costs, benchmarked against relevant statistics where available
        iv. An overview of observed market trends, highlighting shifts in consumer behavior and economic indicators that may impact the sector, along with potential opportunities for innovation and growth
    b. A robust go-to-market strategy, including:
        i. The bank's mission and vision
        ii. An outline of key products and services split by business (retail vs. corporate), including five-year launch roadmap
        iii. Identification of market segments that are underserved or have high demand for specific products or services
        iv. A geographic expansion plan that details deployment in specific governorates, timelines for digital or physical infrastructure activation, and use of agents or correspondent networks where applicable
        v. A detailed mitigation strategy for execution and market risks, including financial fallback options, alternative vendor strategies, and service continuity protocols
    c. An implementation plan, including - but not necessarily limited to - the following elements:
        i. Definition of clear, measurable objectives and milestones with corresponding dates
        ii. Definition of critical path that identifies essential tasks and their dependencies to determine the longest sequence of activities needed to complete implementation
        iii. List of step-by-step actions required to achieve objective of full implementation timelines, assigned responsibilities, and resource allocation

iv. Internal and external communication plan including communication strategies for stakeholders, cadence and content of regular updates, feedback mechanisms, and reporting structure

2. The business plan must be submitted in both Arabic and English.

3. The bank's business plan, strategy, operating model and financial projections must be properly aligned and interlinked.

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.

2. CBI shall conduct the following activities, including but not limited to the following:

   a. Review the business plan

   b. Request and review, as needed, supplementary materials that serve to support the viability, coherence, or robustness of any plans contained within the business plan, including but not limited to vendor quotations, market studies, technical feasibility analyses, or customer research to verify assumptions.

   c. Verify that each point described above in the Assessment Guidelines is addressed

   d. In the event of non-alignment with regulatory requirements or internal inconsistencies, CBI will return the plan for revision, and the bank must respond within 60 (sixty) business days of its receipt.

3. Assessment shall be conducted during the current reform program and repeated by banks based on the request of CBI, potentially every 3 (three) years.

4. Banks may provide, and CBI reserves the right to request any further relevant information to support assessment of the business plan.

Standard B1.2

A. Standard Summary

1. Each bank shall submit details on its operating model, including an overview of its people & organization, capabilities, technology infrastructure, physical infrastructure, and AML/CFT policies & procedures.

B. Assessment Guidelines

1. The operating model details provided shall include:

   a. A section on the bank's human resources and organization, including:

      i. A manpower plan that specifies headcount projections for each year by function (e.g., operations, risk, IT), showing growth trends aligned to customer volume, product complexity, and geographic expansion

      ii. Year 1 staffing plans that designate key leadership roles, including but not limited to: CEO, CFO, Chief Risk Officer (CRO), Chief Information Officer (CIO), Head of Internal Audit, Head of Compliance and Money Laundering Reporting Officer (MLRO).

      iii. An organizational chart reflecting clear reporting lines and key management committees

      iv. A remuneration framework including fixed / variable pay structures, max. bonus limits, long-term incentives, and oversight process for executive pay decisions.

b. A section detailing the bank's executive governance framework, specifically outlining the composition, responsibilities, authority limits, decision-making procedures, and meeting protocols of key committees (e.g. Executive Committee, Credit Committee and Risk Committee).

c. A section on the bank's capabilities, including:

   i. Job descriptions for CEO and all N-1 roles, including educational and professional certification requirements (e.g., CPA, CAMS, CISA) and prior experience thresholds

   ii. A formal succession plan for CEO and all N-1 roles, identifying backups for each function and including onboarding timelines, shadowing arrangements and readiness assessments.

   iii. Executed contracts, performance SLAs, data access protocols, and proof of compliance in cases where staffing is outsourced (e.g., IT, internal audit)

d. A section on the bank's technology infrastructure and information systems, which shall include:

   i. A comprehensive IT architecture and data flow framework, mapping core and peripheral systems, data sources, integration points, and transmission protocols

   ii. A core banking system(s) plan and diagram, specifying whether a single or multiple systems will be deployed, the identity of the system provider(s), and implementation timelines

   iii. A list of third-party Integrations and APIs required for core functionality, including payment gateways, credit bureaus, AML systems, and other critical external linkages

   iv. A cybersecurity and data protection plan, outlining the technical and procedural safeguards implemented to ensure data confidentiality, integrity, and availability, consistent with CBI specifications

   v. A resilience framework, comprising both a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP), clearly identifying recovery time objectives, fallback protocols, and site redundancy arrangements

   vi. A description of key outsourcing arrangements, including service providers, scope of outsourced functions, governance and monitoring mechanisms, and risk mitigation strategies

e. A section on the bank's infrastructure deployment plan, including:

   i. A branch network plan, outlining proposed branch locations, rollout timeline, prioritization by governorate, and anticipated customer coverage

   ii. An ATM network plan, including total number of ATMs, geographic distribution, and compliance with the minimum coverage ratios

f. A description of the bank's key policies, processes, controls, and employ systematic tools related to anti-money laundering (AML) and combating the financing of terrorism (CFT), and sanctions practices

   i. Such policies, processes, controls, and systematic tools must be aligned with global standards, industry best practices, and CBI requirements as detailed in Section D.2

g. A section on the bank's risk management framework covering all types of risks, including:

   i. Risk governance structure, detailing the roles and responsibilities of the Board, Board Risk Committee, Executive Management, and the Chief Risk Officer (CRO) in overseeing risk management activities. The section should illustrate how risk oversight is embedded within the bank's decision-making hierarchy.

   ii. Risk appetite framework, including a documented Risk Appetite Statement (RAS) that articulates the bank's willingness to accept risk across key dimensions (e.g., credit, market, liquidity, operational,

compliance). The RAS should include quantitative and qualitative thresholds, early warning indicators, and escalation procedures.

iii. Risk identification and assessment process, describing how risks are identified at the entity-wide, business line, and product level. This should include the methodologies for assessing inherent vs. residual risks and the tools used for qualitative and quantitative risk analysis.

iv. Risk measurement and monitoring systems, providing details on the metrics used to monitor each major risk type (e.g., Value at Risk (VaR), Expected Credit Loss (ECL), liquidity coverage ratio (LCR), operational loss events), as well as dashboards and frequency of risk reporting to senior management and the Board.

v. Risk mitigation controls and processes, outlining key preventive and detective measures in place to manage identified risks. This should include limits frameworks (e.g., credit exposure limits) and risk transfer mechanisms (e.g., insurance, collateral), and internal control systems.

h. A section on the bank's compliance monitoring framework, including:

i. Compliance governance structure, outlining the role and responsibilities of the Compliance Function, including reporting lines to senior management and the Board (or Audit/Compliance Committee), and the independence of the Compliance Officer or MLRO.

ii. Compliance monitoring plan, describing the bank's approach to identifying, assessing, and monitoring regulatory compliance risks across all business functions. This should include a risk-based monitoring schedule, frequency of reviews, and targeted testing activities.

iii. Issue management and escalation, detailing how compliance breaches are recorded, investigated, escalated, and remediated, including documentation practices and timelines.

iv. Reporting mechanisms, outlining how findings are reported to senior management and the Board, including the format, frequency, and contents of regular compliance reports.

v. Integration with training and awareness, noting how insights from compliance reviews feed into periodic staff training and updates to internal policies and procedures.

i. The Bank's key manuals covering internal policies, lending criteria, etc.

2. The planned operating model must be submitted in both Arabic and English.

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.

2. CBI shall conduct the following activities, including but not limited to the following:

a. Review the operating model details

b. Request and review, as needed, supplementary materials that serve to support the viability, coherence, or robustness of any relevant plans or elements

c. Verify that each point described above in the Assessment Guidelines is addressed

d. In the event of non-alignment with regulatory requirements, the plan will be returned for revision with a compliance response deadline of 60 (sixty) business days

3. Assessment shall be conducted during the current reform program, and repeated by CBI on an as-needed basis.

4. The Central Bank retains the authority to review, interview, or reject any nominee to a control or senior management position on grounds of experience, independence, or regulatory history.

5. Banks may provide, and CBI reserves the right to request, any further relevant information to support assessment of the business plan.

Standard B1.3

A. Standard Summary

1. Each bank shall submit a new financial plan detailing a clear path to profitability, supported by a five-year financial forecast.

B. Assessment Guidelines

1. The forecast must include complete and five-year income statements, balance sheets, and cash flow statements, presented on an annual basis.
2. All revenue projections must be disaggregated by product line (e.g., personal loans, SME loans, debit cards, current accounts), with associated pricing assumptions, uptake rates, and volume metrics explicitly stated.
3. Expense projections must include granular cost categories, such as technology infrastructure, employee compensation, vendor contracts, office operations, marketing, and regulatory compliance.
4. The bank must also provide projections of key capital and liquidity metrics including capital adequacy ratio, liquidity coverage ratio and net stable funding ratio for 5 years.
5. If breakeven is projected beyond twenty-four months, the forecast must include an equity capital injection schedule, with accompanying signed shareholder funding commitments or escrow-backed proof of funds.
6. The financial model must directly correspond with the business plan, including reflected investments in IT, staffing, and infrastructure, and must incorporate all operating costs arising from CBI compliance requirements.
7. The forecast and risk management policy must be certified by the CFO and the Head of Internal Audit, with a formal cover letter confirming internal review, Board approval, and full reconciliation with all supporting plans and assumptions
8. The financial plan must be submitted in both Arabic and English.

C. Assessment Process

1. Assessment against this standard shall be conducted by CBI.
2. CBI shall conduct the following activities, including but not limited to the following:
   a. Review and validate all financial forecasts and plans developed by the bank as per the above guidelines
   b. Verify that each point described above in the Assessment Guidelines is addressed
3. The bank's financial plan and the validator's report must be submitted to the CBI for review.
4. In the event of non-alignment with regulatory requirements or internal inconsistencies, the plan will be returned for revision with a compliance response deadline of 60 (sixty) business days.
5. Assessment shall be conducted during the current reform program and repeated by CBI on an as-needed basis.
6. Banks may provide, and CBI reserves the right to request, any further relevant information to support assessment of the business plan.

B.2 Core Banking and Critical Systems

Standard B2.1

A. Standard Summary

1. Each bank shall maintain a core banking system and the necessary systems providing critical functionalities in alignment with CBI-issued systems requirements.

B. Assessment Guidelines

1. The bank must adopt and operate an integrated suite of systems providing critical functionalities sourced from reputable and internationally recognized providers.
2. Critical functionalities shall be defined as the essential processes and capabilities required to deliver the bank's core products and services in a secure, compliant, and efficient manner. For example, these functionalities should include customer onboarding and KYC, account management, deposits and withdrawals, loan origination and servicing, payments and transfers (domestic and international), trade finance processing, treasury and liquidity management, financial accounting and reconciliation, regulatory and compliance reporting, and internal audit workflows. The systems providing these functions must provide up to date access to data and the design must strive for single authoritative data sources for each data element, where possible.
3. The system(s) must be fully integrated with the applicable national and CBI-mandated platforms in alignment with CBI guidelines, for example:
    a. Real-Time Gross Settlement (RTGS)
    b. Automated Clearing House (ACH)
    c. National Switch (NS)
    d. Anti-Money Laundering (AML) systems
    e. Central Bank Reporting Interfaces (e.g., CBR, CMS)
    f. Intrabank transfers
    g. SWIFT network for MX file extraction
    h. ICI system for CBI Credit Bureau
    i. Payment gateways used by licensed electronic payment companies in Iraq
    j. Card networks
    k. Banking Supervision Reporting System (BSRS)
    l. Instant Payment Scheme (IPS)
    m. Unified Government Payments Gateway (UGPG)
    n. Local Card Scheme
    o. Any new system mandated by CBI
4. The system(s) must enable integrations with external systems and services and must adhere to the following requirements:
        a. All payment communications must comply with ISO 20022 messaging standard;
        b. All Application Programming Interfaces (APIs) should conform to the OpenAPI standard;

c. The system must adopt internationally recognized coding standards, including but not limited to IBAN (International Bank Account Number), BIC (Bank Identifier Code), and ISIC (International Standard Industrial Classification)

5. The system(s) should allow for well-structured data and support the exporting of data for analytics, reporting, logging and archiving, the system(s) should also adhere to the BCBS239 principles for risk reporting.
6. The bank must maintain a secure and isolated test environment where system upgrades and patches are tested before deployment into the live environment.
7. The system(s) must support and enforce role-based access control (RBAC) for all users, particularly for sensitive operations.
8. The system(s) must support and enforce multi-factor authentication (MFA) for all customers with a minimum of the following protections being in place for all customers:
    a. Customer ID, with partial pin and password challenge with second factor authentication OR biometric credentials via TouchID, FaceID or similar, for read-only access to an account;
    b. Additional factor authentication different to the above for any actions pertaining to the instruction of transactions for existing payees;
    c. Full biometric validation, or re-challenge for changes to customer details or addition of new payees
9. Access to unauthorized users from within the bank on critical data and core banking system functionalities must be strictly restricted and there should be clear delineation of roles and authorities to the specific users that shall obtain such access only if necessary.
10. The system(s) must support a tiered notification framework that ensures critical messages are delivered through the most secure and immediate channels. At a minimum:

    a. Security-critical alerts—such as failed login attempts, account blocks, password changes, or suspicious activity—must be sent via SMS or automated voice call, ensuring high visibility and immediate user awareness

    b. General notifications and updates—such as successful transactions, balance updates, or promotional messages—may be delivered via push notification, email, or other channels, in accordance with the customer's selected preferences

11. The system(s) must support electronic onboarding (including self-registration, digital onboarding, and digital KYC) using a comprehensive suite of advanced verification technologies that meet the following minimum functionality standards:

    a. Enable the automated and accurate ingestion of customer data using technologies such as OCR, barcode scanners, or NFC transmission to minimize manual entry and data entry errors.

    b. Leverage biometrics and facial recognition to verify that identity documents correspond to the actual customer and to establish a true likeness.

    c. Incorporate liveness detection to confirm the physical presence of the customer during the onboarding process.

    d. Include safeguards against identity fraud by deploying techniques to detect and prevent the use of AI-generated deepfakes or synthetic identities.

12. The bank must maintain a detailed list of systems and modules integrated with the core banking system, including each module's function and technical configuration.
13. The bank must ensure a minimum system uptime (availability) of at least 99.5% (ninety-nine and one-half percent), measured monthly at the individual customer level, for all critical IT infrastructure and core banking services, excluding periods of planned maintenance notified in advance. The uptime calculation must account for service availability across geographic regions, and the target must be met for at least 95% (ninety-five percent) of the active customer base.
14. The bank must maintain the standards of the following ISO certifications:

a. **ISO 27001**: Information Security Management

b. **ISO 22301**: Business Continuity Management

c. **ISO 20000**: IT Service Management

d. **ISO 25011**: Software Quality

15. The implementation of the required ISO standards and other relevant international standards mentioned in this document shall be in a phased approach and banks shall provide an analysis of the cost and expected timelines for implementation.

16. The bank shall maintain a binding, long-term support and maintenance contract with each core banking system vendor to guarantee continued service and rapid remediation of critical issues. At a minimum, the contract must include:

    a. Service Level Agreements (SLAs) – Detailed, measurable SLAs covering:

        i. Incident severity tiers (e.g., Critical P1, High P2, Medium P3, Low P4);

        ii. Maximum response times (e.g., P1 ≤ 30 minutes, P2 ≤ 1 hour);

        iii. Maximum resolution or workaround times (e.g., P1 ≤ 4 hours, P2 ≤ 8 hours)

    b. Preventive Maintenance & Upgrades – A schedule for regular system health checks, security patching, version upgrades, and regression testing, all executed first in the bank's isolated test environment

    c. Escalation & Governance – A jointly agreed escalation matrix up to senior vendor executives and the bank's CRO/CIO for unresolved P1 or repeated P2 incidents, plus quarterly service-review meetings to track KPI performance and upcoming change releases

    d. Knowledge Transfer & Documentation – Obligations for the vendor to provide updated technical documentation, administrator training, and hand-over of source configuration or deployment playbooks to ensure the bank's self-sufficiency

    e. Business Continuity Support – Commitment to assist in disaster-recovery drills, backup verification, and rapid on-site or remote support during declared BCP events

14. A dedicated senior official must be appointed to oversee the implementation, maintenance, and compliance of the core banking system. This individual must have relevant certifications and report to the executive leadership.

15. The system must be hosted in data centers located within Iraq and be subject to CBI data sovereignty requirements.

16. Banks shall notify the CBI of any major enhancements, feature launches, or policy changes related to their core banking system(s) at least 14 (fourteen) calendar days in advance. Security incidents, system breaches, or customer data exposures must be reported within 48 (forty-eight) hours of discovery. In case of CBI not raising any objections, the bank shall be allowed to proceed with the planned changes.

C. Assessment Process

1. The bank must submit detailed technical documentation on its core banking system(s) to a third-party IT assurance company, including:

    a. Name and version of the system(s)

    b. Name of the provider(s) and implementation date

c. System architecture and integration diagrams

d. Module descriptions and supported functionalities

e. User access protocols and security features

f. Summary of testing environments and disaster recovery arrangements

2. The bank must submit a third-party audit report from a CBI-approved IT assurance firm, which assesses:
   a. Compliance of the core banking system(s) with CBI integration and interoperability requirements

   b. Performance and uptime levels

   c. Compliance with data encryption and storage protocols

   d. Security, access control, and authentication mechanisms

   e. Test environment readiness and failover mechanisms

   f. Accuracy and integrity of reporting modules

   g. Compliance with the above-listed ISO standards

3. On an ongoing basis, the bank's core banking system must be subject to annual assurance reviews conducted by a third-party cybersecurity or IT assurance firm pre-approved by the CBI. The assurance report must be submitted to the Board of Directors and the CBI within 60 (sixty) days of the end of the financial year.
4. The bank must develop a remediation plan in collaboration with the assurance provider to address any compliance gaps or identified weaknesses. This plan must be submitted to the Board and the CBI within 180 days of the financial year-end and the bank must adhere to executing it as per the timelines detailed in the plan.
5. The CBI reserves the right to conduct supplementary audits, request demonstration of functionalities, inspect system logs, or conduct interviews with the system administrators or vendor representatives.

B.3 Online Banking

Standard B3.1

A. Standard Summary:

1. Each bank shall provide online banking services in alignment with CBI-issued specifications.

B. Assessment Guidelines:

1. Each bank must maintain both a web-based and mobile-based digital banking platform accessible to all individual retail account holders. In addition, banks must provide, at a minimum, a web-based online banking platform for corporate account holders. These platforms must offer continuous access to core banking services, comply with CBI-mandated availability and cybersecurity standards, and be fully available in both Arabic and English.

2. For the purposes of this requirement, "online banking" for retail customers shall refer to the delivery of banking services via (i) a secure website operated by the bank, and (ii) a mobile banking application available for public download on iOS and Android platforms. While for corporate customers shall refer to the delivery of banking services at least via a secure website operated by the bank. All these channels must be integrated with the bank's core banking system and capable of real-time transaction processing.

3. The relevant digital channels should also be made available to corporate clients, maintaining different types of corporate accounts with the bank.

4. Banks shall ensure that both the online banking website and mobile application maintain a minimum monthly up-time of 98% (ninety-eight percent), excluding scheduled maintenance. Unplanned outages exceeding 4 (four) continuous hours must be reported to the Central Bank of Iraq within 24 (twenty-four) hours, along with details of the incident and expected resolution timeline.

5. The following core functionalities must be supported across both channels for retail customers: (i) account balance and transaction history (minimum 90-day lookback), (ii) intra-bank and inter-bank fund transfers, (iii) update of personal information (e.g., mobile number, address), (iv) self-registration, digital KYC and digital onboarding, (v) access to electronic statements, and (vi) branch locator and FAQs.

6. The following core functionalities must be supported across online channels for corporate clients: (i) account balance and transaction history (minimum 180-day lookback), (ii) intra-bank and inter-bank fund transfers (including bulk payments and payroll processing), (iii) initiation and approval workflows for transactions (with multi-level authorization), (iv) access to electronic account statements and downloadable reports, and (v) service request management (e.g., cheque book requests, stop payments).

7. All online banking platforms shall implement two-factor authentication (2FA) for login and for sensitive transactions (e.g., fund transfers, profile updates). Acceptable 2FA mechanisms include OTP sent via SMS or email, authenticator applications, or biometric authentication.

8. The online banking interface must be available in both Arabic and English. It must be designed in a user-friendly manner that enables intuitive navigation and complies with basic digital accessibility standards in line with WCAG 2.2 (e.g., minimum font size, contrast, mobile responsiveness).

9. Banks must provide a self-service digital onboarding option for existing retail customers to register for online banking using secure identity verification methods. Mandatory acceptance of the bank's terms of service and privacy policy must be obtained at the time of digital onboarding.

10. All online banking transactions involving account access, fund transfers, card services, and profile updates must generate immediate SMS or email notifications to the customer.

11. An auditable digital activity log must be maintained by the bank for a minimum of 6 (six) months and made available to the CBI upon request.

12. Banks must maintain a clear escalation process and customer support response framework for all digital banking issues. Response timelines for technical or transactional complaints must be disclosed within the application or website, and complaints must be trackable by reference number.

13. Banks shall notify the CBI of any major enhancements, feature launches, or policy changes related to their online banking platforms that are not considered periodic maintenance at least 14 (fourteen) calendar days in advance. Security incidents, system breaches, or customer data exposures must be reported within 48 (forty-eight) hours of discovery. If CBI does not raise any objections, the bank shall be allowed to proceed with the planned changes.

C. Assessment Process:

1. A third-party specialist firm – from a list of CBI-approved firms – shall assess the availability, functionality, and security of each bank's online banking channels at least once per year.

2. This assessment shall include:

    a. A review of uptime and incident logs

    b. Simulated user journeys to test core functionality

    c. A verification of 2FA and alert mechanisms

    d. A review of customer onboarding flow, language accessibility, and complaint resolution processes

3. The third-party specialist firm may also conduct spot audits or initiate targeted reviews based on customer complaints or technology incidents. Banks are expected to cooperate fully with such assessments and provide access to backend dashboards, audit trails, and compliance documentation on request.

B.4 Bank Branches

Standard B4.1

A. Standard Summary:

1. Each bank shall maintain a minimum of 5 (five) physical branches that are located inside Iraq and are open for business to the public on all days and during all CBI-specified office hours as referenced in Article 34 of the 2004 Banking Law.

B. Assessment Guidelines:

1. A "physical branch" means a fixed-location, enclosed facility owned or leased by the bank, offering face-to-face banking services. Each branch must provide core banking functions, including account opening, deposits, withdrawals, fund transfers, and issuance or encashment of instruments such as pay orders and demand drafts. Temporary sites, digital-only service points, standalone ATMs, or mobile units do not qualify.
2. To qualify as an official branch of a bank, the premises must have an average net usable area of 75 (seventy-five) square meters for client-facing activities. The HQ could be also considered as a physical branch if it includes an average of 75 square meters for client facing activities.
3. Banks shall be required to maintain a minimum of 5 (five) physical branches. Of these five, at least 2 (two) branches must be located in small cities and rural areas.
4. For the purposes of this standard, small cities shall mean cities with a population of 0.1-0.5 million, while rural areas shall mean areas with a population less than 0.1 million. Population data must be drawn from the most recent Iraqi Government publications.
5. All physical branches must operate at a minimum from 8:00 AM to 3:00 PM on official business days unless an exemption is granted by the CBI due to holidays or exceptional circumstances. Any deviation requires prior CBI approval.
6. Banks must obtain prior approval from the CBI for any proposed opening, closure, or relocation of branches. Applications must include zone and city information, justification, proposed services, and feasibility assessments. In small cities or rural areas, relocation or closure is permitted only within the same city or governorate and must not interrupt service.
7. Once approval to open a branch is granted, the bank must complete all setup activities — including staffing, infrastructure, and regulatory clearances — within 6 (six) months. A certificate of compliance from internal audit must be submitted before launch. The CBI must be notified within 14 (fourteen) calendar days of commencement.
8. Customers must be notified at least 60 (sixty) days in advance of any branch closure or relocation. Communication must include SMS, email, on-site notices, and updates to the bank's website, along with contact details for assistance.

C. Assessment Process:

1. A supervisory committee appointed by the Central Bank of Iraq shall conduct random inspections of bank branches not less than once per year to assess operational compliance with the branch network plan submitted in accordance with Standard B1.1. These inspections shall include a review of branch accessibility, staffing adequacy, service availability, and adherence to approved operating schedules.

B.5 ATM Coverage

Standard B5.1

A. Standard Summary:

1. Each bank shall maintain a ratio of at least one ATM for every 1,000 (one thousand) retail customers, or such ratio as may be defined by CBI. At least 25% (twenty-five percent) of a bank's total number of ATMs in operation must be located outside the limits of the main cities of Iraq. All ATMs must be operational and available for use by a bank's customers for a minimum percentage of time.

B. Assessment Guidelines:

1. Each ATM shall, at a minimum, provide cash withdrawals, account balance inquiries, and PIN change services. At least 20% (twenty percent) or one (whichever is higher) of the ATMs in the ATM network must be Cash Deposit Machines (CDMs) that support deposits, bill payments, and other advanced features.
2. At least 25% (twenty-five percent) or one (whichever is higher) of a bank's total ATMs in operation must be located outside the limits of the main cities of Iraq, particularly in small cities or rural areas as defined below.
3. For the purposes of this standard, small cities shall mean cities with a population of between 0.1 and 0.5 million, while rural areas shall mean areas with a population less than 0.1 million. Population data must be drawn from the most recent Iraqi Government publications.
4. Banks operating mobile ATMs must maintain deployment schedules, location records, and monthly service reports, to be submitted to the CBI upon request.
5. All ATMs must operate 24/7, except during scheduled maintenance or force majeure. Any service disruption exceeding four continuous days must be formally reported to the CBI with supporting justification and a resolution timeline.
6. Banks must notify the CBI of all new ATM installations, with required documentation including location coordinates, lease or site-use agreement, directional site photos, and any additional materials requested by the CBI.
7. Banks must obtain prior approval from the CBI for any proposed closure or relocation of ATMs. Applications must include location coordinates, lease or site-use agreement, directional site photos, and any additional materials requested by the CBI. In small cities or rural areas, relocation or closure is permitted only within the same city or governorate. Requests for closure will be evaluated based on the network impact and service adequacy in the area.
8. If an ATM does not meet closure criteria but removal is still requested, the bank must propose a replacement within the same governorate and at a location approved by the CBI. Activation of the replacement must be reported within the required timeline.

9. Each ATM must display a visible identification plate with the ATM number and customer support contact in Arabic and English. Card acceptance details must be shown clearly. ATM locations and service information must be accurately reflected on the bank's website and mobile apps.

C. Assessment Process:

1. Assessment against this standard shall be conducted by a supervisory committee appointed by CBI.
2. The committee shall:
    a. Conduct random inspections of ATMs not less than once per year to verify the availability of ATM operability, customer reach, and compliance with approved service levels
    b. Verify adherence to minimum required services (withdrawal, balance inquiry, PIN change) and confirm that at least 20% (twenty percent) of the network comprises active CDMs with deposit and bill payment functions
3. The CBI shall also conduct unannounced inspections of the bank's ATM network to assess compliance with placement, service, technical, and accessibility standards.
4. CBI shall monitor ATM availability through system-generated uptime logs and inspect any reports of outages exceeding four days. Banks must provide incident reports and remediation plans for any extended downtime.

B.6 Customer Services

Standard B6.1

A. Standard Summary:

1. Each bank shall operate a customer service center that meets the minimum service coverage levels prescribed by the Central Bank of Iraq.

B. Assessment Guidelines:

1. The customer service center must be accessible, responsive, and equipped to handle customer inquiries and complaints in a timely and efficient manner for both retail customers and corporate customers.
2. Each bank shall operate a contact center that is accessible to customers through telephone and digital channels 24/7.
3. The contact center must have a dedicated team trained to respond to customer inquiries and record complaints. The bank shall maintain sufficient staffing levels to minimize waiting times and ensure timely responses.
4. All customer complaints received via the contact center must be acknowledged within two business days and resolved within seven business days from the date of receipt. Exceptions may be granted in cases requiring further investigation, provided the delay is documented and communicated to the customer.
5. A centralized complaint management system shall be maintained to record, track, and escalate complaints received through the contact center. The system must enable categorization of complaints, monitoring of resolution status, and reporting of closure rates.
6. The bank shall clearly communicate the availability, contact details, and service hours of its contact center through all customer-facing platforms, including websites and mobile applications.

7. All contact center staff shall receive role-specific training in customer service protocols, complaint resolution procedures, and applicable regulatory standards. Completion of initial and refresher trainings shall be tracked and documented.
8. All complaints lodged against the bank on the government complaints platform shall be resolved by the bank within a maximum of 5 (five) working days.

C. Assessment Process:

1. Assessment against this standard shall be conducted by CBI.
2. CBI shall assess compliance through:
    a. Review of contact center reports
    b. Inspections of operational records
    c. Analysis of complaint resolution timelines
3. During assessments, banks must provide documentation including call logs, complaint registers, escalation records, training files, and internal audit results related to the contact center.
4. Quarterly reports must be submitted to the CBI, detailing:
    a. The total number of complaints received via the contact center
    b. Average response and resolution times
    c. Complaint categories
    d. Corrective actions taken for recurring issues.
5. The bank must demonstrate consistent adherence to the prescribed service hours and complaint resolution timelines, including compliance with the 7-business-day requirement.

B.7 Infrastructure & Data

Standard B7.1

A. Standard Summary:

1. All banks shall establish strong, secure, and stable infrastructure that is resilient and can withstand cyberattacks, aligned with CBI specifications detailed below.
2. Bank should protect all data from unauthorized access and tampering, in alignment with CBI specifications detailed below.

B. Assessment Guidelines:

1. The bank must establish and maintain a secure, resilient, and scalable IT infrastructure capable of protecting sensitive financial, personal, and transactional data across its core and peripheral systems. This infrastructure must support high-availability operations, provide fault-tolerant architecture, and include disaster recovery arrangements specific to the bank's data environment.
2. The bank must adopt a data classification and tiering framework that categorizes data based on its sensitivity and criticality to the bank's operations, customers, and regulatory obligations. Based on this framework, the bank shall apply encryption controls as follows:

a. **Tier 0 / Tier 1 Data (Mandatory Encryption at Rest and in Transit):**

i. **Customer Master Data:** full name, date of birth, identification documents, national identification number, passport number, etc.

ii. **Authentication Data of Customers:** passwords, PINs, security questions and answers, biometric identifiers (fingerprint data, facial recognition data).

iii. **Contact Data of Customers:** phone numbers, email addresses, residential and mailing addresses.

iv. **Static Data:** account identifiers, IBAN numbers, credit card numbers, and similar static customer financial identifiers.

v. **Selected Product Data:** product type, product terms, interest rates, applicable fees where linked to identifiable customer profiles.

vi. **Selected Transaction Data:** transaction amounts, transaction counterparties, transaction reference numbers, time stamps, location of transaction.

b. **Tier 2 Data (Encryption Strongly Recommended but Not Mandatory at Rest; Mandatory in Transit):** Data that is important to bank operations but not directly identifying customers, including internal management reports, certain financial performance metrics, internal audit data, and some non-customer product data.

c. **Tier 3 Data (General Business Data, Optional Encryption):** Publicly available data or internal bank data not containing sensitive customer information (e.g., marketing material, public disclosures, external communications).

3. The bank must implement a multi-layered cybersecurity defense system including for example WAF, Next-Gen Firewall, IDS/IPS, SIEM/SOC, PAM, IAM, EDR/NDR/XDR. These solutions must be sourced from a reputable and recognized provider.

4. The bank must maintain a minimum system uptime (availability) of at least 99.5% (ninety-nine and one-half percent) for its critical IT infrastructure and core banking services excluding scheduled downtime.

5. Tier 0 / Tier 1 data, whether stored in on-premises servers, cloud environments, or off-site backups must be protected by layered security controls, including intrusion prevention systems, access control restrictions, and multi-factor authentication; it should also be accessible only by authorized personnel.

6. Physical data centers and servers used by the bank must exist inside Iraq and must include the following specifications: (i) physical access control device to restrict access to authorized personnel; (ii) include surveillance cameras covering the entire space and recordings kept at least the previous 6 (six) months; (iii) include raised flooring or smart racks with fire suppression pipes installed beneath; (iv) equipped with fire suppression system using FM200 gas; (v) include back up fire extinguishers that are gas based; (vi) equipped with sensors to detect heat, smoke, humidity and water leakage; (vii) connected to a backup power source and (viii) equipped with primary and back up cooling systems. In general, these data centers shall be considered the primary data centers of the bank and shall abide by all Tier 3 data center specifications issued by The Uptime Institute.

7. The bank must maintain a detailed inventory of all data storage environments and processing systems, clearly indicating where and how customer data is stored, encrypted, replicated, and destroyed. Documentation must also include policies on data classification, retention schedules, geographic storage location (local or cross-border), and contingency access protocols.

8. The bank shall establish and implement documented policies governing the deletion of data from all storage and processing environments, in compliance with applicable data protection laws and regulatory requirements.

a. **Permissible Deletion:** Data may be deleted only: (i) where the applicable legal or regulatory retention period has expired; (ii) in response to a verified data subject request, where legally permissible; (iii) upon formal clearance of regulatory, legal, or audit holds; or (iv) as part of approved operational processes for non-critical data

b. **Scope of Data:** Deletion policies shall cover customer data, internal operational data, system data, and ancillary data, with particular attention to data categories defined in the bank's data classification and retention schedules

c. **Logging and Records:** The bank shall maintain a complete and auditable log of all data deletions, recording at minimum: data type, deletion rationale, date and time of deletion, system/environment affected, and identity of the authorized actor. Such logs shall be retained for not less than 5 (five) years or longer where required by applicable law or internal policy

9. The bank must ensure abiding by the requirements and specifications of the following: (i) ISO 27001; (ii) ISO 20000; (iii) ISO 22301; (iv) 25011 and (iv) PCI DSS.

10. The implementation of the required ISO standards and other relevant international standards mentioned in this document shall be in a phased approach and banks shall provide an analysis of the cost and expected timelines for implementation.

11. The bank shall maintain a detailed Incident Response Plan (IRP) related to any cybersecurity breaches and the plan shall be updated on an annual basis.

12. Where the bank outsources any data processing activity or function to a third-party service provider, it shall ensure that such provider complies with security standards that are not less stringent than those applied by the bank to its own systems and processes.

13. Where the bank outsources any data processing activity or core banking function to a third-party service provider, it shall ensure that such provider signs an NDA "Non-Disclosure Agreement" with the bank.

14. A senior executive must be appointed to oversee cyber security, data security governance and infrastructure compliance. This individual must ensure the bank's infrastructure, encryption standards, and storage policies remain up-to-date and aligned with evolving CBI directives and global best practices

15. The bank must abide by all other CBI circulars, regulations and directives related to cybersecurity, data and technology infrastructure.

16. The bank must also ensure full compliance with the Cobit 19 IT governance framework as well as the Cyber Resilience Controls and related instructions issued by the CBI.

C. Assessment Process:

1. The bank must submit documentation evidencing its infrastructure architecture, data encryption configurations, and data storage policies. This must include system diagrams, technical specifications, encryption protocols in use, and a register of key management procedures (excluding sensitive key material).

2. The bank must also submit a third-party audit report issued by a CBI-approved IT assurance firm. This report must include an assessment of the bank's infrastructure, security, encryption robustness, data classification framework, access control configurations and data center/ servers' compliance. The report must be dated within 12 (twelve) months of submission and must include an attestation of independence.

3. On an annual periodic basis, the bank's compliance with all infrastructure and encryption specifications mandated by the Central Bank of Iraq (CBI) must be independently validated by a third-party cybersecurity or IT assurance firm that is pre-approved by the CBI. This firm shall conduct a formalized audit and testing process to evaluate the bank's actual technical configurations, the effectiveness of its encryption protocols, and its overall

cyber risk posture. The firm is required to produce a comprehensive assurance report, which must be submitted to both the bank's Board of Directors and the CBI. This report should include a detailed assessment of compliance, identification of any gaps relative to regulatory requirements and industry best practices, and specific, actionable recommendations for enhancement.

4. The third-party assurance process shall be conducted on an annual basis and the assurance report shall be submitted to the board and the CBI within a period of a maximum of 60 (sixty) days since the close of the financial year.

5. Where material gaps or risks are identified, the bank must submit a remediation plan developed in coordination with the third-party assurance company to ensure closing and existing compliance gap as well as actioning any recommendations for enhancement. This remediation plan shall be shared with the bank's board of directors and the CBI within a period of maximum 180 (one hundred and eighty) days since the close of the financial year, with timelines and ownership clearly assigned.

6. The CBI will supervise the relevant teams within the bank to ensure actioning of all elements of the submitted remediation plan. The CBI shall conduct onsite visits and meetings with the relevant teams, at the discretion of the CBI and throughout the year to ensure that all the required actions regarding the remediation plan have been taken.

7. Where required, the Central Bank may request supplementary testing logs, penetration test summaries, or results of vulnerability assessments conducted as part of the independent assurance process. CBI may also conduct direct interviews with the executives responsible or technical leads.

8. This third-party assurance process shall be conducted in addition to, and not in substitution of, the obligations relating to data storage and processing as specified under Article 38 of the 2004 Banking Law. Compliance with both sets of obligations is mandatory.

B.8 Payment Systems

Standard B8.1

A. Standard Summary:

1. All banks shall have, within the bank, capabilities that allow them to offer required functionalities – as defined by CBI – related to issuing of payment cards to all retail customers.

B. Assessment Guidelines:

1. The bank must have the technical and operational capabilities either in-house or through outsourcing agreements to issue and manage payment cards either as an issuer or a partner, including (at a minimum) debit cards. These capabilities must be embedded or integrated within the bank's infrastructure and should include systems for card generation, issuance, activation, PIN management, 3D Secure security feature, fraud prevention, dispute resolution, and card lifecycle management.

2. All card operations must comply with the Payment Card Industry Data Security Standard (PCI DSS) and the Europay, Mastercard, and Visa (EMV) standard, and must meet any specific technical specifications, certification requirements, or security controls outlined by the Central Bank of Iraq. Where services are outsourced, the bank remains fully responsible for compliance and must maintain end-to-end oversight, risk controls, and exit strategies.

3. In the case of card issuance, the bank must be required to operate a CMS (Card Management System) that is fully integrated with the core banking system to ensure real-time account linkage and settlements.

4. All payment cards and methods must be supported by a fraud detection and prevention framework that enables the application of risk-based authentication, including two-factor authentication (2FA) where appropriate. The system must be capable of dynamically adjusting authentication requirements based on the type, value, and behavioral context of each transaction. 2FA mechanisms—such as PIN entry at PoS or OTP via SMS during online transactions—shall be required for high-risk or unusual transactions, while low-risk or recurring behavior-based transactions shall follow a streamlined authentication process to optimize the customer experience without compromising security.

5. Additionally, banks must comply with other relevant international standards for card security, data encryption, authentication, and tokenization. The full list of applicable standards shall include but is not limited to: (i) ISO/IEC 7812 (Identification of Issuers); (ii) ISO/IEC 8583 (Financial Transaction Card-Originated Messages); (iii) ISO 20022 (Financial services messaging standard); (iv) PCI PIN Security Requirements; (v) 3-D Secure (authentication for online transactions).

6. The banks must have the technical and operational capabilities either in-house or through outsourcing agreements to provide and manage PoS (Point of Sale) and PoC (Point of Contact) devices to corporate clients. These capabilities must be embedded or integrated within the bank's infrastructure and should include systems for device issuance, activation, fraud prevention and dispute resolution.

7. Cards as well as PoC and PoS machines offered by any bank either directly or through partnerships/ outsourcing agreements must support contactless payment features.

C. Assessment Process:

1. The bank must submit evidence of its payment system capabilities, including descriptions of its card issuance infrastructure, integration with each mandated payment system, and governance arrangements. System design documents, contractual frameworks for outsourced elements, and evidence of compliance with technical specifications must be included.

2. The bank must also submit a third-party audit report issued by a CBI-approved cybersecurity or IT assurance firm. This report must include an assessment of the bank's payments system capabilities and completion of all required integrations. The report must be dated within 12 (twelve) months of submission and must include an attestation of independence.

3. If the bank outsources any component of its payment system operations, the Central Bank will require that the outsourcing agreement, business continuity plans related to the vendor, and risk management documentation ensuring the bank retains full control and regulatory compliance shall be submitted to the third-party IT assurance firm referenced below for validation and audit.

4. On an ongoing basis, the bank's compliance with payment systems specifications mandated by the Central Bank of Iraq (CBI) must be independently validated by a third-party cybersecurity or IT assurance firm that is pre-approved by the CBI. This firm shall conduct a formal audit and testing process to evaluate the bank's payment systems and integrations. The firm is required to produce a comprehensive assurance report, which must be submitted to both the bank's Board of Directors and the CBI. This report should include a detailed assessment of compliance with all relevant regulations and standards for payment systems, identification of any gaps relative to the regulatory requirements and industry best practices, and specific, actionable recommendations for enhancement.

5. The third-party assurance process shall be conducted on an annual basis and the assurance report shall be submitted to the board and the CBI within a period of a maximum of 60 days since the close of the financial year.

6. A remediation plan shall be developed by the relevant teams of the bank in collaboration with the third-party assurance company to ensure closing any existing compliance gap as well as actioning any recommendations for

enhancement. This remediation plan shall be shared with the bank's board of directors and the CBI within a period of maximum 180 (one hundred and eighty) days since the close of the financial year.

7. CBI to supervise the relevant teams within the bank to ensure actioning all elements of the submitted remediation plan. The CBI shall conduct onsite visits and meetings with the relevant teams, at the discretion of the CBI and throughout the year to ensure that all the required actions regarding the remediation plan have been taken.

Standard B8.2

A. Standard Summary:

1. All banks shall have, within the bank, capabilities that allow them to offer required functionalities – as defined by CBI – related to integration with payment systems via mechanisms specified by CBI

B. Assessment Guidelines:

1. The bank must be fully integrated with all national payment systems designated by the Central Bank of Iraq, including but not necessarily limited to Real-Time Gross Settlement (RTGS), Central Securities Depository (CSD), Automated Clearing House (ACH), Mobile Switch, ATM operator, and any other local or international clearing or settlement platforms required by regulation or licensing conditions.
2. Integration with all national payment systems must be conducted as per the technical mechanisms and protocols approved by CBI and must enable the bank to perform payment initiation, processing, and settlement securely and in accordance with regulatory timeframes.
3. The bank must ensure implementation and alignment with key international banking identification and messaging protocols, including:
    a. International Bank Account Number (IBAN): All account numbers must be IBAN-compatible
    b. Identifier Code (BIC/SWIFT Code): Required for all cross-border messaging and settlement
    c. ISO 20022: Must be adopted for all messaging formats relating to payment initiation, clearing, and settlement, in line with global best practices and CBI's modernization roadmap.
4. In line with international standards:
    a. Where the bank is the remitter of the payment, it should ensure that the content of the payer fields aligns to the information that it has verified through its AML processes
    b. Where the bank is the receiving payment service provider it should:
        i. ensure that the content of the payee fields aligns to the information that it has verified through its AML processes, and
        ii. ensure that the payer fields do not contain missing, incomplete or meaningless data.
5. The bank must maintain updated technical documentation evidencing successful integration with each relevant system, including system architecture diagrams, APIs used, interface specifications, fallback procedures, and audit trails for transactions.
6. The bank must maintain technical capabilities that enable effective tracking and documentation of all transaction details, including, but not limited to, the identity of the sender, the identity of the recipient, the nature of the transaction, and records of detailed information on all failed transactions, including the reason for their failure.

7. A dedicated officer must be assigned to oversee the bank's payment system infrastructure and compliance obligations. This function must ensure readiness, security, and ongoing monitoring of system performance, and report regularly to senior management and the Board.

8. Where any part of the payment system infrastructure is outsourced (e.g., card processing or network integration), the outsourcing arrangement must comply with CBI's outsourcing regulations. Contracts must guarantee data security, continuity of service, and the right of audit by CBI. However, the obligation to comply with CBI requirements remain the responsibility of the bank.

9. The bank must implement security controls and fraud prevention tools across all payment systems, including transaction monitoring, multi-factor authentication, data encryption, and access control measures. These must be reviewed and updated regularly to respond to emerging threats.

10. The bank must abide by all other CBI circulars, regulations and directives related to payment systems.

C. Assessment Process:

1. The bank must submit evidence of its payment system capabilities, including descriptions of its card issuance infrastructure, integration with each mandated payment system, and governance arrangements. System design documents, contractual frameworks for outsourced elements, and evidence of compliance with technical specifications must be included.

2. The bank must also submit a third-party audit report issued by a CBI-approved cybersecurity or IT assurance firm. This report must include an assessment of the bank's payments system capabilities and completion of all required integrations. The report must be dated within 12 (twelve) months of submission and must include an attestation of independence.

3. If the bank outsources any component of its payment system operations, the Central Bank will require submission of the outsourcing agreement, business continuity plans related to the vendor, and risk management documentation ensuring the bank retains full control and regulatory compliance.

4. On an ongoing basis, the bank's compliance with payment systems specifications mandated by the Central Bank of Iraq (CBI) must be independently validated by a third-party cybersecurity or IT assurance firm that is pre-approved by the CBI. This firm shall conduct a formal audit and testing process to evaluate the bank's payment systems and integrations. The firm is required to produce a comprehensive assurance report, which must be submitted to both the bank's Board of Directors and the CBI. This report should include a detailed assessment of compliance with all relevant regulations and standards for payment systems, identification of any gaps relative to the regulatory requirements and industry best practices, and specific, actionable recommendations for enhancement.

5. The third-party assurance process shall be conducted on an annual basis and the assurance report shall be submitted to the board and the CBI within a period of a maximum of 60 days since the close of the financial year.

6. A remediation plan shall be developed by the relevant teams of the bank in collaboration with the third-party assurance company to ensure closing any existing compliance gap as well as actioning any recommendations for enhancement. This remediation plan shall be shared with the bank's board of directors and the CBI within a period of maximum 180 (one hundred and eighty) days following the close of the financial year.

7. CBI to supervise the relevant teams within the bank to ensure actioning all elements of the submitted remediation plan. The CBI shall conduct onsite visits and meetings with the relevant teams, at the discretion of the CBI and throughout the year to ensure that all the required actions regarding the remediation plan have been taken.

B.9 Business & Operational Resilience

Standard B9.1

A. Standard Summary:

1. Each bank shall maintain fully documented and audited business continuity plans and disaster recovery plans, aligned with CBI specifications.

B. Assessment Guidelines:

1. The bank must maintain a Board-approved Business Continuity Plan (BCP), reviewed and updated annually, that includes business and critical services impact analysis, risk assessment, critical process mapping, and defined maximum tolerable downtime (MTD), in accordance with Clause 8.2 and 6.1.2 of ISO 22301.
2. The BCP must include procedures for activating alternate work arrangements, internal and external communication protocols, staffing continuity, crisis governance, scenario testing schedules and post-incident review.
3. The BCP must reflect Clause 8.4 of ISO 22301 on recovery strategy selection, Clause 9 on performance evaluation, and Clause 10 on continual improvement based on testing outcomes and incident learning.
4. The bank must also maintain a Board-approved Disaster Recovery Plan (DRP), reviewed and updated annually, that includes critical ICT infrastructure mapping, restoration sequencing, fallback strategies, and RTO/RPO alignment, as well as other emergency situations and disaster scenarios in accordance with Sections 6 and 7 of ISO/IEC 27031.
5. The bank must maintain at least one disaster recovery site located inside Iraq. The site must be capable of supporting the recovery of all critical ICT and banking services.
6. The disaster recovery site must include secure access controls with multi-factor authentication (MFA), digital access logging retained for a minimum of one year, and full-room surveillance with a minimum of three-month video retention.
7. The disaster recovery site must be at least 75 kilometers away from primary data sites.
8. The disaster recovery site must include the following specifications: (i) physical access control device to restrict access to authorized personnel; (ii) surveillance cameras covering the entire space and recordings kept at least the previous 3 months; (iii) raised flooring or smart racks with fire suppression pipes installed beneath; (iv) equipped with fire suppression system using FM200 gas; (v) back up fire extinguishers that are gas based; (vi) equipped with sensors to detect heat, smoke, humidity and water leakage; (vii) connection to a backup power source and (viii) equipped with primary and back up cooling systems. In general, it shall abide by all Tier 3 data center specifications issued by The Uptime Institute.
9. The DRP must include identification of critical systems and data, real-time or scheduled backup procedures, tiered system restoration priorities, fallback infrastructure arrangements (hot/warm/cold sites), and procedures for alternate data center failover and restoration.
10. The DRP must specify which systems and data are classified as critical for restoration. At a minimum, this must include: core banking systems, transaction records, customer data, real-time payment infrastructure, communication channels, and user authentication services as well as any systems or data that are related to activities critical for customers to perform.
11. The DRP must align with Section 8 of ISO/IEC 27031 on ongoing performance assessment, recovery maturity, and corrective measures.

12. In the event of a disruption affecting critical banking services, the BCP and DRP protocols must ensure that the bank activates a customer and regulatory communication protocol. This must include: (i) proactive public communication to customers through SMS, email, website, and social media, stating estimated recovery timelines and available alternative service channels (e.g., call centers, branches); and (ii) immediate notification to the Central Bank of Iraq (CBI) on the nature of the disruption, regular updates on root cause identification, recovery progress, interim mitigation actions, and estimated service restoration timelines.

13. In the event of a disruption affecting critical banking services, the bank must ensure resolving such disruption in a maximum period of 24 (twenty four) hours.

14. For the purposes of this guideline, a disruption shall be deemed sufficiently severe to trigger the protocols mentioned above if it meets any of the following criteria:

    a. Duration: The disruption to any critical service is expected to exceed 4 (four) hours or continue for one hour without identified cause

    b. Impact: The disruption affects more than 10% (ten percent) of the bank's customer base, or has potential to impact financial stability, customer trust, or regulatory compliance

    c. Regulatory Risk: The disruption may result in breach of regulatory obligations, delayed settlements, or inaccurate reporting to the Central Bank of Iraq (CBI)

    d. Cybersecurity or Operational Incident: The disruption is caused by a cyberattack, internal system compromise, or major data center failure

    Types of disruption could include, but are not limited to: Core banking system outage; Network or data center failure; Payment processing disruption; ATM or card services failure; Cybersecurity incidents (e.g., ransomware, DDoS attack); Third-party vendor failure impacting critical services; Natural disasters; Rocket strike, bombing, or armed conflict causing physical damage to banks' physical infrastructure.

15. The bank must conduct periodic testing of both BCP and DRP, including simulations and failover drills on an annual basis. Testing outcomes, gaps identified, and corrective actions taken must be formally documented and reported to the Board.

16. A senior executive, such as the Chief Risk Officer, must be designated to oversee the development, testing, implementation, and governance of BCP and DRP frameworks, with regular reporting to the Board.

17. Internal Audit must review the BCP and DRP frameworks annually and submit findings, including any gaps or risks, to the Audit Committee and Board of Directors.

18. Where fallback infrastructure is provided by a third party, the outsourcing must comply with CBI outsourcing guidelines, and the bank must retain full responsibility for operational continuity and regulatory compliance.

C. Assessment Process:

1. The bank must submit the most recent Board-approved versions of the BCP and DRP, documented change logs for the past two years, results of testing exercises, and records of corrective actions taken.

2. Board resolutions or meeting minutes confirming formal approval of the BCP and DRP must be included in the submission.

3. An annual third-party audit of the BCP and DRP must be conducted by a CBI-approved audit or cybersecurity assurance firm. The audit must include evaluation of governance, infrastructure readiness, alignment with ISO 22301 and ISO/IEC 27031, and testing effectiveness.

4. The audit report must include auditor credentials, formal opinion of compliance, detailed assessment findings, remediation recommendations, and a statement of auditor independence.

5. The audit report must be submitted to the Board and the CBI within a maximum of 60 days from the end of the financial year.
6. Where material gaps or risks are identified, the bank must submit a remediation plan developed in coordination with the audit firm in a period no longer than 180 days from the end of the financial year, with timelines and ownership clearly assigned.
7. The CBI may conduct site visits, request demonstrations of failover systems, interview relevant executives, or inspect documentation to validate the operational readiness of the DR site and continuity framework.
8. The CBI shall monitor implementation of remediation plans and may issue additional directives, require re-testing, or enforce supervisory actions to ensure compliance with all continuity and recovery standards.

B.10 Deposit Protection Scheme

Standard B10.1

A. Standard Summary:

1. Each bank shall maintain an active subscription and pay all associated fees to the Iraqi Company for Deposit Insurance according to the defined schedule.

B. Assessment Guidelines:

1. Banks must be formally enrolled in the recognized Deposit Protection Scheme (DPS) and maintain up-to-date certification of membership.
2. Banks must maintain accurate classification of deposits covered by the scheme, in line with DPS rules.
3. Banks must clearly inform customers at account opening and via branch/online notices that their deposits are protected by DPS. Disclosure must specify the maximum coverage limit per depositor, in line with DPS regulations.
4. Banks must also actively promote and advertise the deposit protection scheme to customers.
5. Banks must maintain up-to-date depositor records (name, balance, contact, product type) in a defined format.
6. Banks must share depositor's customer data on a regular basis with the Iraqi Company for Deposit Insurance and as per the regulations of the company.
7. Banks must pay DPS contributions as per defined rules and submit proof of payment within the defined window to the CBI.

C. Assessment Process:

1. Assessment against this standard shall be conducted by CBI.
2. The CBI shall confirm with the Iraqi Deposit Insurance company on the compliance of different banks with regards to:
    a. Payment of all required DPS premiums
    b. The ability of banks to provide full and accurate depositor data when required
    c. The effective exchange of required data and information between different banks and the Iraqi Deposit Insurance company
3. The CBI shall review the above with the Iraqi Deposit Insurance company on an annual basis.

4. The CBI will conduct branch and website checks to ensure clear and visible communication and promotion of DPS. It will also review account opening forms and customer agreements to confirm inclusion of coverage details and maximum protection limits.

B.11 Credit Bureau

Standard B11.1

A. Standard Summary:

1. Each bank shall regularly provide all credit-related customer data to CBI's centralized credit bureau, as per CBI requirements. As provided by Article 51, Paragraph 1, Sub-paragraph (e) of the 2004 Banking Law, the confidentiality requirements of Articles 49 and 50 of the 2004 Banking Law do not apply when providing customer data to the aforementioned credit bureau and in compliance with the provisions of Circular No. (432/4/9) issued in 2017, which includes the required authorization signed by the bank's customers, for the purpose of protecting both the customer and the bank.

B. Assessment Guidelines:

1. Banks must be formally registered as data providers with the national credit bureau and maintain an up-to-date data-sharing agreement. Banks must report all forms of credit exposure across all product types and customer segments, including but not limited to: personal loans, credit cards, overdrafts, SME and corporate loans, leasing arrangements, letters of credit (LCs), letters of guarantee (LGs), mortgages, and other off-balance sheet exposures such as guarantees and credit commitments. Both performing and non-performing accounts must be reported.
2. Banks must submit complete data sets for each borrower and facility, the data points provided shall include national ID or company registration, loan account number, product type, disbursed amount, outstanding balance, credit limit, collateral details, repayment schedule, overdue status, restructuring flags, and write-offs. Data must be submitted in the format required by the bureau. Additionally, banks must provide historical data covering at least the past 36 (thirty six) months for all active credit facilities, and for closed accounts within the last 24 (twenty four) months.
3. Data sharing shall be done through the ICI system of the CBI and the bank shall ensure full integration between its core banking systems and the ICI system to enable CBI to access all required data points mentioned above.
4. Additionally, banks need to share all relevant data with national credit bureau on a monthly basis and in the first 10 (ten) days of the month as a second layer of checking in addition to the existing integration.
5. A designated Data Quality Officer must oversee compliance and coordinate with the credit bureau to resolve file rejections or discrepancies.
6. All banks must obtain the consent of their customers to share relevant data with national credit bureau.

C. Assessment Process:

1. The CBI will confirm the bank's registration status and system integration status with the credit bureau and examine the scope of credit facilities being reported.
2. The bank's effective integration with the ICI system and its ability to provide the required accurate data must be independently validated by a third-party cybersecurity or IT assurance firm that is pre-approved by the CBI.
3. This third-party assurance company shall conduct a formalized audit and testing process to evaluate the bank's integration with the ICI system as well as the accessibility to accurate data as required.

4. This audit process shall be conducted once annually.

5. The CBI will conduct unannounced spot audits on selected banks. These audits shall evaluate both the completeness and accuracy of the credit data being submitted, and the robustness of internal controls and procedures used to generate such data.

4. Financial Metrics

C.1 Capital & Composition

Standard C1.1

A. Standard Summary:

1. Each bank shall maintain a minimum capital as paid-up capital and on an ongoing basis, that is not less than 400,000,000,000 (four hundred billion) Iraqi dinars or such higher amount as may be established by CBI, in accordance with Article 14, Paragraph 1 of the 2004 Banking Law.
2. As provided by Article 16, Paragraph 1 of the 2004 Banking Law, each bank shall at all times maintain its minimum required capital in Iraq, of which not less than one-half of such capital shall consist of core capital (also referred to as "Tier 1 capital").

B. Assessment Guidelines:

1. A bank's capital shall consist of Tier 1 capital components and Tier 2 capital components with Tier 1 capital components representing at least 50% (fifty percent) of the bank's capital.
2. As per the definition detailed in Basel III, Tier 1 capital components also referred to as core capital components shall include (i) common equity paid up capital which shall consist of capital raised through the issuance of ordinary shares to shareholders, such capital should be fully paid and not subject to any repayment obligations; (ii) retained earnings which refer to retained profits that the bank has earned over time but not distributed as dividends, instead they are reinvested in the bank or kept as reserves; (iii) eligible other comprehensive income including unrealized gains or losses that are not included in net profit or loss but are recorded in equity, for example revaluation gains/ losses on financial assets; (iv) eligible non-cumulative preferred shares that are perpetual with no specific maturity date, allows for discretionary cancellation of dividends, be able to absorb losses via write-down or equity conversion and be subordinated to depositors and other creditors.
3. As per the definition detailed in Basel III, Tier 2 capital components shall include (i) subordinated debt instruments referring to long term debts that rank below other senior obligations in case of bankruptcy or liquidation, these debt instruments must have a minimum maturity of at least 5 years, must not include incentives to redeem, must be unsecured and subordinated and cannot contain clauses that allow for acceleration of repayment; (ii) general loan-loss reserves which refers to reserves set aside by the bank to cover future unidentified loan losses, they can be included in Tier 2 capital of up to 1.25% of the bank's risk-weighted assets value (RWAs); (iii) revaluation reserves from fixed assets or foreign exchange which refer to unrealized gains that arise from periodic revaluation of assets such as land, property or FX reserves, a maximum of 45% of these gains can be accounted as Tier 2 capital.
4. Banks that have not yet met CBI's current minimum paid up capital requirement of 400,000,000,000 (four hundred billion) Iraqi dinars should inject the required additional amount of common equity paid-up capital exclusively through cash contributions, any non-cash considerations including but not limited to fixed assets, property, or any similar forms of contribution shall not be recognized. All cash contributions for the purpose of meeting the minimum paid-up capital requirement must be deposited as reserves within the banks dedicated reserve account at CBI.
5. Banks that have not yet met CBI's current minimum paid up capital requirement shall immediately notify CBI of its current capital position and the existing gap.
6. Other legitimate assets equivalent to cash as per the Iraqi corporate law shall also be accepted for paid up capital (e.g. retained earnings).

C. Assessment Process:

1. The capital evaluation process shall be conducted by a third-party independent audit company from the list of third-party independent audit companies approved by the CBI, for every existing bank in Iraq.
2. The third-party independent audit company shall be appointed by the bank under the supervision of CBI.
3. The evaluation process shall assess:
    a. The eligibility of Tier 1 and Tier 2 capital components
    b. The composition and structure of capital (Tier 1 and Tier 2 capital components)
    c. The valuation of assets and recognition of value changes in capital
4. Banks are required to submit a detailed breakdown of all their capital composition and components according to the above, this shall be in the form of a detailed report developed by a third-party independent audit company from the list of third-party independent audit companies approved by the CBI.
5. The report developed by the third-party independent audit company will be reviewed and approved by the relevant teams and departments within CBI. CBI can request any additional detailing or clarifications of the report provided from the bank, these additional details and clarifications shall be provided by the bank and reviewed by the third-party independent audit company they are contracted with prior to submission to the CBI.
6. The reporting template should be provided by CBI in line with P3 reports of Basel III framework.
7. In terms of cadence, banks will be required to provide this detailed report on capital composition and components at the end of each financial year.
8. The CBI reserves the right to conduct spot audits on a bank's capital position at any point during the financial year. This may include requesting an independently audited report detailing the capital position, its composition, and components, provided that the CBI gives the bank a minimum notice period of three months.

C.2 Capital Adequacy

Standard C2.1

A. Standard Summary:

1. As provided by Article 16, Paragraph 1 of the 2004 Banking Law, each bank shall at all times maintain capital of not less than the equivalent of 12.5% (twelve and one-half percent) of the total value of its assets determined on a risk-adjusted basis (also known as risk-weighted assets).

B. Assessment Guidelines:

1. The calculation of Risk-Weighted Assets must follow standardized risk weights for each asset class as issued by the CBI in CBI's relevant templates. The bank's capital structure must meet the eligibility requirements for Tier 1 and Tier 2 capital as defined by CBI standards, including that at least 50% (fifty percent) of total capital be composed of Tier 1 capital.
2. All banks shall be fully responsible to monitor their own capital adequacy ratio and ensure maintaining it on an ongoing basis.
3. Any deficiencies in the Capital Adequacy Ratio shall be immediately reported to the CBI, accompanied by a capital restoration plan which must include: (i) Amount of capital to be raised; (ii) Mode and timeline of capital injection and (iii) Impact on shareholding and governance.

4. For the purposes of this standard and as per Basel III, the Capital Adequacy Ratio shall be defined as a measure of a bank's capital, expressed as a percentage of its risk-weighted assets (RWA), the bank must maintain this ratio at a minimum of 12.5% as mentioned above. CBI reserves the right to require a higher ratio than 12.5% for specific banks, as it deems necessary.

5. For the purposes of this standard and as per Basel III, risk-weighted assets (RWA) also referred to as assets determined on a risk adjusted basis shall be defined as the total of all on- and off-balance sheet exposures, weighted according to their associated credit, market, and operational risks, using specified risk weights. The exact weighting of each asset will follow the issued CBI guidelines on this matter.

6. In case a bank falls short of the required Capital Adequacy Ratio while it remains above the minimum capital threshold, it shall be considered deficient and requires an immediate capital restoration plan.

C. Assessment Process:

1. Third-party specialist firms from a list of CBI-approved firms will prepare a capital adequacy report that details:
    a. Total capital (broken down into Tier 1 and Tier 2) in accordance with Pillar 3 reporting requirements of Basel III framework
    b. Composition of RWAs by asset class
    c. Capital Adequacy Ratio as of each quarter-end.
2. The capital adequacy report must be submitted to the CBI annually at the end of each financial year.
3. In case of any new capital instruments issued by the bank, those new capital instruments must be reviewed and approved by the CBI prior to recognition in the capital base. Banks must submit detailed term sheets and legal documentation for any new capital instruments audited by a third-party specialist firm appointed by the bank, the term sheets and legal documentation shall include subordinated debt, preference shares, etc. The CBI shall review and approve these new capital instruments accordingly.

C.3 Liquidity Ratio

Standard C3.1

A. Standard Summary:

1. Banks shall maintain adequate liquidity, as provided in Article 26, Paragraph 2 of the 2004 Banking Law. Specifically, banks must maintain a Liquidity Coverage Ratio of at least 100%.

B. Assessment Guidelines:

1. The Liquidity Coverage Ratio (LCR) shall be calculated as the ratio of High-Quality Liquid Assets (HQLA) to total net cash outflows over a 30-calendar-day period.
2. For calculating the LCR and as per the definition in Basel III, High-Quality Liquid Assets shall be limited to assets that can be readily and immediately converted into cash in private markets with little or no loss of value. These assets shall include Level 1 assets that are defined in the circulars issued by the CBI and shall include cash, central bank reserves (excluding the mandatory reserve), and financial balances. Those level 1 assets shall cover at least 45% (forty-five percent) of the existing High Quality Liquid Assets. Level 2 assets are divided into two categories: Level 2A and Level 2B:
    a. Level 2A: Those assets include instruments identified in the relevant circulars issued by CBI such as high credit rating debt instruments. They should account for 40% of High-Quality Liquid Assets.

b. Level 2B: Those assets include instruments identified in the relevant circulars issued by CBI such as debt instruments with lower credit rating. They are allowed to account for up to 15% of High Quality Liquid Assets.

3. In line with Basel III, total net cash outflows shall be defined as the total expected cash outflows (e.g. expected retail deposit withdrawals, repayments of maturing bonds) minus the total expected cash inflows (e.g. maturing loans, operational inflows, interest payments) during the 30-day period, with the inflows being capped at a maximum of 75% (seventy-five percent) of the outflows.

C. Assessment Process:

1. Banks shall calculate the LCR on a monthly basis and report the results to the Central Bank of Iraq on a quarterly basis. Reports shall be prepared in accordance with templates and data requirements issued by the CBI and shall be accompanied by supporting documentation, including internal audit verification.

2. All banks must maintain internal systems capable of monitoring and projecting their liquidity positions. In the event of any of the following: (i) the Liquidity Coverage Ratio (LCR) falls below 100% (one hundred percent), (ii) the LCR declines by 10% (ten percent) or more compared to its level at the previous quarter-end, or (iii) any change in LCR that materially affects the bank's valuation—the bank shall be required to immediately report such developments to the CBI. All liquidity reports must be reviewed and approved by the bank's internal compliance or risk management function and formally signed off by senior management and the Board of Directors prior to submission to the CBI.

3. In the event a bank falls below the minimum LCR, it shall immediately notify the Central Bank of Iraq and submit a Liquidity Restoration Plan. This plan shall detail the causes of the breach, the corrective actions to be taken, the timeline for remediation, and the impact on the bank's financial position and governance.

4. The assessment and monitoring of liquidity ratios shall generally be conducted in accordance with the details set out in CBI Circular No. 9/6/357 issued in 2018 and other relevant circulars.

Standard C3.2

A. Standard Summary:

1. Banks shall maintain adequate liquidity, as provided in Article 26, Paragraph 2 of the 2004 Banking Law. Specifically, banks must maintain a Net Stable Funding Ratio of at least 100%.

B. Assessment Guideline:

1. Each licensed bank shall be required to maintain a Net Stable Funding Ratio (NSFR) of not less than 100% (one hundred percent) on an ongoing basis. The NSFR shall be calculated as the ratio of Available Stable Funding (ASF) to Required Stable Funding (RSF).

2. In line with Basel III, available Stable Funding shall refer to the portion of capital and liabilities expected to be reliable over a one-year time horizon, including Tier 1 and Tier 2 capital components, retail and small business customer deposits, and longer-term wholesale funding instruments.

3. For the purposes of this standard, longer-term wholesale funding instruments shall be defined as funding instruments and liabilities provided by institutional investors, large corporate clients, or other professional counterparties with maturities greater than one year. These instruments are considered to provide more stable sources of funding for a bank's long-term assets.

4. As per Basel III requirements, the required Stable Funding shall refer to the portion of a bank's assets and off-balance sheet exposures that require stable funding, with each category assigned a regulatory RSF factor based on its liquidity characteristics and residual maturity. Higher-risk or less-liquid assets shall attract higher RSF factors.

C. Assessment Process:

1. The NSFR shall be calculated and reported quarterly. Reports shall be prepared in accordance with templates and data requirements issued by the CBI and shall be accompanied by supporting documentation, including internal audit verification.

2. All banks must maintain internal systems capable of monitoring and projecting their liquidity positions. In the event of any of the following: (i) the Net Stable Funding Ratio (NSFR) falls below 100% (one hundred percent), (ii) the NSFR declines by 10% (ten percent) or more compared to its level at the previous quarter-end, or (iii) any change in NSFR that materially affects the bank's valuation—the bank shall be required to immediately report such developments to the CBI. All liquidity reports must be reviewed and approved by the bank's internal compliance or risk management function and formally signed off by senior management and the Board of Directors prior to submission to the CBI.

3. In the event a bank falls below the minimum NSFR, it shall immediately notify the Central Bank of Iraq and submit a Liquidity Restoration Plan. This plan shall detail the causes of the breach, the corrective actions to be taken, the timeline for remediation, and the impact on the bank's financial position and governance.

4. The assessment and monitoring of liquidity ratios shall generally be conducted in accordance with the details set out in CBI Circular No. 9/6/357 issued in 2018 and other relevant circulars.

C.4 Scenario Stress Testing

Standard C4.1

A. Standard Summary:

1. All banks shall achieve a positive outcome to regulatory scenario stress testing. Details of this process, including the assumptions of the scenarios to be used, will be defined by CBI and communicated to all banks in due course.

B. Assessment Guidelines:

1. All licensed banks shall participate in regulatory scenario stress testing exercises conducted by the Central Bank of Iraq (CBI) in order to assess the resilience of their capital, liquidity, profitability, and asset quality under adverse but plausible economic and financial conditions.

2. The Central Bank of Iraq shall define and disseminate on an annual basis a set of standardized macro-financial scenarios to be used in each round of stress testing. These scenarios shall be designed to simulate sudden or prolonged economic distress, external shocks, or deterioration in credit and market conditions.

3. The standardized stress testing scenarios shall include one or more of the following simulations:

    a. **Currency Devaluation** involving an assumed depreciation of the Iraqi dinar against the US dollar within one quarter, with sustained depreciation over the following two quarters

    b. **Inflation Shock** involving an assumed increase in headline inflation from baseline to a specific % per annum, driven by food, energy, and import prices, sustained over a 12-month period

    c. **Recession and Credit Deterioration** involving an assumed contraction in real GDP by a certain amount year-on-year, a significant rise in unemployment by a certain amount, and a certain increase in non-performing loans across all asset classes

d. **Liquidity Crunch** involving a sudden significant withdrawal of demand deposits over a 10-day period, in conjunction with a temporary freeze in interbank lending and loss of access to international correspondent banking lines

e. **Real estate crisis** negatively impacting office and/or private real estate prices

f. Parameters of the above scenarios to be defined and provided by the CBI on an annual basis

4. Each bank shall apply the above scenarios to its own portfolio and operations using internal financial models, in accordance with technical instructions to be issued by the CBI, and shall simulate the effects of these shocks over a three-year projection horizon (baseline, year 1 and year 2) in line with all relevant circulars issued by CBI.

C. Assessment Process:

1. For each scenario, banks shall be required to submit a quantitative impact report presenting the evolution of the following outcome metrics at quarterly intervals throughout the two-year period:

   a. Capital Adequacy Ratio (CAR)

   b. Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR)

   c. Return on Assets (ROA) and Return on Equity (ROE)

   d. Net Operating Profit

   e. Exchange Rate Exposure (FX gap)

   f. Total Losses Absorbed (e.g. NPL and provisions)

2. The impact report shall be submitted in both (i) standardized templates issued by the CBI and (ii) a narrative memo of not less than 5 (five) pages summarizing key assumptions, methodology, key sensitivities, management response, and lessons learned.

3. The deadline for submission of the completed stress test outputs shall be no later than 30 (thirty) calendar days from the date the CBI issuing the official stress testing scenarios, unless otherwise specified in writing by the Central Bank.

4. The Central Bank of Iraq shall review each bank's submission to evaluate methodological robustness, appropriateness of assumptions, completeness of reporting, and severity of financial impact. Banks may be required to revise or clarify submissions if deficiencies are found.

5. Any bank whose results indicate a breach or projected breach of minimum regulatory thresholds, including capital adequacy, liquidity, or solvency, shall be required to submit a remedial capital or liquidity restoration plan.

6. All banks shall maintain internal stress testing capabilities, including staff, governance, data systems, and documented methodologies that enable timely simulation and reporting of results upon demand.

7. The CBI shall conduct scenario stress tests at least once annually and at a maximum of 30 (thirty) days after the end of the year.

5. Risk and Regulatory Compliance

D.1 Related Parties and Conflicts of Interest

Standard D1.1

A. Standard Summary:

1. A bank shall not extend credit to a related party if the credit and its financial terms and conditions have not been approved with super-majority approval by the Board of Directors. This requirement is in addition to the requirements of Article 31, Paragraph 1 of the 2004 Banking Law.
2. A bank shall not extend credit to any single entity (including to related parties) if the extension of credit would cause the aggregate amount of credits disbursed to that entity and outstanding to exceed the maximum allowable credit facilities (loans, guarantees, or other financial commitments) as a percentage of the bank's capital base (unimpaired capital and reserves), currently set at 10% (ten percent), with the possibility to increase to 15% after obtaining CBI approval.
3. A bank shall report all related party exposure – including all credits and deposits – to CBI, in addition to internal reporting requirements as outlined in Article 31, Paragraph 2 of the 2004 Banking Law.
4. Banks should have internal policies regarding conflicts of interest that include, but are not necessarily limited to, the following:
    a. Market abuse controls and controls for the handling of confidential / sensitive information (e.g., information barriers);
    b. Conduct rules;
    c. Personal account dealing approval and notification arrangements

B. Assessment Guidelines:

1. All banks shall ensure that both on balance, off-balance sheet exposures and deposits to related parties are comprehensively identified, measured, and reported. For the purposes of this standard, on-balance sheet exposures are loans, advances, investments, and other assets directly recorded in the bank's books whereas off-balance sheet exposures are guarantees, letters of credit, and any other contingent liabilities that may give rise to credit risk.
2. "Related party" shall have the meaning assigned under Article 1 of the 2004 Banking Law and in addition to what is detailed below:
    a. Any administrator of the bank, including Board members, authorized managers, audit committee members, or designated foreign branch managers.
    b. Persons related to administrators by blood, marriage or kinship up to the second degree, including adopted or foster children.
    c. Any individual or entity holding a qualifying holding in the bank.
    d. Any entity in which an administrator or qualifying holder has at least a 10% (ten percent) stake.
    e. Any non-consolidated entity in which the bank holds a qualifying holding.
    f. Senior executives of the bank or of any of its subsidiaries or affiliates and their relatives.
    g. Board members and senior executives of substantial shareholders of the bank.

h. Companies in which a board member or senior executive of the bank or their relatives has a financial interest, acts as a guarantor, or exerts influence over decisions, including through informal means such as providing advice or guidance.

i. And the external auditors of the bank.

j. Friends and people from within the circle of influence/ maintaining an indirect relationship.

3. All related-party transactions must be approved by a super-majority of the Bank's Board of Directors and must remain within prudential exposure limits. Such transactions must be treated as high-risk exposures and be subject to enhanced transparency and regulatory scrutiny. A "super-majority approval" shall mean an affirmative vote by at least two-thirds of the total members of the Board of Directors eligible to vote. The precise threshold shall be defined in the bank's charter and shall not be less stringent than two-thirds. Documentation of this approval, including meeting minutes, credit evaluation reports, voting records, and conflict of interest disclosures, shall be retained and made available for CBI inspection.

4. The "eligible capital base" used to calculate exposure limits shall be the bank's Tier 1 capital as defined above under the requirement for Standard C1.1.

5. If a bank's exposure to related parties exceeds the regulatory limit, it may increase its paid-up capital to remain compliant. Any capital injection must be in the form of new common equity, verifiable via bank statements and shareholder registers, and reflected in audited financial statements. The increase shall not be used to justify prior non-compliant lending and shall only take effect upon CBI approval.

6. Exceeding the maximum allowable credit facilities for related parties could be considered only in the presence of sovereign government guarantees.

C. Assessment Process:

1. A bank is required to have adequate systems and controls in place to identify, measure, monitor, and report related-party transactions of the bank on a timely basis and ensure related party exposures are reviewed at least quarterly.

2. Banks shall report all related party exposures to the CBI on a quarterly basis. The report shall contain: (i) names and relationships of all related parties; (ii) nature, amount, and terms of all credit facilities; (iii) documentation of super-majority Board approvals; (iv) calculation of the exposure as a percentage of the capital base; and (v) any corrective actions taken to reduce excess exposure or enhance governance.

3. An independent third-party assessment shall be conducted annually to verify the bank's compliance with related party exposure limits. The third-party specialist firm must be selected from a list of CBI-approved assessors and shall review: (i) identification and classification of related parties; (ii) exposure calculations and aggregation; (iii) documentation of Board approvals; and (iv) adherence to the 10% (ten percent) or 15% (fifteen percent) thresholds based on verified capital base.

4. In order to increase the threshold of related party transactions to 15% (fifteen percent) of the capital base, the following steps must be completed: (i) submission of the bank's request with detailed justification and supporting financials; (ii) independent review confirming that the deposit terms are no more favorable than those offered to third-party customers; (iii) demonstration of strong internal governance, risk monitoring, and conflict-of-interest safeguards; and (iv) Board resolution with super-majority voting records explicitly approving the exception.

5. Banks shall provide evidence of the existence of internal policies regarding conflicts of interest that include, at a minimum, the elements mentioned in the Standard Summary.

D.2 AML / CFT / Sanctions

Standard D2.1

A. Standard Summary:

1. Each bank shall have policies, processes, controls, and employ systematic tools related to anti-money laundering (AML) and combating the financing of terrorism (CFT), and sanctions practices (collectively "AML/CFT programs"), aligned with CBI requirements. The alignment of bank's policies with CBI requirements and its associated compliance will be tested by a CBI-approved third-party audit firm.

B. Assessment Guidelines:

1. Banks shall structure its AML/CFT/sanctions framework around three core elements: (a) Governance and Organization, (b) Process, and (c) Enablers. These elements must function cohesively, reflect the bank's risk profile, and be reviewed periodically to align with both global standards and regulatory expectations as defined by CBI's circular "*Controls on combating money laundering and terrorist financing and preventing the proliferation of armaments*" published on 8th January 2025.

    a. **Governance and Organization:** Banks must maintain a governance framework that ensures effective oversight, clear accountability, and strategic alignment of the AML/CFT program with regulatory expectations and institutional risk appetite.

        i. **Management Committees**: Banks shall establish formal governance structures including a dedicated AML/CFT oversight committee, chaired or monitored by senior management, with defined roles for escalation, reporting, and decision-making. The committee shall convene at a defined frequency, with its charter and meeting minutes maintained and subject to review.

        ii. **Program Monitoring and Reporting**: Banks shall implement structured monitoring and reporting protocols that provide senior management and the Board of Directors with periodic insights into AML/CFT risks, compliance gaps, escalation logs, and mitigation actions. Reports must include key risk indicators, trends in suspicious activity and transaction reports (SARs/ STRs), and outcomes of regulatory inspections or audits.

        iii. **Program Organization**: Each bank shall appoint a Head of Compliance and a Money Laundering Reporting Officer (MLRO) who operates with sufficient independence and authority, reporting directly to their respective Board committee (or committee chair). The compliance function must be adequately resourced in terms of staff, expertise, and technological capabilities.

        iv. **Policies and Standards**: Banks shall issue formal AML/CFT and sanctions policies, approved by the Board, aligned with CBI directives and FATF guidelines and the Anti Money Laundering Office as well as all related international standards. These policies must be updated periodically and integrated into operational manuals and business unit procedures.

    b. **Process:** The AML/CFT compliance program shall encompass risk-based procedures and controls that reflect the bank's customer base, product offerings, and delivery channels.

        i. **Client Risk Rating (CRR)**: Banks shall adopt a structured methodology to assess the money laundering, terrorist financing, and sanctions risk of each customer. This risk rating must incorporate factors including geography, product type, transaction behavior, and shareholding structure, and shall determine the level of monitoring and due diligence applied.

        ii. **Know Your Customer (KYC)**: Banks shall implement robust KYC processes encompassing Customer Due Diligence (CDD), Identity Verification (ID&V), and identification of Politically Exposed Persons (PEPs).

Onboarding must follow a risk-based approach, with enhanced procedures applied to higher-risk clients. Digital KYC onboarding is permitted for low-risk clients upon CBI approval.

iii. **Enhanced Due Diligence (EDD)**: Banks must apply EDD measures where heightened risk is identified, including for PEPs, high-value clients, cross-border transactions, and complex shareholding structures. EDD measures shall include source of funds verification, heightened transaction scrutiny, and periodic re-assessments.

iv. **AML Investigation**: Banks shall define internal protocols for investigating alerts generated from transaction monitoring or customer behavior. All financial crime investigations must be documented with clear audit trails, performed and/or overseen by suitably qualified and experienced staff, commenced and concluded in a timely manner commensurate to the potential risk, and concluded by determining whether the matter is reportable.

v. **Transaction Monitoring**: Banks shall deploy automated and risk-sensitive transaction monitoring systems calibrated to detect patterns of suspicious activity. The system must support dynamic rule setting, generate alerts, and facilitate investigation workflows, with periodic calibration and quality assurance controls.

vi. **Sanctions Screening**: Banks shall implement real-time and batch sanctions screening tools covering customers, counterparties, and transactions. Sanctions screening must follow documented procedures and ensure resolution timelines comply with CBI and international sanctions obligations. Escalations must be conducted in line with the bank's defined protocol.

c. **Enablers:** The effectiveness of the AML/CFT framework is contingent on the quality of supporting infrastructure, particularly with respect to data integrity and system capabilities.

i. **Data**: Banks must have processes for ensuring data quality and that data is current, accurate, and accessible for all internal functions and regulatory reporting for all AML-relevant processes. Data must be accurate, complete, up-to-date, and accessible for all internal functions and regulatory reporting. Recordkeeping practices must ensure traceability, including SARs, CDD files, and audit records, retained in line with CBI and FATF retention periods for up to 7 years.

ii. **Systems**: Banks shall deploy integrated systems that support KYC, transaction monitoring, sanctions screening, and reporting functions. These systems must be scalable, resilient, and capable of interfacing with regulatory bodies. It should also be integrated with the core banking systems for each bank. Audit logs, user access controls, and system updates must be clearly documented and subject to periodic review.

C. Assessment Process:

1. A CBI-approved third-party specialist firm shall conduct an independent review of the bank's AML/CFT/sanctions framework at a regular frequency. This review shall evaluate the existence and effectiveness of all core components listed in Standard D2.1, paragraph B.1 to ensure full compliance with CBI regulations.

a. **Governance and Organization:** The third-party specialist firm shall review governance documentation including committee structures, MLRO and Head of Compliance appointment letters, policy approval records, and internal reporting protocols. Evidence shall be assessed for comprehensiveness, independence, and alignment with CBI's regulatory architecture.

b. **Process**: The third-party specialist firm shall examine a representative sample of customer files across all risk levels to validate risk classifications, KYC completeness, EDD application, and client monitoring outcomes. Transaction monitoring systems shall be tested for rule logic, alert generation, investigator workflows, and feedback loops. Suspicious transaction handling and sanctions match reviews shall be examined for timeliness, completeness, and escalation documentation.

c. **Enablers**: The third-party specialist firm shall evaluate system capabilities and configuration files, verifying alert thresholds, user access permissions, audit trail integrity, and integration across the KYC, monitoring, and sanctions modules. Data governance controls shall be tested for completeness, backup procedures, and compliance with statutory retention periods. Furthermore, the audit shall evaluate whether the data used to detect and report suspicious activity is traceable, accurate, and fit for purpose.

2. The outcome of the audit shall be documented in a detailed report, specifying areas of full compliance, partial compliance, and non-compliance, with clear timelines and action plans for remediation. Banks shall be required to implement corrective measures as per CBI-mandated timelines, subject to follow-up inspections or audits as necessary.

D.3 Transparency of Reporting / Audit

Standard D3.1

A. Standard Summary:

1. A bank's financial statements shall be audited according to international accounting standards (e.g. IFRS9 accounting standards) by at least two independent auditors. At least one of those auditors must be from the list approved by the Central Bank of Iraq. This review shall also cover the creditworthiness of the bank. All this shall be in accordance with previous CBI circulars and relevant regulations.

2. The independent auditors shall ensure that the bank properly reassessed all its financial assets (e.g. loans, investments) as per the relevant international standards (e.g., IFRS9, IFRS 13)

3. This requirement is in addition to auditing requirements for banks as detailed in Articles 46 and 47 of the 2004 Banking Law, and is not intended to replace or supersede any requirements specified therein.

B. Assessment Guidelines:

1. The selected firm must meet all eligibility criteria set by the CBI, including professional qualifications, sector-specific audit experience, and absence of conflicts of interest. The bank shall obtain prior written confirmation from the CBI on the firm's approved status before engagement.

2. Each audit shall evaluate the bank's financial position, asset quality, provisioning practices, off-balance sheet exposures, adherence to regulatory limits, and adequacy of disclosures, including related-party transactions.

3. The audit process shall also assess the reliability of internal financial controls and verify the accuracy of liquidity, capital adequacy, and profitability figures of the bank.

C. Assessment Process:

1. The third-party auditor shall:

   a. Conduct, according to global best practices, a full audit of financial statements, including:

      i. Confirmation of key balance sheet items (e.g., loans, deposits, investments, etc.)

      ii. Review of income statement components (e.g., interest income, fees)

      iii. Assess disclosures (e.g., credit risk, liquidity risk, operational risk)

   b. Verify data integrity through check of whether financial and operational transactions are accurately captured and correctly classified within the bank's core banking system, using global best practices

2. Any material weaknesses identified by auditors shall be formally addressed by bank management through a corrective action plan, which must be submitted to the CBI with specific implementation deadlines

3. The audit shall take place annually and the audit findings shall be formally reported to the Board of Directors and to the CBI within a maximum of 120 calendar days following the close of the financial year

D.4 Internal Controls

Standard D4.1

A. Standard Summary:

1. Each bank must implement internal controls that establish a relationship between the bank's business units (first line of defense), its compliance and risk functions (second line of defense), and its internal audit function (third line of defense) that comprise the "three lines of defense" model.

B. Assessment Guidelines:

1. Each of the lines of defense shall have clear reporting lines and responsibilities, namely:

    a. The business units shall report directly to senior management. Business units undertake risks within assigned limits of risk exposure and are responsible and accountable for identifying, assessing and controlling the risks of their business, with documented policies and timely escalation to senior management.

    b. The compliance and risk management functions shall report directly to their respective Board committee (or committee chair), with a secondary reporting relationship ("dotted line") to the CEO, CFO, or CRO. These functions shall ensure ongoing monitoring of regulatory obligations, operational risks, and emerging threats, with documented policies and timely escalation to senior management and/or the Board.

    c. The internal audit function of the bank shall report directly to the Board Audit Committee and operate independently from all business and control units. Its work shall be based on a risk-based audit plan approved by the Board.

2. The assessment of the internal control systems shall focus primarily on relevant elements of the organizational structure, risk-related roles & responsibilities, risk identification processes, control execution (i.e., the day-to-day operational management of risks), and escalation mechanisms.

3. Each bank shall maintain documentation of its internal control policies, procedures, roles and responsibilities, and reports from its control functions, which must be made available to the CBI upon request.

4. The reports and documents related to the internal control system must be up to date at all times and shall be provided to the CBI immediately whenever requested.

C. Assessment Process:

1. The effectiveness of the internal control system including the autonomy and effectiveness of the audit function, the compliance function and the risk management function shall be reviewed at least once annually by a third-party specialist firm from the list of firms approved by the CBI.

2. The audit report shall be provided to the CBI by maximum 120 (one hundred and twenty) days after the end of the financial year.


CBI
1947
CENTRAL BANK OF IRAQ