বাংলাদেশ ব্যাংক
প্রধান কার্যালয়
মতিঝিল, ঢাকা-১০০০
বাংলাদেশ
www.bb.org.bd

ব্যাংকিং প্রবিধি ও নীতি বিভাগ-২

বিআরপিডি-২ সার্কুলার নং-০৩

তারিখ : ০৬ শ্রাবণ ১৪৩৩ / ২১ জুলাই ২০২৬

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা
বাংলাদেশে কার্যরত সকল তফসিলি ব্যাংক

প্রিয় মহোদয়,

Guidelines on Internal Control Management System in Banks

সংশ্লিষ্ট বিষয়ে বিআরপিডি সার্কুলার নং ০৩, তারিখঃ ০৮ মার্চ ২০১৬ এবং বিআরপিডি সার্কুলার নং- ০৬, তারিখঃ ০৪ সেপ্টেম্বর ২০১৬ এর প্রতি দৃষ্টি আকর্ষণ করা যাচ্ছে।

২। বাংলাদেশের ব্যাংকিং খাতে রিস্ক বেইজড সুপারভিশন (আরবিএস) বাস্তবায়ন ত্বরান্বিত করার নিমিত্তে বর্ণিত সার্কুলারের মাধ্যমে জারীকৃত Guidelines on Internal Control and Compliance in Banks (ICC)-টি যুগোপযোগী ও স্বয়ংসম্পূর্ণ করার লক্ষ্যে গাইডলাইন্সটির শিরোনাম, বিভিন্ন অধ্যায় ও অনুচ্ছেদ সংশোধন/পরিমার্জন/পরিবর্ধন করে "Guidelines on Internal Control Management System in Banks" শীর্ষক নীতিমালা এতদ্সঙ্গে জারি করা হলো। এ নীতিমালাটি যথাযথভাবে অনুসরণ/পরিপালন করার জন্য সংশ্লিষ্ট সকলকে নির্দেশনা প্রদান করা হলো।

৩। এ নীতিমালায় বর্ণিত Internal Control Management System (ICMS) এর সাথে সামঞ্জস্যতা আনয়নের নিমিত্তে আগামী ৩১ ডিসেম্বর ২০২৬ তারিখের মধ্যে ব্যাংকসমূহ স্ব স্ব সাংগঠনিক কাঠামোতে প্রয়োজনীয় পুনর্বিন্যাস/পুনর্গঠন সম্পাদন করবে।

৪। ইতঃপূর্বে জারীকৃত বিআরপিডি সার্কুলার নং- ০৩/২০১৬ এবং ০৬/২০১৬ এ সার্কুলার দ্বারা রহিত করা হলো।

৫। 'ব্যাংক কোম্পানী আইন, ১৯৯১ (২০২৩ পর্যন্ত সংশোধিত)' এর ৪৫ ধারায় অর্পিত ক্ষমতাবলে এ সার্কুলার জারি করা হলো।

আপনাদের বিশ্বস্ত,

(মোঃ বায়েজীদ সরকার)
পরিচালক (বিআরপিডি-২)
ফোন ঃ ৯৫৩০০৯৫

GUIDELINES ON

INTERNAL CONTROL MANAGEMENT SYSTEM

IN BANKS

(July, 2026)

BANGLADESH BANK

The page is intentionally left blank

Preamble

A sound and effective Internal Control Management System (ICMS) is fundamental to ensuring the safety, stability, and resilience of the banking sector. In an increasingly complex financial environment characterized by technological transformation, diversified products, evolving risk dynamics, and heightened regulatory expectations, banks must establish robust governance and control frameworks to safeguard depositors' interests and maintain public confidence.

Bangladesh Bank, as the regulatory authority, is committed to strengthening risk governance, enhancing supervisory effectiveness, and promoting a culture of compliance and accountability across the banking industry. In line with the transition to Risk-Based Supervision (RBS) and internationally recognized standards, including the Basel Core Principles for Effective Banking Supervision (April 2024) and the Global Internal Audit Standards (January 2024), this "Guideline on Internal Control Management System (ICMS)" provides a clear and structured framework for internal control in banks.

This guideline replaces the "Guidelines on Internal Control & Compliance in Banks" issued in September 2016 and reflects contemporary best practices in governance, risk management, compliance, internal audit, data analytics, Shariah audit, information systems audit, and progressive control mechanisms. It emphasizes the formal adoption of the Three Lines of Defense model, strengthening the independence and accountability of internal audit and compliance functions, and enhancing the role of the Board of Directors and senior management in overseeing internal control processes.

The objective of this guideline is to establish minimum standards for internal control management applicable to all scheduled banks operating in Bangladesh, including conventional, Islamic Shariah-based banks, and Islamic banking branches/windows. Banks are encouraged to adopt more sophisticated control frameworks proportionate to their size, complexity, and risk profile, while ensuring full compliance with the minimum regulatory expectations outlined herein. Banks are advised to review their existing internal control architecture and take necessary measures to align their governance, risk management, and supervisory reporting mechanisms with the provisions of this guideline.

Bangladesh Bank expects that the effective implementation of this guideline will foster a strong compliance culture, improve operational efficiency, enhance transparency and reporting quality, mitigate emerging risks, and ultimately contribute to the stability and sustainable growth of the banking sector.

The page is intentionally left blank

Guidelines on Internal Control Management System in Banks

Working Committee

Team Leader

Mr. Md. Alauddin, Director (BRPD-2)
Banking Regulation and Policy Department-2, Bangladesh Bank

Members

Mr. Md. Shafiul Alam, Additional Director
Banking Regulation and Policy Department-2, Bangladesh Bank

Mr. Shathi Rangan Dey, Additional Director
Bank Supervision Department-4, Bangladesh Bank

Mr. Mohammad Mahbubur Rahman, Additional Director
Bank Supervision Department-12, Bangladesh Bank

Mr. Syed Shayfur Rahman, Additional Director
Bank Supervision Department-12, Bangladesh Bank

Mr. Rizwanul Karim, Joint Director
Banking Regulation and Policy Department-2, Bangladesh Bank

Mr. S M Zubayer Hussain, Joint Director
Banking Regulation and Policy Department-2, Bangladesh Bank
and Member Secretary

Mr. Md. Abu Sayed, Deputy Managing Director
Sonali Bank PLC.

Mr. A K M Saif Ullah Kowchar, Deputy Managing Director
City Bank PLC.

Mr. Mohammed Ashfaqul Hoque, FCA, FCS, Senior Executive Vice President
Shahjalal Islami Bank PLC.

Mr. Omar Faruque, Chief Compliance Officer
Standard Chartered Bank, Bangladesh

In addition, the following officials have also contributed:

Ms. Shahina Hossen, Deputy Director
Banking Regulation and Policy Department-2, Bangladesh Bank

Mr. Md. Sayeed Al Mamun Anik, Assistant Director
Banking Regulation and Policy Department-2, Bangladesh Bank

The page is intentionally left blank

Table of Contents

List of Acronyms

A&IT	Audit & Inspection Team
AAOIFI	Auditing and Accounting Organization for Islamic Financial Institution
ACB	Audit Committee of the Board
AD	Authorized Dealer
ADP	Automated Data Processing
AML	Anti-Money Laundering
BAS	Bangladesh Accounting Standards
BB	Bangladesh Bank
BCP	Basel Core Principles for Effective Banking Supervision
BCBS	Basel Committee on Banking Supervision
BFIU	Bangladesh Financial Intelligence Unit
BIS	Bank for International Settlement
BoD	Board of Directors
BRPD	Banking Regulation &Policy Department
BSEC	Bangladesh Securities and Exchange Commission
CEO	Chief Executive Officer
CRA	Compliance Risk Assessment
CRM	Compliance Risk Management
CMP	Compliance Monitoring Plan
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSR	Corporate Social Responsibility
DCFCL	Departmental Control Function Check List
DMD	Deputy Managing Director
EDP	Electronic Data Processing
ERM	Enterprise Risk Management
FRSB	Financial Reporting Standards Boards
HoC	Head of Compliance
HoIA	Head of Internal Audit
IAS	International Accounting Standards
ICMS	Internal Control Management System
ICT	Information & Communication Technology
IFSB	Islamic Financial Services Board
IIA	Institute of Internal Auditors, Inc
IT/IS	Information technology/ Information System
LDCL	Loan Documentation Check List
MANCOM	Management Committee
MIS	Management Information System
MD	Managing Director
NBR	National Board of Revenue
QAIP	Quality Assurance and Improvement Program
QOR	Quarterly Operations Report

RBAP	Risk-Based Audit Plan
RBIA	Risk-Based Internal Audit
RBS	Risk Based Supervision
SAAFIC	Self-Assessment Anti-Fraud Internal Control Checklist
SMT	Senior Management Team
SPCD	Supervisory Policy and Coordination Department
SSC	Shariah Supervisory Committee
STR	Suspicious Transaction Report
TBML	Trade-Based Money Laundering
VaR	Value at Risk

Chapter 1: Introduction

1.1. Background

This guideline is issued by Bangladesh Bank (BB) under section 45 of the Bank Company Act, 1991(amended up to 2023) with a view to providing a framework for an effective internal control system, good governance, transparency of all financial activities, and accountability towards its stakeholders and regulators.

This guideline is prepared in line with internationally accepted standards, principles and best practices for internal control management. The guideline is also aligned with the Basel Core Principles for Effective Banking Supervision (BCP) published by the Basel Committee on Banking Supervision (BCBS) in April 2024. The BCP26 on 'Internal control and audit' requires that banks have an independent, permanent and effective internal audit function. It also advocates that the banks have an adequately staffed, permanent and independent compliance function that assists senior management in managing effectively the compliance risks faced by the bank. The guideline also conforms with the "Global Internal Audit Standards" published by the Institute of Internal Auditors, Inc (The IIA) in January 2024.

1.2. Scope of the Guideline

The guideline is applicable for all scheduled banks (conventional, Islamic Shariah and Islamic banking branches/windows of conventional banks) operating in Bangladesh. In issuing the guideline, Bangladesh Bank intends to provide guidance to all banks on minimum standards for Internal Control Management System (ICMS). A bank may, depending on its size and complexity, establish a more sophisticated framework than outlined in this document.

However, Bangladesh Bank considers compulsory for all banks to self-assess their present operational context, and customize their ICMS architecture and approach to attain organizational goals while meeting the minimum requirements set out in the guideline. This guideline is issued replacing the "Guidelines on Internal Control & Compliance in Banks" published in September, 2016. However, this guideline shall supplement all the relevant existing policies and/or guidelines published/to be published by Bangladesh Bank from time to time.

Although, Risk Management is an integral part of ICMS, this guideline does not cover the risk management function, as it is comprehensively covered under a separate regulatory framework: 'Risk Management Guidelines for Banks' (DOS Circular No. 04, dated 8 October 2018).

1.3. Definition of Internal Control

Banking is a diversified and multifarious financial activity which involves different risks. So an effective internal control management system has become essential in order to underpin effective risk management practices and to ensure smooth performance of the banking industry. Specially, as a cornerstone of adopting the Risk Based Supervision (RBS), a forward-looking and process-based internal control management system can enable early identification and mitigation of key risks. As such, to ensure smooth and effective transition, all banks are required to take preparatory measures and align their risk governance, internal control structures, management information systems and supervisory reporting mechanisms with RBS principles.
In general, internal control is a process, effected by a bank's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

Internal control is not a separate activity disconnected from the rest of business activities, rather is an integral part of those activities. It is a dynamic, continuing series of activities planned, implemented and monitored by the board of directors and management at all levels within an organization. A part of internal control consists of policies and procedures. Policies are board or management statements about what should be done, and may even be unwritten and implied by management's actions. Procedures are the actions that implement a policy, or how it should be done.

1.4. The Three Lines of Defense Model

The responsibility of implementing internal controls starts with the business lines, which are the "first lines of defense" against breaches that could cause the bank not to fulfill its objectives, not to report properly, or not to comply with laws and regulations. Beyond that, in any bank, the three important "control functions" are risk management, compliance, and internal audit. The first two of these control functions constitute the "second lines of defense" against mishaps. The final, or "third line of defense" is the internal audit function.

Banks must formally adopt and implement a Three Lines of Defense model to ensure clear accountability and effective risk management.

- ✓ **First Line of Defense (Business Units):** Management and staff in business units own and are directly responsible for identifying, assessing, and managing the compliance risks inherent in their activities. They are responsible for executing internal controls and complying with internal policies and external regulations in their day-to-day operations.
- ✓ **Second Line of Defense (Compliance & Risk Functions):** The Compliance Function provides independent oversight, challenge, and specialist expertise to the first line. It is responsible for developing the compliance risk management framework, policies, tools, and for monitoring the effectiveness of the first line's controls.

- ✓ **Third Line of Defense (Internal Audit):** Internal Audit provides independent and objective assurance to the Board of Directors and the Board Audit Committee of the Board (ACB) on the overall effectiveness of the bank's governance, risk management, and internal control processes, including the effectiveness of the first and second lines of defense.

1.5. Objectives of Internal Control Management System

The primary objectives of internal control management system in a bank are to help the bank perform better through the use of its resources, to communicate better internally and with external stakeholders, and to comply with applicable laws and regulations. The main objectives of internal control management system can be categorized under i. Operational, ii. Reporting, and iii. Compliance, as follows:

1.5.1. Operational Objectives

To achieve a bank's basic mission and vision, internal control helps:

- ✓ financial performance (the size, profitability, liquidity, and capital adequacy of the bank);
- ✓ productivity (minimizing operating expenses);
- ✓ customer and employee satisfaction;
- ✓ achievement of social goals (corporate social responsibility, financial inclusion);
- ✓ safeguarding of assets (preventing unauthorized acquisition, use, or disposition); and
- ✓ compliance with a bank's internal policies and procedures.

1.5.2. Reporting Objectives

The ***reporting objectives*** of internal control ensure that all the necessary information flow within the bank, into the bank, and out of the bank. Reporting objectives can be subdivided into four categories:

- ✓ **External financial reporting** includes supervisory reporting to BB, unaudited and audited financial statements submitted by banks to BB and the BSEC, and other required financial disclosures such as intent to issue shares.
- ✓ **External non-financial reporting** includes submission of Board minutes to BB, public statements issued by banks on their new products and services, CSR initiatives, etc.
- ✓ **Internal financial reporting** includes "management information systems" or MIS related to reports to the Board on liquidity, asset quality, profitability, capital adequacy, etc., reports on profitability by line of business or by customer, and reports on major expenditures that require approval of the Board.
- ✓ **Internal non-financial reporting** includes communication between and among senior management and staff on policies and procedures, HR-related communications on compensation and benefits, internal transfers and promotions, corporate codes of ethics and conduct, etc.

1.5.3. Compliance Objectives

The compliance objectives of internal control refer to:

- ✓ ensuring that the bank stays in compliance with all applicable laws and regulations, not only those specifically pertaining to banks, but also those laws and regulations (such as labor laws and environmental protection laws) applying to corporations in general;
- ✓ adhering to laws and regulations as the minimum standards of conduct expected by BB as the regulatory authority;
- ✓ conducting activities and taking specific actions in accordance with applicable laws and regulations.

1.6. Components of Internal Control

According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the above three categories of objectives – operations, reporting, and compliance – are supported by five ***components* of internal control**. Underlying these five components is a set of 17 principles, organized in the following manner:

1.6.1. Control Environment

1. The bank demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The bank demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The bank holds individuals accountable for their internal control responsibilities in pursuit of objectives.

1.6.2. Risk Assessment

6. The bank specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The bank identifies risks to the achievement of its objectives across the bank and analyzes risks as a basis for determining how the risks should be managed.
8. The bank considers the potential for fraud in assessing risks to the achievement of objectives.
9. The bank identifies and assesses changes that could significantly impact the system of internal control.

1.6.3. Control Activities

10. The bank selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The bank selects and develops general control activities over technology to support the achievement of objectives.
12. The bank deploys control activities through policies that establish what is expected and procedures that put policies into action.

1.6.4. Information and Communication

13. The bank obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The bank internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The bank communicates with external parties regarding matters affecting the functioning of internal control.

1.6.5. Monitoring Activities

16. The bank selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The bank evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.

1.7. Internal Control Function Concepts

The internal control functions involve risk management, compliance, and internal audit. Again, the compliance function of a bank comprises of two activities, i.e., i. compliance and ii. monitoring. These functions are interlinked as described below:

1.7.1. Risk Management as a function of Internal Control

Risk management, as a function of internal control, involves the systematic identification, assessment, and mitigation of threats towards the achievement of the bank's objectives, with internal controls providing the specific policies, procedures, and structures (like segregation of duties, authorization processes) that implement and monitor these risk responses, ensuring goals are met reliably and operations remain efficient and compliant. Essentially, risk management sets the strategy for handling threats, while internal controls are the tools and actions used to execute that strategy, forming an integrated system.

1.7.2. Compliance as a function of Internal Control

Compliance, as a function of internal control, ensures a bank adheres to external laws/regulations and internal policies. It involves designing, implementing, and monitoring processes (controls) to prevent, detect, and correct violations, thereby safeguarding assets,

reputation, and achieving objectives. Essentially, internal controls provide the framework (policies, procedures), and the compliance function executes, verifies and monitors adherence to that framework.

1.7.3. Internal Audit as a function of Internal Control

Internal Audit acts as the independent "control of controls," providing objective assurance that a bank's risk management, governance, and internal control processes are effectively designed and operating to help achieve business objectives, identifying weaknesses, and recommending improvements. While management owns internal controls, the internal audit function evaluates their adequacy, efficiency, and compliance, offering an unbiased review of the entire system.

1.7.4. Interrelationship among the functions of internal control

Risk Management, Compliance, and Audit are interconnected pillars of internal control, forming a continuous cycle- Risk Management identifies and assesses risks, Compliance ensures adherence to rules, and Audit provides independent assurance on the effectiveness of both, providing feedbacks to improve risk strategies and controls. Risk management sets the *what* (risks to manage), compliance sets the *rules* (laws, policies), and audit validates *how well* they're working, all within the broader internal control framework to achieve objectives.

Chapter 2: Internal Control Management Framework

2.1. Composition of Internal Control Management

All departments, and all business lines, are responsible for developing, implementing, and making sure that the controls are observed and not breached. Individual departments or business lines will be vigilant and will participate fully in the internal control regime where Internal Control Management System (ICMS), consisting of Internal Audit, Compliance and Monitoring, should act as internal watchdog of the organization. They will oversee whether bank is following regulatory guidelines, institutional policies and procedures set by/and approved by the Board of Directors covering related Laws of land and whether there is any deficiency in internal policy and procedure.

2.2. Organization Structure/ Organogram of ICMS

For smooth functioning of Internal Control Management System, it shall be comprised of three major functions, which are as follows-

a. Internal Audit Function

b. Compliance Function

c. Risk Management Function (covered in 'Risk Management Guidelines for Banks', DOS Circular No. 04, dated 8 October 2018)

For convenient way of action and effective administration according to the nature of the bank, volume of work, no. of branches, (rural, urban, AD, corporate), assets involvement, concentration of assets, risk involvement etc., Internal Audit Function and Compliance Function may be further divided in to the following divisions/ units. A brief of the organization structure of ICMS is illustrated in Chart-1.

2.2.1. Internal Audit Function

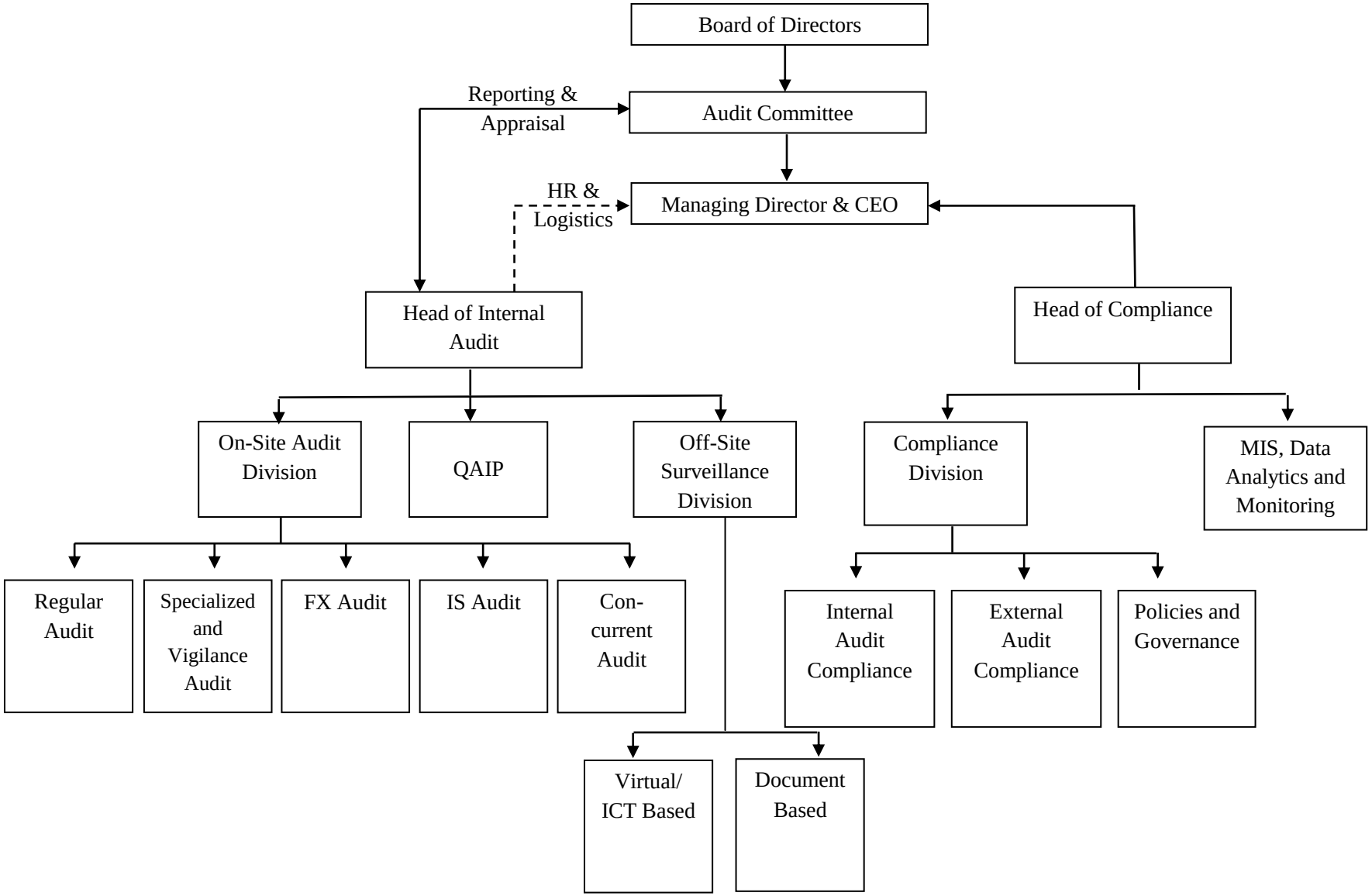
Internal Audit Function is responsible for planning and conducting audits across business units, branches, divisions, subsidiaries, and support functions to assess compliance, operational effectiveness, and risk exposure. It may be sub-divided into- a. On-site Audit Division and b. Off-Site Surveillance Division.

2.2.1.1. On-Site Audit Division

Auditors go to the branch or department or business units in person and conduct different types of audits:

a) **Regular Audit:** regular, planned, in-depth checks of whether an operating segment (branch/sub-branch/wing/division/unit/subsidiary, etc.) is conforming to the rules.
b) **Specialized, Surprise and Vigilance Audit:** investigations into specific issues such as suspected fraud, whistleblower complaints, serious irregularities, or areas identified as high-risk by management or the Board.

Chart 1: The Organogram & Structure of Internal Control Management System (ICMS)



c) **Foreign Exchange (FX) Audit:** Specialized audits focusing on foreign trade transactions, compliance with applicable foreign exchange laws and regulations, and assessment of related operational and compliance risks.
d) **Information Systems (IS) Audit:** Evaluation of the organization's information technology environment, including system security, data integrity, application controls, infrastructure resilience, and IT governance.
e) **Concurrent Audit:** Continuous, on-site, and real-time review of banking operations and financial transactions as they occur, with the objective of early detection of fraud, errors, and regulatory non-compliance

2.2.1.2. Off-Site Surveillance Division

This division shall keep an eye on things and conduct audits from the desk without going to the site.

a) **Virtual/ICT Based Audit:** Use Management Information Systems (MIS), data analytics tools, software/systems to remotely monitor transactions, identify patterns and anomalies (red flags), and generate data-driven insights to conduct audit or keep an eye on system logs and transaction alerts.
b) **Document Based Audit:** Checking for compliance or lapses by looking over periodic reports, returns, and statements that branches and departments send in.

2.2.1.3. Quality Assurance and Improvement Program (QAIP)

Another important part of the Internal Audit Division/Unit is QAIP, which is a structured framework designed to ensure the Internal Audit Function maintains independence, objectivity, and consistently delivers high-quality assurance in line with the International Standards for the Professional Practice of Internal Auditing (IIA Standards).

2.2.2. Compliance Function

The Compliance Function is established to ensure that the organization operates in full adherence to applicable laws, regulations, regulatory guidelines, internal policies, and ethical standards. The major divisions of under this function are discussed below.

2.2.2.1. Compliance Division

This division is responsible for ensuring timely and effective closure of compliance issues arising from internal and external sources. Its scope covers the following key areas:

a) **Internal Audit Compliance:** this function is responsible for tracking and monitoring internally detected instances of regulatory, statutory, and Risk-Based Supervision (RBS) non-compliance, whether identified before or after the stipulated reporting timelines. It ensures timely escalation, coordination with responsible units, formulation and monitoring of corrective action plans, validation of remediation effectiveness, and confirmation of closure to prevent recurrence and mitigate regulatory risk.

b) **External Audit Compliance:** To monitor compliance activities of branch, Office and sub-divisions under external audit (Bangladesh Bank Audit/Inspection, Commercial Audit, External Audit /statutory audit and other regulatory authorities).

c) **Policies and Governance:** The responsibilities of this division/department includes developing, reviewing, and updating compliance-related policies, manuals, and standard operating procedures; ensuring alignment of internal policies with regulatory requirements and best practices; supporting governance frameworks, including code of conduct, compliance culture, and ethical standards; assisting management and the Board in strengthening overall compliance governance, etc.

2.2.2.2. MIS, Data Analytics and Monitoring Division

This division/department supports the Compliance function through continuous and risk-based monitoring using Management Information Systems (MIS), data analytics, and surveillance tools. Its primary responsibilities include: using data analytics to detect trends, exceptions, unusual activities, and potential regulatory breaches; developing dashboards, exception reports, and early warning indicators to support proactive compliance risk management; providing analytical inputs for compliance risk assessments and regulatory reporting, etc.

2.3. Roles, Responsibilities and Key Aspects in ICMS

2.3.1. Internal Audit Function and Head of Internal Audit (HoIA)

Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk Management, control and governance processes. The following aspects should be addressed:

2.3.1.1. The internal audit activity should be independent and objective oriented.

2.3.1.2. The purpose, authority and responsibility of the internal audit activity should be formally defined in a charter, consistent with the Auditing standards, approved by the Audit Committee of the Board (ACB) and the Board.

2.3.1.3. Internal auditors should have to be bold, honest and truthful. These qualifications will be the basis for trust on the internal auditor's professional judgment.

2.3.1.4. Internal auditors should keep strict confidentiality of information found during audit. They should not use such information for personal gain or malicious action and should be responsible for protection of such information.

2.3.1.5. The Head of the internal audit and all internal auditors should avoid conflicts of interest and should abide by the bank's code of ethics. A code of ethics

should address the principles of objectivity, competence, confidentiality and integrity.

2.3.1.6. The HoIA shall report his/her activities and findings directly to ACB and will be responsible to the ACB. S/he shall have full and free access to the ACB.

2.3.1.7. Appraisal of the HoIA shall be done by the ACB and the any personnel of Internal Audit Department shall be conducted under the purview of HoIA.

2.3.1.8. Any complaint against HoIA will be placed to the ACB by the MD/CEO. The management shall not alter any appraisal of the ACB unless such alteration is reported to and approved by the ACB.

2.3.1.9. The management shall be responsible for providing HR and logistic support to the Internal Audit Division.

2.3.1.10. Human Resources of the Internal Audit Division shall be a combination of business, Professional and IT knowledge based personnel. Number of officials shall depend on the number of branches to be audited, frequency of audit, efficiency of the auditors (depending upon the past experience) etc.

2.3.2. Compliance Function and Head of Compliance (HoC)

The Compliance Function ensures that an organization follows laws, regulations, and internal policies through risk assessment, policy development, staff training, regular audits, and incident response, acting as a crucial advisor and watchdog to prevent legal/financial harm and uphold ethical standards, reporting findings to management and regulatory bodies. Their core function is continuous oversight, identifying vulnerabilities, and driving corrective actions to embed a strong compliance culture.

2.3.2.1. The purpose, authority and responsibility of the Compliance Function shall be formally defined in a Compliance Policy Charter, which shall approved by the Audit Committee of the Board (ACB) and the Board.

2.3.2.2. The charter shall also define the relationship of Compliance Function with other risk management units and the internal audit functions.

2.3.2.3. The HoC shall be liable for developing and maintaining the bank's Compliance Policy Charter, Compliance Risk Management Framework, annual Compliance Risk Assessment (CRA) process, Risk-based Annual Compliance Monitoring Plan (CMP) etc.

2.3.2.4. The HoC must possess high professional competence, and integrity, with expert knowledge of applicable laws, regulations, and the bank's products and activities.

2.3.2.5. The operation of Compliance Function shall be independent from the business lines;

2.3.2.6. The HoC shall report to the ACB through MD/CEO. However, the HoC will have right to express and disclose findings freely to the ACB/BoD, if necessary.

2.3.2.7. The HoC shall be appraised by the Senior Management/ MD/ CEO. The officials of Compliance Function shall be appraised under the purview of the HoC.

2.3.2.8. The HoC shall serve as the primary point of contact for regulators on compliance issues including tracking, validation, and settlement of regulatory observations for satisfactory closure.

2.3.3. Other Key Aspects Related to ICMS

2.3.3.1. The designation/rank of the Head of Internal Audit (HoIA) and Head of Compliance **(**HoC**)** shall ideally be not lower than two steps immediate below the CEO. However, the Board of the Directors may relax the rank considering bank's size, operation, manpower etc. subject to approval from the concerned Bank Supervision Department of Bangladesh Bank.

2.3.3.2. The HoIA and HOC shall be of same designation. Both of them shall be out of any other responsibilities.

2.3.3.3. The officials of ICMS shall have unrestricted access to all functions, records, property and personnel.

2.3.3.4. Officials of ICMS shall have thorough professional knowledge and banking experience with good academic background.

2.3.3.5. Track record of officers to be checked and maintained before posting them in ICMS. Persons punished for major offence and persons under disciplinary proceedings must not be posted in ICMS.

2.3.3.6. The officials of Internal Audit Division shall not audit their own works performed in their previous Departments/Offices.

2.3.3.7. During the audit period, if the present audit team finds any lapse or irregularity which was not detected or identified by the previous auditor, then that will be reported to the ACB.

2.3.3.8. In compliance with the essence of anti money laundering and fraud forgery prevention, unit heads under ICMS should prepare a confidential mandatory annual (10 days per year) leave plan for employees working under her/him with the consent of the HoIA and HoC. The HoIA and HoC shall also be under same compulsion planned by the Chairman of Audit Committee and the MD/CEO respectively.

2.3.3.9. Such mandatory leave shall be sanctioned by the management at any time as required/planned and the sanctioned leave can only be changed by the management, employee cannot claim for alteration.

2.3.3.10. The officials of the ICMS shall be rotated among different divisions as per the instructions contained in the BRPD circular no. 15 dated 25 October 2018 or any subsequent policies/circulars by BB. However, any posting or transfer of officials to and from Internal Audit Department shall not be made without the consent of the HoIA and the transfer/posting/ appointment/removal of HoIA and HoC shall be approved by the ACB.

2.3.3.11. Officials of the ICMS shall be provided with appropriate advance local and foreign trainings to acquire updated knowledge of modern banking in areas including, but not limited to, Internal Audit & Compliance; Credit Risk Grading, Compliance of Regulatory Inspection; Accounting & Auditing Standards; IT Auditing etc.

2.3.3.12. For foreign banks operating in Bangladesh, the ICMS may have structural flexibility. However, all functions of the ICMS described in this guideline must be present in the organization, regardless of the name or structure.

2.4. Roles and Responsibilities of Board and Management

2.4.1. Responsibilities of the Board of Directors (BOD)

The responsibility of the Board of Directors in respect of implementing a modern, scientific and acceptable Internal Control Management Process in a Bank has been described in Banking Companies Act, 1991 (BCA) Rule 15 (Kha) and exclusively in section 15 (Ga). The responsibility of BOD can be summarized as follows:

2.4.1.1. The board shall be observant on the internal control system of the bank in order to accomplish a satisfactory standard of its portfolio.

2.4.1.2. The board will form an Audit Committee with such directors who are not the members of Executive Committee of BOD and a Risk Management Committee from its members.

2.4.1.3. The board will also establish such an internal control system so that the whole internal audit process can work independently from the management which will report to the Audit Committee of the Board (ACB).

2.4.1.4. The BOD shall review the reports submitted by the ACB on quarterly basis regarding compliance of recommendations made in internal and external audit reports and as well as Bangladesh Bank inspection reports.

2.4.1.5. They should set up an organizational structure of Internal Management System in such a way that, it should have no conflict of interest with the

regular management of the bank and fulfill the requirements as directed in the Rule 15 (Ga) (1) of BCA 1991 for establishing and maintaining effective internal control and risk management having regard to the complexity of the activities of the bank, its size, scope of operations and risk profile;

2.4.1.6. The board of directors should, at least annually, conduct a review meeting about the effectiveness of internal control process and report to the shareholders accordingly;

2.4.1.7. The board of directors should hold meetings in suitable intervals with interested parties such as senior management, internal auditors, external auditors and the audit committee in the evaluation of the effectiveness of the internal control system.

2.4.1.8. It shall be ensured that the internal audit reports are provided to the board (if asked for) without management filtering and that the internal auditors have direct access to the board's audit committee as and when required requiring timely and effective correction of audit issues by senior management.

2.4.2. Responsibilities and Structure of the Audit Committee of the Board

The board will approve the objectives, strategies and overall business plans of the bank and the audit committee will assist the board in fulfilling its oversight responsibilities. The committee will inspect/review the inspection process of financial reporting, internal control system, the audit process and the bank's operations being conducted within the existing Acts and laws & regulations imposed by the regulatory authorities and its own code of business conduct. The responsibilities and structure of the Audit Committee of the Board shall be determined by the BRPD Circular-02 dated 11 February 2024 or any subsequent policies/circulars by BB.

2.4.2.1. Organizational structure

i) The audit committee will comprise of a maximum 05 (five) members, among whom at least 2 (two) independent directors will be included.
ii) One chairman/president of the audit committee will be elected from the independent directors.
iii) The tenure of the chairman/president of the audit committee will be 3 (three) years. An independent director cannot serve consecutively for two terms as the chairman/president of the audit committee.
iv) No member of the executive committee can be included as a member of the audit committee.
v) Members may be appointed for a period of 03 (three) years;
vi) Company secretary of the bank will be the secretary of the audit committee.

2.4.2.2. Qualification of the Members of the Audit Committee

i) Individuals who are capable of contributing effectively and efficiently to the committee's functions should be appointed as members.
ii) Committee members must have a thorough understanding of the Bank Company Act, 1991, relevant other Acts and regulations related to banking operations, auditing, banking business, management of banks, various risk factors, and the duties & responsibilities of members of the committee.
iii) Individuals with practical experience in the field of banking operations, especially those with educational qualifications in Accounting, Cost Accounting, Finance, Banking, Management, and Economics, should be given priority in forming the committee. In the case of a digital bank, at least one person with expertise in ICT matters must be nominated as a committee member.

2.4.2.3. Roles and Responsibilities of the Audit Committee

i) Internal Control:
   1. The Audit Committee will evaluate whether management has been able to set the appropriate compliance culture, whether clear directives have been given to the bank's officials/employees regarding their roles and responsibilities and whether there is full compliance and control over their work;
   2. The Audit Committee will review whether the recommendations made periodically by internal and external auditors on internal control strategies/framework, have been implemented by the management and provide necessary guidance;
   3. The Audit Committee will regularly update the board about irregularity, fraud, forgery, and weaknesses in internal control detected by internal and external auditors and inspecting team of the regulatory authority or the corrective actions taken regarding similar issues detected by them.

ii) Financial Reporting:
   1. The audit committee will check whether the financial statements reflect the comprehensive and concrete information and determine whether the country's prevailing rules & regulations and accounting standards, as well as the relevant accounting standards prescribed by the Bangladesh Bank in this regard, have been followed in preparing the financial statements.
   2. The audit committee will discuss with the inspection team of the Bangladesh Bank, the external auditors and management to review the financial statements before its finalization.

iii) Internal Audit:
   1. The audit committee will ensure whether internal audit working independently from the management.
   2. The audit committee will review the activities of the internal audit and the organizational structure.

3. The Audit Committee will assess the efficiency and effectiveness of internal audit function and recommend necessary measures accordingly;
4. The Audit Committee will also verify whether the findings/recommendations made by the internal auditors regarding regularizing irregularities detected by them, management of the bank's operations etc. are being properly addressed by the bank management and provide necessary guidance.

iv) External Audit

1. The Audit Committee will review audit activities conducted by the external auditors and their audit reports;
2. The Audit Committee will also verify whether the findings/recommendations of the external auditors on regularizing irregularities, fraud and forgeries detected by them and the management of the bank's operations are being properly considered by the management authorities or not.
3. The Audit committee will recommend regarding the appointment of the external auditors from the list of external auditors announced by the Bangladesh Bank from time to time.

v) Compliance with existing laws and Regulations:

The Audit Committee will review whether banking laws, rules & regulations, policies and guidelines issued by regulatory authorities (Central Bank and other institutions), and internal policies approved by the Board are being properly complied with.

vi) Other Responsibilities:

1. The Audit Committee will submit compliance report to the board on quarterly basis on regularization of the irregularity, fraud and forgeries detected by the internal and external auditors and inspection team of the Bangladesh Bank and directions described in any observation;
2. External and internal auditors will submit their related assessment report, if the committee solicit;
3. The committee will evaluate any matter as desired lawfully by the Board of Directors and submit a report/recommendation on it.

2.4.2.4. Meetings of the Audit Committee

i) The audit committee should hold at least 4 meetings in a year and it can sit any time as it may deems necessary;
ii) The committee may invite the Chief Executive Officer of the bank, the officer in charge of internal audit, or any other official to its meetings, if it deems necessary;
iii) To ensure active participation and contribution by the members at every meeting, a detailed memorandum should be distributed to committee members at least 2 (two) days prior to each meeting.
iv) All recommendations/observations of the committee should be noted in minutes.

2.4.3. Responsibilities of the Senior Management

In setting out a strong control framework within the organization, the role of the senior management, lead by the Managing Director/ CEO, is very important.

2.4.3.1. The board of directors of the bank will define/form Senior Management Team (SMT) that should include the MD/CEO and the Chief Financial Officer. Any officer that perform a policy making function or is in charge of a principal business unit/function may be member of SMT.

2.4.3.2. Although, the HoIA shall not be a member of SMT, s/he must attend the meetings of the SMT as an observer.

2.4.3.3. The bank shall report the composition of the SMT (and update thereto) to the concerned Bank Supervision Department of Bangladesh Bank.

2.4.3.4. SMT shall monitor the adequacy and effectiveness of the Internal Control Management System based on the bank's established policy and procedure.

2.4.3.5. The SMT will review on a yearly basis the overall effectiveness of the control system of the organization and provide a certification on a yearly basis to the Board of Directors on the effectiveness of Internal Control policy, practice and procedure.

2.4.3.6. The management will enrich audit teams with adequate skilled manpower and proper IT support as per requisition of the ACB for purposeful and effective audit.

2.4.3.7. The management will ensure compliance of all laws and regulations that are circulated by various regulatory authorities such as, Bangladesh Bank, Ministry of Finance, Bangladesh Securities and Exchange Commission, etc.

2.5. Management Information Systems (MIS)

- ✓ An effective internal control system requires that there is an efficient reporting system of information that is relevant to decision making. The information should be reliable, timely accessible and provided in a consistent format.
- ✓ Information system shall include external market information about events and conditions that are relevant to decision making. Internal information should include financial, operational and compliance data.
- ✓ There should be appropriate committees within the organization which would evaluate data received through various information systems. This will ensure supply of correct and accurate information to the management.
- ✓ Internal information must cover all significant activities of the bank. Electronic data must be secured, monitored independently and supported by contingency arrangements.

- ✓ The channels of communication must ensure that all staff fully understand and adhere to policies and procedures effecting their duties and responsibilities and that other relevant information are reaching the appropriate personnel.

2.6. Role of External Auditors in Evaluating the Internal Control System

- ✓ The external auditors, by dint of their independence from the management of the bank, must provide recommendations on the strengths and weaknesses of the internal control system of the bank and submit their findings in the management report.
- ✓ They should examine the records, transactions of the bank and evaluate its accounting policy, disclosure policy and methods of financial estimation made by the bank; they will cooperate the Board and the Management to have an independent overview on the overall control system of the bank.
- ✓ The external auditors shall evaluate whether the internal audit and internal control systems of the bank are functioning effectively and whether they are independent of the bank management, as per Section 15 (Ga) of the Bank Company Act, 1991; and whether any serious irregularities or weaknesses have been observed in this regard.
- ✓ They shall provide opinions on whether appropriate steps have been taken to settle the irregularities detected during the comprehensive and special inspections conducted by Bangladesh Bank and also whether the irregularities identified in the internal audits and other statutory audits of the previous year have been properly settled or resolved.

2.7. Dispute Settlement

- ✓ Any unresolved issue between SMT and ICMS shall be referred to the Board of Directors through SMT and ACB respectively and then to Bangladesh Bank (if needed).
- ✓ If any irregularity is found against the Board of Directors or MD/CEO during any Audit, it shall be communicated confidentially directly to Banking Regulation and Policy Department-2 and the concerned Bank Supervision Department of Bangladesh Bank.

Chapter 3: Identification & Assessment of Risk

3.1. Assessing Business and Control Risk

Risk is the net negative impact of vulnerability in banking operations, considering both the probability of occurrence and the potential impact. Effective risk assessment must identify and consider both internal and external factors.

An effective internal control system continually recognizes and assesses all material risks that could adversely affect the achievement of the bank's goals. Internal audit differs from business risk management by focusing more on reviewing business strategies to maximize risk/reward trade-offs within different areas of the bank. The risk assessment by internal audit focuses on all risk areas, especially those affecting banking industry compliance with regulatory requirements, social, ethical, technological, enterprise and environmental risks.

The internal audit function plays a pivotal role in ensuring that the bank’s internal control system effectively recognizes and evaluates all material risks that could hinder the achievement of organizational objectives. It seeks to provide independent assurance over all critical risk areas, with particular emphasis on regulatory compliance; ethical and social responsibilities; and environmental and sustainability risks.

Unlike management’s risk assessments, which often balance risks against opportunities in pursuit of strategic goals, internal audit adopts an independent, assurance-oriented perspective that emphasizes reliability, compliance, and sustainability.

Internal audit evaluates whether the bank’s control environment adequately captures significant risks across operations, financial reporting, and compliance. The function emphasizes early recognition of threats that could compromise operational integrity, financial soundness, or reputation, ensuring that risks are not overlooked as business activities evolve.

3.1.1. Internal Factors

The following internal factors must be evaluated to assess how they contribute to business and control risks as they directly influence business risks (e.g., operational inefficiencies leading to losses) and control risks (e.g., weak segregation increasing fraud likelihood):

- ✓ **Complexity of the Organization Structure**: hierarchical layers, decentralization levels, interdepartmental dependencies, and integration of subsidiaries or affiliates.
- ✓ **Nature of the Bank's Activities**: volume and diversity of products (e.g., retail banking, investment services), transaction complexity (e.g., derivatives, foreign exchange), and exposure to high-risk segments like leveraged lending.
- ✓ **Quality of Personnel**: skills, training levels, experience, and ethical standards of employees; adequacy of staffing in key areas like compliance and IT.

- ✓ **Organizational Changes**: mergers, acquisitions, restructuring, or system upgrades that disrupt operations.
- ✓ **Employee Turnover**: high attrition rates leading to knowledge gaps, especially in specialized roles like risk management or audit.
- ✓ **Control Environment**: tone at the top, segregation of duties, access controls, and monitoring mechanisms.
- ✓ **IT Systems and Cybersecurity**: reliability of core banking software, data integrity, vulnerability to internal breaches, and disaster recovery plans.
- ✓ **Internal Policies and Procedures**: Adequacy of fraud prevention, training programs, and performance variances from budgets.
- ✓ **Operational Processes**: Efficiency in cash handling, reconciliation, and third-party vendor management.

3.1.2. External Factors

External factors are often beyond the bank's direct control but must be monitored for their impact on business viability and control effectiveness. These factors amplify business risks (e.g., economic downturns increasing Credit/Investment defaults) and challenge control risks (e.g., new regulations requiring updated compliance systems). The external factors include:

- ✓ **Fluctuating Economic Conditions**: inflation rates, interest rate volatility, GDP growth/decline, unemployment levels, and currency fluctuations affecting loan/investment repayments.
- ✓ **Changes in the Industry**: competitive pressures, market consolidation, emergence of fintech disruptors, and shifts in customer preferences (e.g., digital banking).
- ✓ **Socio-Political Realities**: geopolitical tensions, social unrest, demographic shifts (e.g., aging populations), and cultural factors influencing consumer behavior.
- ✓ **Technological Advancements**: adoption of AI, blockchain, or cloud computing; risks from cyber threats, data privacy regulations (e.g., GDPR equivalents), and obsolescence of legacy systems.
- ✓ **Changes in Rules and Regulations**: updates to Basel accords, anti-money laundering (AML) laws, capital adequacy requirements, or environmental/social governance (ESG) mandates.
- ✓ **Market Volatility**: commodity price swings, stock market fluctuations, and supply chain disruptions (e.g., from global events like pandemics).
- ✓ **Geopolitical Risks**: trade wars, sanctions, or political instability in key markets.
- ✓ **Environmental and Social Factors**: climate change impacts on asset values (e.g., stranded assets in fossil fuels), reputational risks from ethical lapses, or community expectations for sustainable banking.

3.2. Construction of Audit Risk Model

The audit risk model in internal auditing is built around three interrelated components—business (inherent) risk, control risk, and detection risk—which collectively determine the auditor's ability to provide reliable assurance on the bank's financial reporting and risk management processes.

3.2.1. Business (Inherent) Risk

Business or inherent risk refers to the susceptibility of a bank's activities, processes, or account balances to material error, failure, or misstatement in the absence of any related internal controls. It stems from the very nature of banking operations, strategies, and environmental exposures. For example, defaults on credit or investment portfolios, volatile market conditions, complex financial products, large transaction volumes, organizational changes, or elevated staff turnover all contribute to inherent risk. This makes it a central factor in prioritizing audit plans, as it reflects vulnerabilities that exist before any mitigating controls are applied.

A list of topics which can be incorporated into the Business (Inherent) Risk analysis is given below. They focus on inherent vulnerabilities in core banking activities, including both qualitative and quantitative elements influenced by internal and external factors (e.g., organizational complexity, economic fluctuations). (This is a sample list Banks may add more topics to the category for better risk analysis):

Category	Subtopics
Credit/Investment Risk	- Credit/Investment risk quality and composition - Provisioning for Credit/Investment process - Quality of assessment and appraisal - Sanction processes - Organizational structure for managing Credit/Investment risk - Borrower default susceptibility - Counterparty failure in guarantees/derivatives - Exposure to high-risk segments (e.g., mortgages, Credit/Investment cards)
Earning Risk	- Profitability achievement - Income generation and sustainability - Revenue stream diversity - Interest rate exposure - Fee-based income volatility - Investment portfolio performance
Liquidity Risk	- Funding sources and liquidity positions - Asset-liability matching - Cash flow forecasting - Short-term liability over-reliance

Category	Subtopics
	- Illiquid asset concentration - Customer confidence erosion
Strategy and Business Environment Risk	- Strategic planning and alignment - Market share dynamics - Business model adaptability to changes - Adverse business decisions - Failure to respond to industry shifts - New product/service vulnerabilities
Operational Risk	- Fraud prevention and follow-up effects - Documentation and compliance with terms - Total process monitoring and follow-up - Accounting system balancing (manual/computerized branches) - Anti-money laundering related issues - Customer service operations - System failures/interruptions - Human errors in transactions
Market Risk	- Equity market unpredictability - Commodity price fluctuations - Interest rate volatility - Credit/Investment spread changes - Foreign exchange exposure
Technological Risk	- Cybersecurity and Data Privacy Risks - IT Infrastructure and Operational Risks - IT Governance and Change Management - Third-Party and Supply Chain Risks - Emerging Technology Risks
Environmental/ Climate Risk	- Financial impacts of acute weather events - New environmental mandates that increase operating costs - Environmental events' transition into bank's core risk, etc.
Money Laundering and Terrorist Financing Risk	- Customer Risks - Products or Services Risks - Business Practices and/or Delivery Method Risks - Country or Jurisdictional Risks
Legal or Regulatory Risk	- Changes in Regulatory Requirements - Contractual Disputes - Litigation Risk - Geopolitical and Sanctions Risk

Category	Subtopics
Internal Factors Influencing Business Risk	- Complexity of the organization structure - Nature of the bank's activities - Quality of personnel - Organizational changes - Employee turnover - IT system reliability - Process inefficiencies
External Factors Influencing Business Risk	- Fluctuating economic conditions - Changes in the industry - Socio-political realities - Technological advancements - Changes in rules and regulations - Geopolitical tensions - Pandemic or natural disaster impacts

3.2.2. Control Risk

Control risk arises when the bank's internal control systems fail to prevent, detect, or correct a material misstatement or operational issue in a timely manner. Such failures may not be violations of law yet are essential to effective governance and operational integrity. In practice, inadequate segregation of duties, poor vendor oversight, or insufficient monitoring of IT systems can elevate control risk. Internal audit often assesses this risk through structured departmental checklists and focused reviews on compliance, fraud prevention, and IT governance.

A list of topics which can be added to the Control Risk analysis is given below. They are based on samples emphasizing control weaknesses not backed by law but essential for operations, with a focus on monitoring, compliance, and mitigation. (This is a sample list Banks may add more topics to the category for better risk analysis):

Category	Subtopics
Credit/Investment Control	- Follow-up and monitoring - Credit/Investment review, renewal, time, and control - Non-performing asset/special mention account (NPA/SMA) management - Monitoring of NPA quality - Recovery from NPA (including rescheduling/waiver of interest) - Level of SMA - Collateral management weaknesses - Credit/Investment approval overrides
Internal Control	- Business lines (deposit, collection, remittance, fee-based services) - Agency and other fiduciary services - Back-up operations

Category	Subtopics
	- Branch cash/petty cash management - Security forms and protective arrangements - Branch documents, records, and stationery - Control systems (e.g., AC system balancing, office accounts follow-up) - Branch control functions - Submission of periodical returns - Letter receiving and disposal - General administration and staff matters - Premises and furniture maintenance - IT access controls and disaster recovery - Dual approvals for transactions
Compliance Control	- External compliance requirements - Follow-up on audit reports - Regulatory examination results - Industry trends and environmental factors - Anti-money laundering (AML) procedures - Consumer protection policies - Data privacy (e.g., GDPR equivalents)
Management and Operational Control	- Substantial performance variations from budget - Time elapsed since last audit - Proposed changes in business lines or focus - Significant changes in management/key personnel - Reports of external auditors - Results of latest regulatory examination - Vendor management and third-party oversight - Cybersecurity incident response - Business continuity planning
Risk Recognition and Assessment	- Breach quantification (e.g., percentage of breaches as low/medium/high) - Magnitude of breaches in value terms - Linking breach levels to risk matrices - Awarding scores based on risk levels (e.g., maximum marks for low/good, medium/satisfactory, high/weak/poor) - Impact and probability evaluation (e.g., before/after mitigation) - Scenario analysis for emerging risks
Off-Site and On-Site Control Assessment	- Preparation of branch/activity profiles - Collection of data from previous audits, compliance reports, and changes - Determination of inherent business and control risk levels - Surprise checks and on-site observations - Continuous monitoring tools (e.g., data analytics)

3.2.3. Detection Risk

Detection risk is the risk that audit procedures themselves fail to identify a material misstatement or weakness in a process, account balance, or transaction. Even if inherent and control risks exist, the auditor must design procedures to minimize the possibility of missing them. In internal audit, this is addressed through tailoring methodologies—such as employing data analytics, surprise checks, and deeper substantive testing—aligned with IIA Standard 2300: *Performing the Engagement*.

3.3. Risk Assessment Process and Matrix

The risk-based approach involves identifying the audit universe, assessing entities based on risk categories, scoring factors, and prioritizing audits. A risk assessment matrix can be used to evaluate business and control risks by combining probability (likelihood of occurrence) and impact (severity of consequences). This 3x3 matrix combines **Probability** (likelihood of control failure, post-mitigation) and **Impact** (potential financial/operational harm) to determine overall assessed risk level. This matrix is a generalized guide, which can be customized by the banks to suit their own risk profile. A sample of Risk Assessment Matrix is provided in **Annexure-A**.

3.4. Branch Audit Risk Rating

The branch audit rating has to be done on the basis of the scoring arrangement stipulated in **Annexure-B**. The risk assessment by Internal Audit focuses more on compliance with regulatory requirements; controls over implementation of management policies, procedures and decisions related to the risks which were communicated and asked to enforce along with all other risks at branch level.

3.5. Risk Based Audit Plan

To arrive at the decision of Risk Based Audit planning, Rating may be defined from the below mentioned parameters:

Risk grading / Rating of Business Units:

SL	Risk grading Event	Particulars	To be scored by	Total Score	Weight	Score availed	Weighted score
1	Branch rating Sheet	Branch Rating as per ICC Guidelines	Audit Unit/Div				
2	Pre-audit - Control Functions	DCFCL	Monitoring Unit/Div				
		QOR					
		IDCL/LDCL					
3	AML Score	Independent Testing Procedures	Audit Unit/Div				
4	Risk Based Internal Audit (RBIA)	Comprehensive Audit on seven core risk of the branch	Audit Unit/Div				
5	Post-audit - Compliance	Compliance on latest internal audit report	Compliance Unit/Div				
		Bangladesh Bank Inspection/ other regulatory audit/ external audit compliance					

Based on the risk grading/ rating of the business units, the audit plan/frequency may be determined follows:

Percentage of Score	Risk Level	Audit Frequency
From 0.00% to 40%	Low	Yearly
From 40.01% to 60.00%	Moderate	Yearly
From 60.01% to 80.00%	Above Average	Half-yearly
From 80.01% to 100.00%	High	Quarterly

Chapter 4: Risk Based Internal Audit (RBIA)

Comprehensive risk-based planning helps the internal audit in aligning and focusing its limited resources to produce insightful, proactive, and future-focused assurance and advice. Advanced planning is required to ensure that the internal audit priorities are risk-based, and the HoIA is responsible for developing a plan of internal audit engagements based on a risk assessment performed at least annually.

Risk-based internal audit plans should be dynamic and agile. To achieve those qualities, the internal audit plan may be updated quarterly (or a similar periodic schedule), or make the plans to be "rolling," subject to minor changes at any time.

4.1. Development of Annual Risk-Based Audit Plan (RBAP)

a. Annual Risk-Based Audit Plan (RBAP):

- Internal audit engagements shall be executed under a Risk-Based Audit Plan (RBAP), with focus on inherent and control risks, legal/regulatory compliance, and organizational objectives. Each year, the Head of Internal Audit (HoIA) shall prepare a Risk-Based Audit Plan (RBAP) covering the full audit universe (branches, units, business lines, processes, IT systems, Shariah governance, agents, outsourced activities, and subsidiaries). The plan shall be based on a documented risk assessment considering inherent risk, control effectiveness, regulatory priorities, and emerging risks (e.g., cyber, fraud, third-party, ESG etc.).
- Requirements of Internal audit given by the Supervisory Policy and Coordination Department (SPCD) or any other Bangladesh Bank regulation and coverage of External Auditor as stipulated in Bank-Company External Audit Rules, 2024 issued by the Banking Regulation and Policy Department (BRPD) or any changes thereon must also be taken into consideration in preparing the RBAP.

b. Prioritization & Coordination: High-risk and sensitive areas shall be given priority. Coordination with other assurance functions (e.g., compliance, risk management, external audit etc.) shall be ensured to avoid duplication of audit coverage**.**

c. Dynamic Review: The RBAP shall be dynamic, reviewed at least quarterly and adjusted/updated promptly for material events (e.g., when new risks, regulatory changes, frauds, or significant control failures etc. emerge**)**.

4.2. Risk-Based Audit Plan (RBAP) Process

a. **Risk assessment:** The Risk-Based Audit Plan (RBAP) process shall be grounded in a documented risk assessment process that consists of two phases: the assessment of business and control risk**.**

b. **The first phase, assessing the business (inherent) risk focuses on:**
   - Identification of the auditable units**;**
   - Defining the risk criteria;
   - Construction of a risk model/scoring; and
   - Ranking the auditable units.

c. **The second phase, assessing the control risk focuses on:**
   - Identifying control weaknesses, and typical failure scenarios, incorporating inputs from senior management, risk and compliance functions, and prior audit results.
   - The output shall drive prioritization and resource allocation.

d. **Approval by Audit Committee of the Board:**
   - The HoIA shall submit the RBAP, along with methodology, resource needs, and assurance coverage to the ACB for review and approval.
   - ACB approval for next year must be completed by September of current year so that there is time to arrange necessary resourcing and logistics.
   - Any material plan changes and resource constraints shall be reported to the ACB for approval**.**

e. **Use of Technology:** The RBAP should leverage data analytics and technology for continuous auditing and monitoring where feasible.

4.3. Formation of Audit Team

a. **Risk-based team composition, alignment with unit complexity:** Audit teams shall be constituted based on the risk profile, size, complexity, and nature of operations of the unit under review.

b. **Inclusion of subject matter experts:** Teams must include members with appropriate knowledge, & skills and professional expertise relevant to the area they are auditing (e.g., treasury experts for treasury audits, IT experts for IT audits). They must be trained on relevant laws, regulations (e.g., BB circulars, AML/CFT acts), and the bank's internal policies. Where required, subject matter experts may be co-opted.

c. **Auditor's ethics and integrity:** All auditors shall adhere to the highest standards of ethics, integrity, and professional objectivity as per the Auditor's Code of Ethics.

d. **Surprise/quality checks by senior auditors**: Senior internal audit officials may conduct surprise reviews or quality checks during fieldwork, particularly for high-risk or large units, to ensure audit quality and independence.

4.4. Execution of the Internal Audit Engagement

4.4.1. Selection of Audit Unit

a. Audit units shall be selected from the approved Risk-Based Audit Plan (RBAP).
b. Ad-hoc selection is permitted where technical need, emerging risk, regulatory direction, management/ board request or credible intelligence (e.g., whistleblower/fraud tip etc.) warrants immediate coverage.
c. The audit universe shall be reviewed periodically to reflect operational and regulatory changes.

4.4.2. Scope and Coverage

a. For each engagement, the internal audit team shall define auditable areas, objectives, period under review, and materiality thresholds.
b. Scope shall be risk-focused and proportionate to unit complexity and exposure.
c. Management input may be obtained but must not constrain independence.

4.4.3. Preparatory Work

Prior to fieldwork, the auditor shall:

a. Engagement Letter: issue an engagement letter/notification to the audit unit stating objectives, scope, timing and staffing;
b. Entrance Meeting: hold an entrance meeting with the leadership team of the audit unit to align expectations and gather preliminary concerns; and
c. Gather Information: obtain documentation and review key information to tailor the audit program, such as:
- organization chart,
- job descriptions,
- policies,
- procedures,
- process flows,
- MIS/statistical data,
- departmental reports,
- prior audit reports, etc.

4.4.4. Fieldwork and Evidence Gathering

a. Fieldwork shall be conducted using structured audit programs.
b. Auditors must obtain sufficient, relevant and reliable evidence (documents, system extracts, observations, interviews, analytic results etc.) to support their audit findings. Use of data analytics, sampling and inquiry should be documented.

4.4.5. Testing of Controls (Preventive, Detective, and Corrective Controls)

a. **Design Effectiveness Testing (DET):** Evaluate if the controls, as designed, are capable of effectively preventing or detecting errors or fraud. This is a prerequisite for operating effectiveness testing.
b. **Operating Effectiveness Testing (OET):** Perform testing to determine if the controls are operating as designed and throughout the period under review. Methods include:
   - **Inquiry**: Seeking information from knowledgeable persons.
   - **Observation**: Looking at a process or procedure being performed.
   - **Documentation Review:** Examining policies, procedures, transaction records, reconciliations, exception analysis, tangible assets, minutes of meetings, and other relevant documentations.
   - **Re-performance**: Independently executing the control procedure.
   - **Data Analysis**: Mandate the use of Artificial Intelligence (AI) or Computer-Assisted Audit Techniques (CAATs), or use Spreadsheets in case of unavailability of a CAAT tool, to analyze the entire populations of data for anomalies, trends, exceptions, and control overrides. This includes tools for data extraction, scripting, and visualization.
c. **Previous issues:** Auditors shall take special consideration of previous issues/ findings from IA/ Bangladesh Bank/ External Audit on the audit unit or any other part of the bank but relevant for the current audit.
d. **Fraud Indicators:** Auditors shall remain alert to red flags such as override of controls, unusual transactions, or dual credential misuse. In cases of suspected fraud, enhanced procedures shall be applied to preserve evidence and escalate per policy.

4.4.6. Sampling Techniques

Internal auditors do not typically examine 100% of a population of items. Instead, they use audit sampling, which is the application of an audit procedure to less than 100% of the items within a population to obtain and evaluate evidence about some characteristic of the population, thereby forming a conclusion about that population.

- Sampling must be risk-based, focusing on areas with the highest potential for material misstatements, fraud, or regulatory non-compliance.
- The sample size and method must be adequate and representative to provide sufficient and appropriate audit evidence.
- Sampling approach must be documented in audit working papers, including rationale, methodology, and limitations.
- Appropriate Risk-Based Sampling statistical or judgmental sampling techniques shall be adopted based on risk assessment and experience.

4.4.7. Working Papers / Documentation

a. All audit work shall be recorded in working papers that support conclusions and recommendations.
b. Working papers must include, at least, following documents:
   - engagement letter;
   - risk assessment planning;
   - audit program/methodology;
   - audit evidence;
   - interview memos;
   - exception listings;
   - working calculations;
   - reviewers' notes;
   - justification for any modification of findings;
   - formal recording of exit meetings;
   - audit findings and recommendations, etc.
c. Documentation must be indexed with professional standards and organized in a way that enables supervision, quality review and external assessment.
d. The audit files are to be securely stored and retained permanently as per Bank Companies Document Preservation Rules, 1993.

4.4.8. Establishing Findings and Corrective Actions

a. Prior to, during and after the fieldwork, audit team will issue draft findings along with root cause as and when they can identify issues. They shall give specific time to the Audit Unit to confirm factual accuracy of the draft findings, additional information/ material to support it's position related to the findings. Audit team may drop or modify the findings based on the inputs from audit unit.
b. Audit team shall rate individual findings and the total audit. They shall engage seniors within Internal Audit where required. Audit team leader shall review all ratings.

4.4.9. Audit Exit Meeting

Upon completion of the fieldwork, an audit exit meeting shall be held with the leadership/management team of the audited unit to discuss the preliminary findings, recommendations, and potential action plans.

4.4.10. Reporting of Audit Findings/Lapses

a. Internal audit reports shall be prepared promptly (within 15 working days of fieldwork completion, unless urgent escalation is required).
b. A formal, written audit report shall be issued for each engagement upon completion of fieldwork. The report must be accurate, objective, clear, concise,

constructive, and timely.

c. The report shall state the scope, objectives, and period of the audit. It must include:
   - **Criteria**: The standard, policy, or law used for the evaluation.
   - **Condition**: The factual evidence of what was found.
   - **Cause**: The root reason for the discrepancy between the condition and the criteria.
   - **Consequence**: The risk or impact of the condition.
   - **Classification**: The risk classification of the audit findings/lapses based on severity.
   - **Auditor's Recommendation**: Proposed actions to resolve the issue and improve processes.
   - **Management Action Plan**: Management's response and action plan, including action owner and realistic timelines for completion.
d. A graded opinion on the overall control environment (e.g., Satisfactory, Needs Improvement, or Unsatisfactory) shall be included.
e. All findings must be logged in a tracking system and followed up until closure.
f. **Low and medium risk** findings shall be reported to relevant management (Branch/Unit Head, with copy to Line Management, including relevant MANCOM/SMT) for corrective action.
g. **High and Critical risk** findings will be reported to relevant management for corrective action, and escalated to MD/CEO and ACB with recommended corrective actions and timelines. Significant findings such as fraud or other illegal activity, control weaknesses, or non-compliance shall be escalated directly to the ACB immediately for appropriate action. The status such findings shall be tracked and reported to ACB until closure.

4.4.11. Classification of Audit Findings/Lapses

a. Audit findings shall be classified by severity based on impact, likelihood, regulatory sensitivity and reputational effect.
b. Based on severity of the lapses, audit findings shall be classified into following 4 (four) groups:
   - Low Risk,
   - Medium Risk,
   - High Risk, and
   - Critical Risk.
c. Auditors shall record facts and evidence supporting classification, which shall guide escalation, recommended actions and disciplinary referral.

4.5. Quality Assurance and Improvement Program (QAIP)

a. **Objective:** The QAIP provides a formal structure to safeguard the Internal Audit Function's independence and objectivity, ensuring all work meets the high-quality benchmarks set by IIA Standards.

b. **Components of QAIP:** The QAIP shall include both **internal** and **external assessments**, covering:

   i. **Ongoing Monitoring:** Conducted continuously as part of day-to-day operations:
      - Supervision and review of audit engagements.
      - Use of standardized audit methodologies and checklists.
      - Monitoring of KPIs (e.g., timeliness, coverage etc.).
      - Real-time feedback from auditees and stakeholders.

   ii. **Periodic Internal Assessments:** Performed at defined intervals (e.g., annually) by senior audit staff independent of the work being reviewed:
      - Self-assessment against conformance with Bangladesh Bank's guidelines, the Internal Audit Charter and auditor's Code of Ethics.
      - Peer reviews peer working papers within the audit unit.
      - Thematic reviews of audit quality and documentation.
      - Identify improvement opportunities and training needs.
      - Reporting of results to the HOA/CAE, HOICC and ACB.

   iii. **External Assessments:**
      - Independent assessment by a qualified external reviewer or team at least once every five years.
      - External assessors to be approved by the ACB in consultation with the HoIA.
      - Scope includes conformance with Bangladesh Bank's guidelines, the Internal Audit Charter and auditor's Code of Ethics and stakeholder feedback.
      - Reporting of results to the ACB.

c. **Scope of QAIP:** The QAIP must evaluate:
   - All internal audit activities, including assurance and concurrent audit function.
   - Conformance with Bangladesh Bank's guidelines, and auditor's Code of Ethics, and may also cover IIA Audit Standards.
   - Adequacy of audit planning, risk coverage, and execution.
   - Quality and timeliness of reporting.
   - Staff competency, independence, and ethical standard of the internal audit function.
   - Stakeholder satisfaction (Board, Management, Regulators).

d. **Reporting & Accountability:**
   - Results of QAIP assessments (internal & external) shall be reported to the ACB.
   - Significant deficiencies and improvement plans must be disclosed, along with timelines for remediation.
   - ACB shall review the outcomes of the QAIP process and monitor the implementation of corrective actions, ensuring sustained support from senior management

- A summary of QAIP results (internal & external) shall be included in the Annual Assurance Report submitted by the HoIA.

e. **Continuous Improvement:**
   - The Internal Audit Function must adopt structured processes for root cause analysis of the identified deficiencies.
   - Audit methodology, technology enhancements, resource allocation and training plans must be undertaken based on QAIP findings.
   - Lessons learned from QAIP outcomes must be incorporate into future audit cycles.
   - Best practices from global standards and peer banks shall be periodically integrated based on availability.

4.6. Annual Assurance Report on the Bank's Control Environment

4.6.1. The HoIA shall submit an annual assurance report to the Board of Directors, through the ACB. This report shall provide an independent opinion on the adequacy and effectiveness of the bank's governance, risk management, and internal control environment, based on the year's audit results, risk assessment, and may include input from other assurance providers (e.g., compliance, risk management, external audit etc.).

4.6.2. The assurance must be supported by sufficient and appropriate audit evidence gathered during the year. It must consider the control environment across all material legal entities, products, functions, and processes, including outsourced activities.

4.6.3. The report shall include, at a minimum:
   - The scope of internal audit work performed and risk coverage.
   - A summary of significant control deficiencies identified during the period, along with the status of management's corrective actions.
   - An assessment of the bank's response to emerging risks.
   - A summary of the results of the Internal Audit Function's Quality Assurance and Improvement Program (QAIP).
   - The annual internal audit plan and a statement on whether the function operated with adequate resources and with independence in accordance with the Internal Audit Charter.
   - Any limitation in scope, access, or resources that may affect the reliability of the assurance.

4.6.4. The report shall be reviewed by the ACB and submitted to the Board for approval.

Chapter 5: Compliance

5.1. Regulatory Compliance

Compliance refers to operating the bank in conformance with all applicable laws, regulations, circulars, policies, standards, guidelines, and codes of conduct, both domestic and international. It includes timely and effective responses to supervisory criticism, inspection observations, and corrective directives issued by regulators or law enforcement agencies.

Compliance also encompasses preventive and risk-based measures to mitigate compliance risk. Compliance risk is the risk of legal or regulatory sanctions, material financial loss, reputational damage, customer harm, or systemic risk arising from failure to comply with applicable requirements.

5.2. Regulatory Compliance Environment

For the banks, Bangladesh Bank is the primary regulator which governs their activities. Besides, regulators are also defined as National Board of Revenue (NBR), Registrar of Joint Stock Companies and Firms (RJSC), Bangladesh Securities and Exchange Commission (BSEC), Ministry of Finance, Ministry of Commerce, Ministry of Environment, Ministry of Home Affairs, Bangladesh Financial Intelligence Unit (BFIU), whose directives have a significant impact on any bank's business.

To ensure effective compliance:

a. Each bank must maintain a comprehensive and up-to-date inventory of regulatory obligations covering domestic and cross-border requirements.
b. Banks must establish processes for timely monitoring, dissemination, and implementation of regulatory updates across all relevant functions.
c. Compliance must be embedded into all operations and supported by automated monitoring systems where feasible.
d. Banks should adopt a Compliance Risk Management (CRM) framework that includes:
    - ✓ Annual enterprise-wide compliance risk assessments;
    - ✓ Defined remediation timelines;
    - ✓ Escalation procedures for unresolved issues; and
    - ✓ Independent monitoring and reporting to senior management and the Board.

5.3. Compliance Risk Management (CRM) Framework

5.3.1. Objective:

The primary objective of the Compliance Risk Management (CRM) framework is to ensure that all banks operating in Bangladesh establish a robust, independent, and effective framework designed to manage the bank's exposure to compliance risk by ensuring adherence to all applicable laws, regulations, internal policies, and codes of conduct, thereby safeguarding the bank's reputation, financial soundness, and the interests of its stakeholders.

5.3.2. Guiding Principles:

The Compliance Function and its framework shall be guided by the following principles:

- ✓ **Independence:** The function must operate independently from the business units it oversees.
- ✓ **Integrity:** It shall perform its duties with the highest degree of professional integrity and objectivity.
- ✓ **Proactivity:** It shall adopt a forward-looking approach to identify, assess, and mitigate emerging compliance risks.
- ✓ **Proportionality:** Its scope, resources, and activities shall be based on a comprehensive risk assessment.
- ✓ **Integration:** Compliance risk shall be integrated into the bank's overall Enterprise Risk Management (ERM) system.

5.3.3. Consideration for Developing the CRM

5.3.3.1 The BoD shall ensure tone-from-the-top that promotes honesty, integrity, and compliance culture.

5.3.3.2 The ACB, on behalf of the Board, shall review the comprehensive compliance report from the HoC at least quarterly.

5.3.3.3 A whistleblowing mechanism shall be established and be operational effectively and free from retaliation.

5.3.3.4 The senior management shall be responsible for implementing the compliance framework as approved by the Board.

5.3.3.5 Timely and unrestricted flow of information to the Compliance Function shall be ensured.

5.3.3.6 Significant compliance breaches must be immediately reported to the Board or ACB if there is a significant risk of legal or regulatory sanctions or fines, financial loss, or loss to reputation.

5.3.4. Functioning of the CRM Framework

Banks must establish a formal, documented, and dynamic Compliance Risk Management (CRM) Framework consisting of following elements:

5.3.4.1. Compliance Policy:

The Board must approve a comprehensive policy that defines the mandate, authority, independence, and structure of the Compliance Function.

5.3.4.2. Compliance Risk Assessment (CRA):

A bank-wide CRA must be conducted at least annually to:

- ✓ Identify inherent compliance risks across all material business activities, products, and geographies.
- ✓ Assess the effectiveness of existing controls.
- ✓ Determine the level of residual risk.
- ✓ Prioritize resources and inform the annual Compliance Monitoring Plan.

5.3.4.3. Compliance Monitoring Program (CMP):

The HoC must develop a risk-based CMP derived from the CRA. The program must include a schedule of ongoing and periodic reviews to test the design and operating effectiveness of key controls. Findings must be documented, reported to management for corrective action, and tracked to resolution.

5.4. Core Compliance Processes

5.4.1. Regulatory Change Management:

Banks must implement a formal process to:

- ✓ Identify and track new and amended laws and regulations.
- ✓ Assess the impact of these changes on the bank's operations.
- ✓ Disseminate information to relevant business units.
- ✓ Ensure necessary policies, procedures, and systems are updated to implement changes.

5.4.2. Advice, Guidance & New Product Approval:

The Compliance Function must be consulted and provide written approval on all new products, processes, and major strategic initiatives before their launch to ensure compliance risks are identified and mitigated at the design stage.

5.4.3. Training & Awareness:

The Compliance Function, in conjunction with Human Resources, must develop and deliver a mandatory, role-based compliance training program. The program's curriculum must be based on the CRA, and its effectiveness must be measured and reported.

5.4.4. Reporting:

The HoC must provide comprehensive reports to the ACB and Senior Management at least quarterly. Reports must include:

- ✓ Summary of monitoring and testing results.
- ✓ Status of regulatory changes and implementation.
- ✓ Details of any material compliance breaches and corrective actions.
- ✓ Assessment of the overall health and effectiveness of the CRM Framework.

5.5. Tracking, Validation, and Settlement of Audit Observations

Banks must maintain a structured and risk-based process for the settlement and closure of audit, inspection, and compliance files.

a. **Observation Logging & Tracking:**
   i. **Centralized Register:** The HoC is responsible for maintaining a centralized audit/inspection observation tracking system/register. This system shall be a dynamic tool that tracks all audit findings from issuance to closure.
   ii. Each observation must have:
      - A unique identifier,
      - Risk classification (e.g., critical, high, medium, low),
      - Required corrective action(s),
      - Responsible owner (management), and
      - Target completion date.
   iii. Tracking must cover all levels: audit engagement-level findings, recurring issues, regulatory lapses, and fraud-related cases.

b. **Management's Responsibility:**
   - Management is primarily responsible for designing and implementing corrective actions.
   - Action plans must be specific, measurable, achievable, realistic, and time-bound (SMART).
   - Updates on progress must be provided to HoC periodically (e.g., monthly/ quarterly).

c. **Compliance Function's Role in Follow-Up:**
   - **Monitor and Track:** Compliance function must continuously track status through the observation tracking system.
   - **Validate:** For each reported "closed" observation, compliance staff shall verify closure by:
      - Reviewing documentary evidence,
      - Forward the internal audit observations to the respective internal audit team for performing re-tests of controls to validate closure, and
      - Conducting discussions with process owners.

- **Partial Closure:** If corrective actions are incomplete, compliance function may accept partial progress but keep the issue "open" until full mitigation is achieved.

d. **Escalation & Reporting:**
   - Unresolved or overdue high-risk observations must be escalated to senior management and the ACB.
   - Periodic reports (monthly/quarterly) should highlight:
     - Open issues by risk rating,
     - Ageing of open observations,
     - Overdue actions vs. agreed timelines, and
     - Repeat findings indicating systemic weaknesses.

e. **Closure Criteria:**
   - An audit/inspection observation may be considered closed only if:
     - The corrective action has been implemented as agreed,
     - Internal audit's validation testing confirms that the risk is mitigated, and
     - No further significant residual risk remains.
   - For critical/high-risk observation, closure must be formally confirmed by the HoIA and reported to the ACB.

5.6. Settlement of Commercial Audit Objections

Commercial audit objections may be settled through the following processes:

a. **Spot Rectification:** Certain irregularities can be corrected immediately during the course of the audit. The audit team must ensure such rectifications are carried out on the spot and record them in the audit report.

b. **Discussion Meeting:** On the closing day of the audit, a meeting must be held between the branch head and the audit team. Some irregularities may be resolved through this discussion.

c. **Post-Audit Settlement:** Audit objections are classified into two categories:
   - Ordinary (Normal) Objections and
   - Advance (Serious) Objections.

   i. **Settlement of Ordinary (Normal) Objections:**
      - Settled upon submission of written evidence of corrective action by the bank, supported by appropriate documents.
      - If the auditor is not satisfied, a bi-party meeting (auditor and bank) will be held for further review.
      - Upon satisfactory resolution, the auditors will issue an office order confirming settlement.

ii. **Settlement of Advance (Serious) Objections:**
   - Require written confirmation by the bank of corrective action with supporting documents such as vouchers, account statements, or compliance report.
   - If auditors remain unconvinced after the stipulated period, a tri-party meeting (auditor, bank, and relevant authority) will be convened.
   - Upon satisfactory resolution, the auditors will issue an office order confirming settlement.

5.7. Settlement of Inspection Objections of BB and Other Regulators

Settlement of inspection objections raised by Bangladesh Bank and other regulators shall follow the procedures below:

a. **Corrective Action and Documentation**
   - Branches must take corrective actions and submit compliance reports, duly signed by the Branch Manager and countersigned by the Zonal Head and Circle Head (as applicable).
   - The Compliance Unit will review the evidence and determine whether the objection can be formally closed.

b. **Transfer of Previous Objections**
   - If unresolved objections are found and reported again in the current inspection report, they will be carried forward automatically and the earlier file considered closed.

c. **Settlement of Long-Standing Objections**
   - For long outstanding objections, the Compliance Unit will arrange meetings with the concerned regulator and the bank's senior management.
   - During these meetings, some objections may be resolved while others may require further review.
   - If the regulator is not satisfied, it will issue a re-notice for the unresolved objections.
   - The Compliance Division must promptly communicate the status of resolved and unresolved objections to the concerned branches.

d. **Periodic Review Meetings**
   - A periodic meeting with Bangladesh Bank and other regulators may also be held to review the status of corrective actions and ensure timely resolution.

Chapter-6: MIS, Data Analytics and Monitoring

This chapter outlines the framework for the ongoing monitoring, independent evaluation, and timely correction of control deficiencies to ensure the internal control system remains robust and effective in mitigating the bank's risks.

6.1. Ongoing Monitoring Activities by the Business Units (First Line):

The First Line of Defense owns and is responsible for the continuous monitoring of risks and controls within its operations. This ongoing monitoring must be embedded in daily activities and involves the regular use of key control tools to verify that processes are operating as intended and in compliance with established policies. The primary control tools for this purpose include, but are not limited to, the followings:

6.1.1. Departmental Control Function Checklist (DCFCL): Annexure-C

- DCFCL deals with matters relating to review/verifications of departmental functions to ensure that prescribed procedures are being followed by each branch/unit.
- All departments/units, in collaboration with Monitoring Division, shall identify all critical and high-risk items within each unit's operations and prepare a risk-based DCFCL accordingly. The DCFCL must be reviewed and updated annually, or whenever there are significant changes to products, processes, or systems.
- Department Heads and Branch Managers must complete the DCFCL at prescribed frequencies (daily, weekly, monthly, quarterly) to verify that all mandated procedures and controls are functioning as intended.
- Each branch/unit must submit the completed checklists to the Monitoring Division by the 5th of the following month and retain a copy for on-site review by the Monitoring Division and the Audit Team.

6.1.2. Quarterly Operations Report (QOR): Annexure-D

- QOR relates to reporting of operational functions of each branch/sub-branch under the following headings on the prescribed format:
  - ✓ Policies, Procedures and Controls
  - ✓ Protection of Valuables
  - ✓ Proofs/Verifications and Internal Checks
  - ✓ Personnel and Supervision
  - ✓ Premises Management
  - ✓ Confirmation on Regulatory Compliance
- Each branch/sub-branch must prepare and submit a QOR to its Line Manager and the ICC Monitoring Unit by the 10thof the month following each quarter.
- The items which are not applicable for a branch/sub-branch should be marked as N/A.
- Any deviations must be detailed in a separate Exception Report.

6.1.3. Loan Documentation Checklist (LDCL): Annexure-E

- For every credit facility, branches/units must complete the LDCL to ensure all security documentation and legal formalities are perfected to safeguard the bank's interests.
- On a quarterly basis, a copy of the completed LDCL must be submitted to the Monitoring Division by the 10th of the month following each quarter.

6.1.4. Concentrated Credit Exposure Dashboard:

- Banks should prepare a live dashboard that aggregates exposure to a single borrower, connected group, industry, or geographic region to oversee credit concentration risk.
- Flags should be raised when single borrower exposure limits or internal concentration limits are in breach, alerting the Senior Management Team to justify and mitigate any over-exposure.
- On a monthly basis, reports on breaches of single borrower exposure limit and internal concentration limits must be submitted to the Monitoring Division by the 5th of the following month.

6.1.5. Trade-Based Money Laundering (TBML) Red Flag Analyzer:

- Banks should analyze data from Letters of Credit/Documentary Credit, bills of lading, and invoices to flag discrepancies such as over/under-invoicing, mis-description of goods and cross-reference parties involved with global sanctions lists and adverse media.
- Alerts should be generated to freeze the transaction and file a Suspicious Transaction Report (STR) with the regulator.
- On a monthly basis, list of Alerts must be submitted to the Monitoring Division by the 5th of the following month.

6.1.6. LC & Guarantee Expiry and Exposure Tracker:

- Banks should develop calendar to track all contingent liabilities to proactively alert the business units 15 days before a large LC or guarantee is set to expire, allowing for client engagement on renewal.
- The calendar should also monitor the utilization of approved limits to prevent excess over limit.
- On a monthly basis, list of expired contingent liabilities and excess over limit must be submitted to the Monitoring Division by the 5th of the following month.

6.1.7. Real-Time Value at Risk (VaR) & Limit Breach System:

- Banks should develop a system integrated with the treasury trading platform to calculate the bank's potential loss (VaR) based on its trading portfolio and market volatility.
- The system should also be capable to monitor dealer-level and bank-level limits for various products (FX, bonds, derivatives).

- The system should be capable to automatically block a dealer's ability to trade the moment a risk limit is breached and send an immediate alert to the Head Dealer, Head of Treasury, and CRO, mandating a formal review and forced position reduction.
- On a monthly basis, calculated VaR and breach of dealer-limits must be submitted to the Monitoring Division by the 5th of the following month.

6.1.8. Counterparty Risk Re-Assessment System:

- Banks should develop a system to trigger a re-assessment of a counter-party's credit rating based on triggers like a downgrade by a credit rating agency, negative profit warnings, or significant adverse news.
- The system should be capable to automatically reduce the trading limit for a counterparty or requires additional collateral if their risk profile deteriorates.
- On a monthly basis, report on the reduction of counterparty limits due to downgrade of credit score, negative profit warnings, or adverse news must be submitted to the ICC Monitoring Unit by the 5th of the following month.

6.1.9. IT Project & Cyber Security Control Monitoring:

- Banks should effectively monitor IT project delivery and vendor performance to ensure that all third-party and internal IT projects deliver fit-for-purpose outcomes, and that payments are tied strictly to validated delivery milestones.
- Banks should maintain a Cyber-Security Control Effectiveness Dashboard under the Monitoring Division to continuously track the performance, uptime, and assurance of preventive and detective controls across all digital environments.
- The dashboard shall, at a minimum, include the following domains and indicators such as, Patch and Vulnerability Management, Endpoint Security and Malware Protection, Identity and Access Control, Network and Perimeter Defense, Phishing and User Awareness, Data Classification and Protection, Third-Party and Cloud Security, Incident Prevention and Response Readiness, etc.
- Unresolved critical vulnerabilities or systemic control failures exceeding a threshold, defined by the bank, must be escalation immediately to SMT for urgent attention and remediation.
- On a monthly basis, a report shall be submitted to the Monitoring Division by the 5th of the following month.

6.1.10. Self-Assessment Anti-Fraud Internal Control Checklist (SAAFICC):

- On a semi-annual basis, Department Heads and Branch Managers must complete this comprehensive checklist to proactively identify and assess vulnerabilities to fraud within their operations.
- The self-assessment must evaluate the design and operational effectiveness of controls related to Internal Control Management System (ICMS), General Banking & Operation,

Loans & Advances, Foreign Exchange Operation, and Information & Communication Technology (ICT).

- The completed checklist, in format prescribed by Bangladesh Bank, requires attestation by the respective head/manager and must be placed to the Monitoring Division for independent review and submission to Bangladesh Bank.

6.2. Independent Monitoring & Corrective Measures by C&M:

The ICMS Compliance and Monitoring Divisions (C&M) shall provide independent oversight of the Bank's Internal Control System. Its primary functions are to challenge the effectiveness of the First Line's controls, ensure enterprise-wide compliance, and drive the timely remediation of deficiencies. This is achieved through a structured framework of monitoring, validation, and escalation.

6.2.1. Development and Maintenance of the Monitoring Framework:

- The C&M is responsible for overseeing the development, updating, and validation of the key control tools (described under Section 6.1). This includes working with all business units to identify critical processes and risks, ensuring the monitoring tools are risk-based, comprehensive, and aligned with the Bank's evolving risk profile.

6.2.2. Monitoring of Control Tools:

a. **Routine Review:** Monitoring Unit will systematically review and validate the reports on the key control tools (described under Section 6.1 above) submitted by the Business Units (First Line) to assess the effectiveness of compliance and control functions across the bank.

b. **Validation of Controls:** Monitoring Unit will analyze and validate the reports on the key control tools, through onsite visit/offsite validation approach considering their available resources, to verify the first line's assessments, identify potential control gaps or underestimation of risks, and ensure the integrity and thoroughness of the control process.

c. **Monitoring of Regulatory Submissions:** Monitoring Unit will proactively monitor the timely and accurate submission of all regulatory returns, reports and correspondences to the Bangladesh Bank and other regulators as per the official calendar of returns and/or specific deadlines to avoid regulatory imposition.

6.2.3. Regulatory & Management Reporting:

a. **Risk-Based Analysis & Reporting:** Based on the activities in (a) through (c) under Section 6.2.2 above, the Monitoring Unit shall prepare a consolidated Quarterly Monitoring Report. This report must analyze findings thematically, highlight emerging risks, and prioritize issues based on their significance and potential impact

on the bank, containing at least the followings:

- ✓ Validation results of DCFCL;
- ✓ Validation result of the Quarterly Operations Report;
- ✓ Discrepancies in credit documentation from LDCL;
- ✓ Breaches of Concentrated Credit Exposure Dashboard;
- ✓ Summary of Alerts from the TBML Red Flag Analyzer;
- ✓ Summary of expired and excess over limits from the LC & Guarantee Expiry and Exposure Tracker;
- ✓ Analysis of VaR and breach of dealer-limits from the VaR & Limit Breach System;
- ✓ Summary of reduction of counterparty limits from Counterparty Risk Re-Assessment System;
- ✓ List of lapses and alerts from IT projects and Cyber Security Control Monitoring.

b. **Management Engagement & Escalation:** The significant findings of the Quarterly Monitoring Report shall be actively discussed with the Senior Management Team (SMT) to agree on corrective actions and accountability. A summary of the report, along with SMT's feedback and actions, must be presented to the ACB in each quarter.

c. **Submission of SAAFICC:** Monitoring Unit will ensure the timely submission of the bank's Self-Assessment Anti-Fraud Internal Control Checklist as per DOS Circular letter no.10 dated 09.05.2017 (or any subsequent instructions/circulars in this regard) to the Bangladesh Bank under signature by the MD/CEO and counter signature by the Chairman of the ACB.

6.2.4. Issue Management & Corrective Actions:

a. Upon identifying a deficiency, the Monitoring Unit shall instruct the responsible branch/unit to rectify the issue and provide evidence of the correction.

b. Based on the gravity of the deviation, the HoC may request the Audit Unit (Third Line) to conduct a specific audit.

c. The Monitoring Unit must report all material control deficiencies to the SMT immediately upon identification, and subsequently to the ACB on quarterly basis. The report to the ACB must include specific recommendations for resolution and a timeline for implementation. A deficiency is considered material if it is related to, or could lead to:

- ✓ Direct or indirect financial loss beyond a specific threshold defined by the bank's policy.
- ✓ Significant reputational damage.
- ✓ Potential license revocation or restrictive regulatory action.
- ✓ Major regulatory non-compliance.

6.3. Independent Assurance by Internal Audit (Third Line):

The Audit Unit shall validate the effectiveness of the internal control system through a program of routine and surprise audits, as per the risk-based audit plan. Its findings and assessments shall be reported directly to the ACB, providing independent assurance on the adequacy and effectiveness of the first and second lines of defense.

6.4. Annual ICMS Report on Health of the Bank

All banks are required to prepare an Annual Health Report for submission to the ACB, Bangladesh Bank, inspection teams, and other relevant regulatory authorities. This report, based on the most recent data, reflects the bank's financial, reputational, and sustainability position, providing stakeholders with a foundational understanding of the bank's general health. The objectives of the Health Report include: assessing bank soundness, informing stakeholders, guiding decision-making, ensuring compliance, enhancing transparency etc.

6.4.1. Methodology of Assessing Health

- **Data Collection:** Monitoring unit shall gather inputs from ECB (Financial Health), ACB (ICMS Health), and EA (Image & Reputation).
- **Scoring:** Each component is rated against defined parameters using a uniform scoring scale.
- **Risk Analysis:** Deviations from regulatory standards and internal benchmarks are highlighted.
- **Consolidation:** Component scores are combined into a composite health score.
- **Review:** Findings are validated by ICC/Internal Audit.
- **Reporting:** Final report submitted annually to Board Audit Committee, Bangladesh Bank, and regulators.

6.4.2. Sample Scoring Matrix:

Parameter	Weight (%)	Score Range	Rating	Interpretation
Financial Health	40%	90 and above	Excellent	Strong Capital, Profitability, Liquidity
		80-89	Very Good	Adequate, Minor Weaknesses
		70-79	Good	Minor Weaknesses
		60-69	Satisfactory	Weaknesses Requiring Corrective Action
		Below 60	Marginal	High Risk, Unsustainable Position
ICMS Health	35%	90 and above	Excellent	Strong ICC Framework, Full Compliance
		80-89	Very Good	Generally Compliant, Minor Gaps
		70-79	Good	Minor Gaps
		60-69	Satisfactory	Several Gaps, Corrective Action Needed
		Below 60	Marginal	Ineffective Controls, High Compliance Risk
Image & Reputation	25%	90 and above	Excellent	Strong Governance & Public Trust
		80-89	Very Good	Generally Positive, Minor Concerns
		70-79	Good	Minor Concerns
		60-69	Satisfactory	Notable Reputational Issues
		Below 60	Marginal	Poor Governance, Reputational Risk

A sample of Health scoring is given in **Annexure-F.**

6.4.3. Reporting Line and Approval Process

- The MIS, Data Analytics and Monitoring Division of ICMS shall be responsible for coordinating the preparation of the Annual Health Report (AHR).
- The draft report shall be reviewed internally by the HoC.
- Validation of accuracy and completeness shall be performed by the Internal Audit team to ensure conformity with Bangladesh Bank guidelines.
- Upon validation, the AHR shall be placed before the ACB for review and approval.
- After approval by the ACB, the report shall be formally adopted by the Board of Directors.
- The approved report shall be submitted to the respective Bank Supervision Department of Bangladesh Bank.

6.4.4. Follow-Up

- The MIS, Data Analytics and Monitoring Division of ICMS shall monitor the implementation of the recommendations included in the report.
- Progress updates shall be reported to the ACB on a periodic basis (at least quarterly) until full compliance is achieved.

Chapter 7: Shariah Audit

7.1. Introduction

Islamic banking in Bangladesh is conducted under the provisions of the Banking Companies Act, 1991 (as amended in 2023) and regulatory instructions issued by Bangladesh Bank. In addition to meeting general banking regulations, Islamic banks, Islamic banking windows, and units must operate in conformity with Shariah principles as endorsed by their respective Shariah Supervisory Committee (SSC).

To ensure compliance, ICMS functions must contain a dedicated Shariah Audit, which serves as an independent mechanism to verify that the bank's activities, contracts, and reporting remain consistent with Shariah principles. This requirement is reinforced by international standards, particularly the AAOIFI Governance Standard (GS) No. 11 on Shariah Review, which defines Shariah audit as a systematic examination of Islamic financial institutions' activities to ensure adherence to Shariah rulings and SSC guidelines.

Accordingly, this chapter provides the guiding principles, objectives, scope, methodology, and reporting framework for Shariah Audit within the ICMS structure, aligning Bangladesh Bank regulations with global best practices to strengthen governance, accountability, and trust in the Islamic banking system.

7.2. Risks and Consequences Related to Shariah Violation

7.2.1. Risks

Shariah compliance is a fundamental requirement in Islamic banking operations. Any violation exposes an institution to significant compliance, reputational, operational, and financial risks. Failure to comply with Shariah principles may result in the following adverse consequences:

- **Religious Non-Compliance:** Direct violation of the commands of Allah (SWT) and His Prophet (SM).
- **Loss of Barakah:** Banking activities may lose the spiritual value of *'ibādah* and be deprived of the blessing (*barakah*) of Allah (SWT).
- **Regulatory Breach:** Contravention of Bangladesh Bank's *Guidelines for Islamic Banking, 2009*, which may lead to supervisory or regulatory action.
- **Reputational Damage:** Erosion of the bank's image and credibility as a Shariah-based financial institution.

- **Contractual Invalidity:** Non-compliant agreements and their execution may render the contract null and void from a Shariah perspective. Any profit generated from such contracts would be considered non-halāl.
- **Income Purification:** Earnings derived from Shariah non-compliant transactions cannot be recognized as regular or halāl income. If such income is received unintentionally, it must be transferred to the bank's Corporate Social Responsibility (CSR) activities, as advised by the Shariah Supervisory Committee (SSC).

7.3. Areas of Shariah Inspection:

Shariah inspection ensures that all operations of Islamic banks and banking windows comply with Shariah principles, Bangladesh Bank regulations, and AAOIFI standards. The key areas include:

a. Product Structuring & Documentation

- Verify that all Islamic products (Murābaḥah, Ijārah, Mushārakah, Muḍārabah, Salam, Istisnā, etc.) are SSC-approved.
- Review contracts, agreements, and operational manuals for Shariah compliance.

b. Transaction Execution & Operations

- Sample-check transactions to ensure they follow approved Shariah structures.
- Avoid prohibited elements: riba (interest), gharar (excessive uncertainty), maysir (gambling), and harām activities.

c. Investment & Financing Portfolio

- Ensure investments and financing avoid non-permissible sectors.
- Review equity-based contracts (Mushārakah/Muḍārabah) and Ijārah agreements for Shariah compliance.

d. Profit Calculation & Distribution

- Examine profit-sharing ratios for fairness and transparency.
- Ensure non-halāl income, if any, is allocated to CSR or charity as per SSC guidance.

e. Governance & SSC Functioning

- Review independence, effectiveness, and implementation of SSC resolutions.
- Assess the Shariah governance framework within ICC and the bank.

f. Financial Reporting & Disclosures

- Ensure financial statements reflect only Shariah-compliant activities.
- Confirm disclosure of income purification and compliance with AAOIFI standards.

g. Internal Policies, Controls & Training

- Verify internal policies, manuals, and audit procedures align with BB guidelines and Shariah rules.
- Assess staff training programs on Shariah compliance.

7.4. Methodology of Shariah Audit

The Shariah Audit process shall include:

a. **Planning**

- Head of SSC/IAD prepares the annual Shariah Audit Plan.
- Plan shall be risk-based, prioritizing sensitive areas and branches/windows with higher Shariah non-compliance.
- The Plan shall be approved by the Member-Secretary of SSC with SSC concurrence.
- Review Bangladesh Bank circulars, SSC resolutions, and AAOIFI guidelines.
- Identify risk areas of potential Shariah non-compliance.

b. **Execution**

- Conduct field audits according to the risk-based schedule (High, Above Average, Moderate, Low).
- Inspect products, transactions, contracts, income streams, and operational processes.
- Deploy auditors with expertise in Islamic banking and ICT literacy.
- Perform surprise checks for branches/windows with recurring deficiencies.

c. **Evaluation**

- Compare actual practices against Shariah rulings, SSC decisions, and BB regulations.
- Identify non-compliance, weaknesses, or governance gaps.

d. **Reporting**

- Identify and document all deficiencies/non-compliance issues.
- Notify:
  - Appropriate branch/window management
  - Member-Secretary of SSC
  - Audit Committee of the Board (ACB)
  - MD/CEO (copy)
- At the end of each quarter, submit a summary report on findings and corrective measures to SSC, ACB, Board of Directors, and MD/CEO.

e. **Follow-up**

- Ensure management implements recommended corrective measures.
- Track and monitor recurring issues for continuous improvement.
- Reassess branch/window risk rating in subsequent audit cycles.
- Monitor continuous compliance and provide feedback to SSC and the Board.

f. Income Verification

- Verify at least a proportion of the branch/window's income, as decided by SSC/Shariah Board.
- Ensure non-compliant income is handled according to SSC guidance.

g. Continuous Improvement

- Update audit methodology and risk indicators regularly.
- Provide training to auditors to maintain compliance knowledge and ICT skills**.**

7.5. Shariah Non-Compliance Risk Rating:

7.5.1. Assign Scores

- Evaluate each branch based on operational performance and compliance indicators as per **Annexure-G**.
- Total possible score: 100 marks.

7.5.2. Category-wise Frequency of Shariah Audit

Score Range	Risk Category	Frequency of Shariah Audit
50.00 – 100.00	High Shariah Non-Compliance Risk	Twice a year
30.00–49.99	Above Average Non-Compliance Risk	At least once a year
15.00 – 29.99	Moderate Shariah Non-Compliance Risk	As decided by Shariah Board / SSC / ICMS
0.00 – 14.99	Low Shariah Non-Compliance Risk	As decided by Shariah Board / SSC / ICMS

7.6. Measures against Shariah Violation

- Shariah non-compliance shall be categorized into two types: Major Violations and Minor Violations **(Refer to Annexure-G for detailed classification)**
- All employees or units found responsible for Shariah violations, particularly major violations, must be sanctioned appropriately to reinforce a culture of compliance.

- Repeat offenders shall be subjected to stricter disciplinary measures to prevent recurrence and strengthen overall Shariah governance.
- These measures aim to ensure that the bank's operations remain fully aligned with Shariah principles and regulatory expectations**.**

7.7. Monitoring and Follow-up

- In line with the Banking Companies Act, 1991 (as amended), Bangladesh Bank's Guidelines for Islamic Banking, AAOIFI Standards, and IFSB Guiding Principles, each bank shall develop a comprehensive Shariah compliance checklist.
- The checklist shall cover both branch-level and Head Office-level operations to systematically monitor Shariah adherence.
- Findings from compliance and monitoring shall be submitted on a **quarterly** basis to:
  - ✓ Shariah Supervisory Committee (SSC)
  - ✓ Audit Committee of the Board (ACB)
  - ✓ Board of Directors
  - ✓ MD/CEO
- The quarterly reports shall include observations, corrective actions taken, and recommendations, enabling timely follow-up and continuous improvement in Shariah compliance.

7.8. Organizational and Professional Standards for Shariah Audit:

7.8.1. Independence & Organizational Structure:

- A fully Shariah based bank shall follow the organogram illustrated in the Chapter 2 of this guideline.
- The conventional banks having Shariah window shall establish separate functional units/departments under HoIA and HoC. Head of the Shariah audit function should report to the ACB / Shariah Supervisory Board (or equivalent), possibly through HoIA.

7.8.2. Fit & Proper / Qualifications

- The head of Internal Shariah Audit shall be suitably qualified with knowledge in Shariah, possibly certified by recognized bodies (e.g. AAOIFI, CIBAFI).
- Good moral character (no criminal record for dishonesty, etc.).
- Ability to understand both Shariah and banking/financial operations.

7.9. Timeliness

- **Branch Audit Reports:** Draft reports must be submitted to the Head of Shariah Audit / SSC Secretariat within **15 working days** of the audit visit.
- **Quarterly Consolidated Reports:** Head Office-level reports for all branches/windows must be submitted to SSC, ACB, and MD/CEO within **30 working days** after the quarter-end.
- **Annual Shariah Audit Report:** Finalized reports, including risk assessment and corrective actions, must be submitted to the Board, SSC, and Bangladesh Bank within **60 working days** of the financial year-end.
- **Branch Compliance Notes:** Branches/windows must submit corrective action responses within **15 working days** of receiving audit findings.
- **Surprise/Ad-hoc Audits:** Preliminary findings communicated within **5 working days**, full report follows standard timelines.
- Delays or non-compliance with timelines are escalated to SSC/ACB; extensions allowed only under exceptional circumstances with formal approval.

Chapter 8: Progressive/Contemporary Controls

8.1. Concurrent Audit

8.1.1. Definition and Objectives

Concurrent Audit is a **real-time, continuous examination** of banking transactions and processes, designed to:

- Detect and prevent irregularities or operational errors promptly,
- Ensure timely compliance with regulatory requirements and internal policies, and
- Provide immediate assurance on the adequacy and effectiveness of internal controls.

It serves as a critical management tool for mitigating operational risks, preventing financial losses and reputational damage, and fostering a sound control environment.

8.1.2. Scope of Concurrent Audit

The scope of Concurrent Audit should be comprehensive and cover all high-value, high-risk, and sensitive areas. Key areas include, but are not limited to:

a. **Treasury & Investment**: Front, middle, and back office activities, including dealing, investments, derivatives, foreign exchange transactions, and reconciliation.

b. **Credit Administration**: Scrutiny of large-value sanctions (e.g., above a threshold defined by risk), verification of security documentation, pre-disbursement checks, post-disbursement monitoring, income recognition and provisioning.

c. **Branch Banking**: High-value clearing, remittances & payments, large cash transactions, vault operations, sensitive customer transactions (e.g., politically exposed persons), suspicious transaction/activity monitoring and compliance with KYC/AML/CFT guidelines.

d. **Digital Banking & IT Operations**: Review of system access controls, user permissions, Fintech/API integrations, and digital transaction logs.

e. **Card Operations**: Authorization, transaction processing, and fraud monitoring.

f. **Outsourced Activities**: Critical processes outsourced to third-party vendors.

8.1.3. Resourcing and Staffing

a. **Dedicated Team:** A separate, dedicated team of Concurrent Auditors must be established, reporting directly to the HoIA.

b. **Qualified Staff:** Team members must possess appropriate knowledge, skills and professional expertise relevant to the area they are auditing (e.g., treasury experts for treasury audits, IT experts for IT audits). They must be trained on relevant laws, regulations (e.g., BB circulars, AML/CFT acts etc.), and the bank's internal policies.

c. **Adequate Resources:** Management must allocate sufficient manpower and technological resources to ensure comprehensive coverage of branches, functions, and processes

without being overstretched, which could compromise audit quality. The resource plan must be justified and approved as part of the annual audit budget.

8.1.4. Risk-Based Planning and Selection

a. **Mandatory RBIA Integration:** The selection of areas for Concurrent Audit must be an integral part of the annual Risk-Based Internal Audit (RBIA) Plan, approved by the Audit Committee of the Board.

b. **Risk Criteria:** Selection should be based on a dynamic risk assessment considering:

- Financial materiality and transaction volumes.
- Complexity and novelty of products/processes.
- History of control failures or fraud.
- Findings from previous internal and external audits.
- Directives from Bangladesh Bank

8.1.5. Methodology

a. **Real-Time Verification:** Auditors should examine transactions on a daily or weekly basis, not retrospectively. The focus is on "verification as it happens."

b. **Checklists & Programs:** Standardized audit programs and checklists must be developed for each auditable area, ensuring comprehensive coverage of key controls and regulatory requirements.

c. **Onsite and Offsite Techniques:** Combination of branch/division-level concurrent checks and central monitoring using data analytics.

d. **Sample Selection:** Use a risk-based sampling approach, focusing on high-value and exceptional items, in addition to random sampling.

e. **System-Based Audit:** Leverage core banking and digital audit tools to flag anomalies in real time.

f. **Working Papers:** Maintain detailed working papers that document the procedures performed, evidence obtained, and conclusions reached. These must be reviewed by a supervisor.

g. **Escalation of Critical Issues:** Critical findings such as fraud or other illegal activity, significant control breaches, or major regulatory violations, must be escalated immediately for appropriate action.

8.1.6. Independence and Quality Assurance

a. **Independence:** Concurrent auditors must remain independent of line functions. Staff engaged in concurrent audit shall not be involved in operations or approve transactions of the auditee unit.

b. **Periodic Review:** The Internal Audit Function shall conduct periodic reviews of the concurrent audit quality, coverage, and reporting standards.

c. **QAIP Inclusion:** The Concurrent Audit function must be included within the scope of the Internal Audit Function's Quality Assurance and Improvement Program (QAIP).

8.1.7. Responsibilities

a. The HoIA shall ultimately be responsible for the overall effectiveness, planning, execution, and reporting of the Concurrent Audit function.

b. Business/Unit Management: Responsible for implementing corrective actions to address audit findings and ensuring a control-conscious environment.

c. Audit Committee of the Board (ACB): Responsible for approving the scope and resource plan for Concurrent Audit, reviewing significant reports, and ensuring management's timely corrective action.

8.1.8. Reporting

a. Concurrent audit reports shall be prepared on a monthly basis and when required.

b. The report must contain detailed findings, recommendations, and a written response from process owners on the audit findings, root cause analysis, corrective actions, and a realistic timeline for implementation.

8.2. Information System (IS) Audit

This framework provides a principles-based, high-level policy outline which establishes mandatory minimum requirements and standards for conducting Information System (IS) Audits to ensure sound IT governance, data security, regulatory compliance, and operational resilience.

8.2.1. Requirements for Bank-Specific IS Audit Manual

a. Banks must develop and implement a comprehensive, bank-specific IS Audit Manual based on their unique operations, business model, risk profile, and ICT infrastructure.

b. The manual shall incorporate detailed procedures, checklists, templates, responsibilities, and evidence requirements while fully complying with Bangladesh Bank's ICT Security Guidelines, Cybersecurity Guidelines, Circulars, and relevant international standards (e.g., ISO/IEC 27001, PCI DSS, NIST Cybersecurity Framework, COBIT 5, ISACA ITAF, ITIL etc.).

c. The manual shall be approved by the Board and reviewed annually.

d. A detailed manual shall include, but not limited to:

- ✓ team structure, qualification criteria, and conflict-of-interest policies;
- ✓ roles for planning, execution, reporting, and follow-up;

- ✓ customized procedures and checklists for all control areas;
- ✓ integration with enterprise risk management;
- ✓ minimum audit frequencies (e.g., annual for high-risk areas);
- ✓ training and competency requirements and plan for ongoing training on emerging risks and standards;
- ✓ mechanisms for updates and Bangladesh Bank submissions;
- ✓ planning templates, risk assessment tools, and adjustment procedures for emerging threats;
- ✓ definition of sampling methodologies, evidence retention standards, documentation quality requirements; etc.

8.2.2. Scope of IS Audit

- IS audits shall encompass all digital and physical elements of a bank's ICT ecosystem, adopting a comprehensive, risk-based methodology. At minimum, audits must cover:
- IT governance and strategies.
- Asset management and service delivery.
- Physical, environmental, and infrastructure security.
- User access, identity, and privileged management.
- Network, database, and application security.
- Change, patch, incident, and problem management.
- Data integrity, retention, disposal, and privacy.
- System acquisition, development, and maintenance.
- Business continuity, disaster recovery, and backups.
- Vendor and outsourcing arrangements.
- Emerging technologies and digital channels.

8.2.3. Risk-Based Audit Planning

- Banks shall establish a dedicated Internal ICT Audit Team within the Interal Audit Division, comprising qualified professionals (e.g., CISA, ISO 27001 certified).
- Annual IS audit plans shall be risk-based, evaluating all branches, divisions, and units for inherent ICT risks. Factors to consider:
  - ✓ Inventory and categorization of information systems.
  - ✓ Impact on critical functions or assets (e.g., core banking, payment systems).
  - ✓ Risk severity (likelihood × impact), including regulatory, operational, and reputational exposures.

- ✓ Prior audit findings, resources, and logistical constraints.

- Plans require approval by the Board Audit Committee and shall prioritize high-risk areas.

8.2.4. Audit Execution and Evidence

- Auditors shall obtain **sufficient, reliable, relevant, and verifiable evidence** through:
  - ✓ Physical inspections and infrastructure reviews,
  - ✓ Technical testing and configuration reviews,
  - ✓ Interviews and process walkthroughs,
  - ✓ Review of logs, alerts, reports, SLAs, and audit trails.
- Evidence must support conclusions on:
  - ✓ Control design,
  - ✓ Operating effectiveness,
  - ✓ Regulatory compliance.

8.2.5. Reporting, Scoring, and Follow-up

- Lapses shall be scored as Serious, Major, Moderate, Minor, or Negligible based on impact.
- Low/medium-risk findings shall be reported to the MD/CEO; high-risk to the ACB.
- Reports shall be submitted within 5 working days.
- Follow-up by Internal Audit Division with half-yearly Board updates.

8.2.6. Assessment of Emerging Risks

Audits shall address evolving threats, including:

- Cybercrime and advanced persistent threats,
- Cloud and shared service risks,
- AI/ML governance and bias risks,
- Data localization and cross-border processing,
- Interoperability and fintech integration risks.

8.2.7. Quality Assurance and Improvement Program (QAIP)

- Internal quality reviews of IS audits.
- Periodic independent assessment.
- Alignment with IIA / ISACA QA expectations.

8.2.8. Use of Technology in IS Audit

- CAATs, data analytics, continuous auditing.
- Secure use of remote / virtual audit techniques.
- Tool governance and access control.

8.3. Virtual / Remote Audit Policy

8.3.1. Introduction & Regulatory Context

With the increasing reliance on Information and Communication Technology (ICT) and the need for operational flexibility, the virtual/remote auditing can be an effective audit methodology when physical presence is impractical or inefficient. Virtual audits enable the ICMS to perform assurance and compliance activities across geographically dispersed locations while maintaining audit quality, independence, and objectivity.

This policy establishes a structured framework for planning, executing, and reporting virtual audits in accordance with ISO 19011:2018 – Guidelines for Auditing Management Systems, which allows flexibility in off-site and remote auditing techniques. This policy mandates that all virtual audit activities must strictly comply with Bangladesh Bank's ICT Security and Cybersecurity requirements, particularly concerning:

- Secure remote access,
- User authentication,
- Data encryption,
- Audit logging and traceability, and
- Protection of sensitive banking information.

Audit Team Leaders are responsible for assessing technology-related and operational risks to ensure that the integrity, reliability, and effectiveness of the audit process are not compromised.

8.3.2. Scope

- Virtual audits may be applied by the Internal Auditors in audits of Branches and sub-branches, Off-site ATMs and agent banking outlets, Shared service centers, Head Office departments, Third-party service providers and vendors (where permitted by contract).
- Virtual audits may be used to Substitute on-site audits where risks are assessed as low to moderate, or Supplement on-site audits as hybrid approach (on-site and off-site) of audit to enhance audit coverage and efficiency.
- High and above average risk areas (e.g., cash management, vault operations, major fraud investigations) shall generally require physical verification unless explicitly approved by the ACB in special cases.
- It can ensure continuity of audit coverage during travel restrictions, emergencies, or cost-efficiency initiatives.
- The virtual audits shall support the Bank's Risk-Based Internal Audit (RBIA) approach.
- There shall be a policy for virtual audit, which shall be reviewed periodically or upon issuance of new regulatory guidance from Bangladesh Bank or relevant international standards.

8.3.3. Pre-requisites of a Virtual Audit

Before confirming a virtual audit, the following criteria must be satisfied:

- **Connectivity Stability**: a pre-audit technical test must confirm reliable internet connectivity, video conferencing capability, and system access.
- **Authentication & Identity Verification**: the identity of auditees must be verifiable, preferably through live video interaction or secure authentication mechanisms.
- **Observability of Processes**: where physical observation is critical (e.g., vault limits, cash counters, document custody), real-time video streaming, CCTV access, or alternative reliable methods must be available.
- **Confidentiality, Security, and Data Protection (CSDP)**: ensuring confidentiality and data protection is fundamental to virtual auditing.
- **Secure Access and Platforms**: all remote access must be routed through Bank-approved VPNs or other encrypted channels.
- Use of personal cloud storage, personal email, or unauthorized collaboration tools is strictly prohibited.
- Only ICT platforms approved by the Bank's IT Security Department may be used for:
    - ✓ File sharing,
    - ✓ Video conferencing,
    - ✓ Screen sharing,
    - ✓ Data analysis.
- The key risks and opportunities associated with the virtual audit techniques shall be assessed before selecting the appropriate audit methods under a Risk-Based Internal Audit (RBIA) framework. A list of commonly used virtual audit techniques and associated risks and opportunities is given in **Annexure-H**.

8.3.4. Data Handling and Retention

- Data Minimization Principle: auditors shall collect only information necessary to meet audit objectives.
- Audit evidence must be stored in secure Bank systems with proper access controls.
- Non-essential documents must be deleted from local devices immediately after audit completion.
- Retention of audit working papers shall follow the Bank's record retention policy.
- Taking screenshots of records requires prior authorization from the Audit Team Leader.
- Taking screenshots or recordings of auditee personnel is strictly prohibited.
- Any recording of meetings must be approved in advance and documented in the audit file.

8.3.5. Privileged Access Controls

- Remote system access must follow the **"least privilege"** principle.
- Auditors shall have read-only access unless exceptional circumstances are approved.
- Under no circumstances shall auditors modify live banking data.

8.3.6. Audit Planning, Execution, and Evidence Collection

8.3.6.1. Planning and Audit Agenda

Virtual audits require enhanced planning compared to on-site audits:

- A detailed audit agenda with defined time slots must be shared in advance.
- Breaks must be incorporated to mitigate screen fatigue.
- Availability of key personnel must be confirmed beforehand.
- If audit objectives cannot be fully achieved virtually due to risk or complexity, an on-site audit must be scheduled.

8.3.6.2. Audit Execution

- Opening and closing meetings must be conducted via secure video conferencing.
- Clear communication protocols must be established.
- Auditors must maintain professional skepticism and independence.
- Live video evidence should be cross-verified with floor plans, layouts, or GIS/location data.
- Verbal explanations must be corroborated with system logs, reports, vouchers, or scanned documents.
- Preference should be given to system-generated reports over manual documents.
- Any time lost due to technical issues must be excluded from official audit duration and documented.

8.3.7. Audit Reporting, Follow-Up, and Continuous Improvement

- Feedbacks from auditors and auditees shall be documented.
- The Audit Team Leader shall update the Risk Matrix based on virtual audit outcomes.
- Lessons learned shall be incorporated into future audit planning and methodology.
- The report shall:
  - ✓ clearly disclose the extent and nature of ICT usage.
  - ✓ Assess the effectiveness and limitations of virtual audit methods.
  - ✓ Identify processes or areas that could not be adequately audited virtually.
  - ✓ Recommend follow-up on-site audits where necessary.

8.4. Whistleblower Framework

The whistleblower mechanism forms an integral part of the ICMS structure. It complements other components of internal control such as internal audit, compliance, monitoring, risk management, and governance oversight and contributes directly to the bank's ethical and compliance culture. To strengthen ethical governance, transparency, and accountability in banking operations, every bank shall establish a robust Whistleblower Framework under its ICMS. The framework will provide a formal mechanism through which employees and other stakeholders can confidentially report any suspected misconduct, fraud, irregularity, or breach of laws and internal policies without fear of retaliation.

This framework shall apply to:

- All employees of the bank, including permanent, contractual, and temporary staff.
- Members of the Board and Senior Management.
- External stakeholders such as customers, vendors, consultants, and agents having official dealings with the bank.

8.4.1. Reportable Issues

Whistleblowers may report, in good faith, any suspected act of:

- Fraud, embezzlement, misappropriation, or corruption.
- Bribery or kickbacks.
- Manipulation of books of accounts, financial records, or regulatory reports.
- Violation of internal policies, procedures, or code of conduct.
- Non-compliance with regulatory directives or ethical standards.
- Environmental, Social, and Governance (ESG) non-compliance.
- Retaliation or harassment against any whistleblower.

8.4.2. Reporting Channels

Banks shall ensure multiple confidential reporting channels, such as:

- A dedicated email address or hotline.
- Secure online reporting system through the bank's intranet or website.
- Written complaints submitted in a sealed envelope marked "Confidential Whistleblower Report" addressed to the HoC or the Chairman of the ACB or to Bangladesh Bank as per Section 2.7 of this guideline.

8.4.3. Confidentiality and Anonymity

- The identity of the whistleblower shall be kept strictly confidential.
- Anonymous complaints shall also be entertained, provided they contain adequate information for investigation.
- All data and documents related to whistleblower cases shall be handled on a "need-to-know" basis and stored securely within the issue handling division.

8.4.4. Protection of Whistleblowers

- No whistleblower shall suffer demotion, suspension, harassment, or any form of retaliation. Rather, any credible whistle blowing shall be appraised and rewarded appropriately.
- Bangladesh Bank may take action if any bank is found retaliating against whistleblowers.
- Protection shall extend even if the allegation is found unsubstantiated, provided it was made in good faith.

8.4.5. Investigation Process

Upon receiving a complaint, the assigned auditor/team/division shall:

- Register and acknowledge the report.
- Conduct a preliminary assessment to determine validity and scope.
- Refer to appropriate authority (Internal Audit, Forensic Audit, or other committees) for full investigation, as required.
- Document findings and recommendations for submission to the Chairman of the ACB.

8.5. Forensic Audit:

Timely detection and prevention of fraud, embezzlement, money laundering (ML), terrorism financing (TF), proliferation financing (PF) etc. is extremely critical to protect interest of the depositors. A forensic audit is an examination and evaluation of a firm's or individual's financial information for use as evidence to pursue further for legal measures. Therefore, forensic audit has received paramount importance for banks to meet the growing need of good governance. Banks may engage Forensic Audit for large advances, non-performing assets (NPAs) cases, restructuring of accounts, wilful default cases, detect, investigate and prevent financial fraud. Bangladesh Bank may time to tome advise threshold, parameters etc. to define coverage for conducting Forensic Audit.

8.5.1. Difference between Audit and Forensic Audit:

- ✓ Objective of financial auditing is to express opinion as to 'true & fair' presentation. Forensic Audit determines correctness of the accounts or whether any fraud has actually taken place.
- ✓ Techniques used in the financial auditing are more of 'Substantive' and 'compliance' procedures. The techniques used in the forensic auditing are analysis of past trend and substantive or 'in depth' checking of selected transactions.
- ✓ Normally all transactions for the particular accounting period are covered under the financial audits. Forensic audits don't face any such limitations. Forensic auditors may be appointed to examine the accounts from the beginning.
- ✓ For ascertaining the accuracy of the current assets and the liabilities financial auditor relies on the management certificate or representation of management. Forensic auditors are required to carry out the independent verification of suspected or selected items.

- ✓ Whenever the financial auditor has adverse findings, then the auditor expresses the qualified opinion, with/without quantification. In case of the adverse findings, the forensic auditors are required to quantify the damages to the clients and is also supposed to point the culprit. Many a times, Legal action will be sought.

8.5.2. Scope of Forensic Audit:

- ✓ **Fraud Investigation and Detection:** Proactively identifying, tracing, and analyzing financial fraud, embezzlement, and misappropriation of assets.
- ✓ **Financial Statement Manipulation:** Investigating whether financial records have been altered to present a false picture of financial health to stakeholders, such as investors or creditors.
- ✓ **Legal Support and Expert Testimony:** Gathering, analyzing, and presenting evidence that is admissible in civil or criminal courts.
- ✓ **Internal Control Review and Risk Management:** Evaluating the effectiveness of an organization's existing internal controls to identify gaps and recommending improvements to prevent future fraud.
  - ✓ **Banking and Bankruptcy Investigations:** Analyzing accounts to identify "willful defaulters" (borrowers who can pay but do not) and investigating financial transactions leading up to insolvency cases.
  - ✓ **Economic Offences and Compliance:** Investigating cases involving bribery, money laundering, and non-compliance with regulatory requirements.
  - ✓ **Computer Forensics:** Utilizing technology to recover, analyze, and secure digital financial data, including recovering deleted files and examining emails.

8.5.3. Procedures of Forensic Audit:

- ✓ **Forensic Audit:** an examination of evidence regarding an assertion to review its trail for reporting in a manner regarded suitable by the court of law.
- ✓ **Forensic Investigation:** the utilization of specialized investigative skills in carrying out an inquiry conducted in such a manner that the outcome will have application to a court of law. A Forensic Investigation may be grounded in accounting, medicine, engineering or some other discipline.
- ✓ **Agreed Upon Procedural Engagement:** as the purpose of the forensic audit is to ensure that there is no financial deception in the organizations and it collects evidence after the examination of accounts and its records, therefore, it is required that forensic audit is done under the agreed procedures of Audit and Evidence.
- ✓ **Predicting the Unpredictable:** a Proactive search for fraud comprises a Forensic Audit Thinking. Forensic Audit Thinking involves – The critical assessment throughout the audit of all evidential matter and maintaining a higher degree of professional scepticism that the fraud may have occurred, is occurring, or will occur in the future.

- ✓ **Analysing Patterns:** it involves deciphering pattern, evaluating reports with figures to study their number patterns and comparing them with standards established looking for prima facie area of suspicion. In this scenario, Forensic auditing aids in detecting, investigating and preventing frauds.
- ✓ **Capacity and capability building for Forensic Audit:** banks shall build the capability and deploy adequate resources to perform forensic audit. If need be, banks may engage private forensic auditors subject to approval from Bangladesh Bank.

Chapter 9: Miscellaneous

9.1. Penalty for Non-Compliance

- If a bank fails to comply with any instructions provided in this guideline may be subject to punitive actions under section 109(11) of the Bank Company Act, 1991(amended up to 2023).
- If a bank's employee willfully/knowingly furnishes false information in reporting to BB, such an offence is punishable under section 109(2) of the Bank Company Act, 1991(amended up to 2023). BB may impose penalty as per section 109(7) of the said Act if a bank fails to submit the reports mentioned in this guideline within stipulated time without any acceptable/satisfactory reason.

9.2. Right to Amend

- Bangladesh Bank reserves the right to amend, extend and modify any part of this guideline, when it deems necessary.

Annexures

Table of Contents

Annexure-A: Sample Multi-dimensional Branch Risk Rating/ Risk Grading

To assist the multi-dimensional branch risk rating/ risk grading in this task, the following matrix (**Table 1**) can be used. However, some banks may consider customization of this matrix to suit their own risk profile. Where appropriate, additional details (e.g. financial values) can be added. The key principle is that all banks should be able to differentiate between different levels of risk in their own area of activity and then ensure appropriate controls are established.
To arrive at the decision of what constitutes a high, medium or low risk, the following template can be used:

Table-1: **Risk Assessment Matrix**

Risk Score	Probability (after considering of risk mitigation)	Impact (before considering of mitigation)
3	✓ High probability or almost certainty ✓ High/frequently recurring ✓ Governed by widely anticipated external factors/frequency of management review not established ✓ New area of risk with no policy & procedure to deal with the matter ✓ Probability uncertain ✓ Complex, requires specialized skills to mitigate	✓ Catastrophic/major impact on the bank ✓ Potential loss more than BDT 1Million. ✓ Serious regulatory implications (Revocation of license, imprisonment)/sanctions. ✓ Potential/actual damage to reputation Major corporate governance failure
2	✓ Evidence of increasing trends ✓ Management reviews largely to manage exceptions ✓ Policies exists but compliance is complex ✓ External factors have medium bearing on ability to follow established standards ✓ Process requires moderate degree of supervision	✓ Significant impact on the bank. ✓ Potential loss more than BDT 1,00,000 ✓ Possibility of fines/penalties from regulators ✓ Medium financial loss with some potential for recovery ✓ Medium level of reputation risk Exposure due to control weakness
1	✓ Unlikely ✓ Isolated incident/Not likely to be repeated ✓ Frequent management review/ well documented ✓ Clear policy exists ✓ External factors have low impact on ability follow established standards ✓ Process simple	✓ Potential or actual loss less than BDT 1,00,000 ✓ Low impact on business or reputation ✓ Exposure on regulatory sanctions low ✓ Customer service issues are within expected levels ✓ Impact on local business unit level

The above checklist is not specific to any individual bank, and the terms of reference may not be generalized in some cases. This should be replaced by a comprehensible list based on business and control parameters, which are quantifiable, and then should be commonly available for all banks.

Scores should be plotted on the following table to determine a category of high, medium and low:

		Impact		
Probability		**Low (1)**	**Medium (2)**	**High (3)**
	High (3)	Medium	High	High
	Medium (2)	Low	Medium	High
	Low (1)	Low	Low	Medium
		Assessed Risk Level		

- **Probability Scale**:
  - Low (1): Unlikely (<10% chance of failure in a year).
  - Medium (2): Possible (10-50% chance).
  - High (3): Likely (>50% chance).
- **Impact Scale**:
  - Low (1): Minimal disruption (<1% of revenue affected).
  - Medium (2): Moderate (1-5% of revenue; localized operational issue).
  - High (3): Severe (>5% of revenue; systemic or regulatory breach).
- **Usage**: Plot scores from control checklists (e.g., Departmental Control Function Checklist). High-risk areas require immediate mitigation; low-risk areas may receive biennial reviews.
- **Example Application**: If a loan/investment approval process has medium probability of override (due to manual checks) and high impact (potential large defaults), it scores Medium × High = High risk.

Annexure-B: Branch Audit Rating

Branch Audit Rating			
… .....Branch			
Sl	**Physical cash (opening/ closing) verification with statements of affairs**	**Allotted Score**	**Score obtained**
1	Detected (short)/ excess	10	0
	Detected(short) but cheque of the same found in safe	5	
	Found as per statements of affairs	0	
Sl	**Physical verification of stamps in hand with statements of affairs**	**Allotted Score**	**Score obtained**
2	Detected (short)/ excess	10	0
	Detected(short)/ excess due to non passing of voucher	5	
	Found as per statements of affairs	0	
Sl	**Physical verification of prize bond with statements of affairs**	**Allotted Score**	**Score obtained**
3	Detected(short)/excess	10	0
	Found as per statements of affairs but register not updated	5	
	Found as per statements of affairs	0	
Sl	**Holding of excess cash over safe limit**	**Allotted Score**	**Score obtained**
4	Exceed 50% & above of days	10	0
	Exceed 30%-< 50% of days	8	
	Exceed 10%-< 30% of days	6	
	Exceed 0%-< 10% of days	4	
	Not exceed	0	
Sl	**Holding of mutilated/ torned notes in safe**	**Allotted Score**	**Score obtained**
5	Holding 5% or more out of total cash	10	0
	Holding 3%-< 5 out of total cash	8	
	Holding 1%-< 3 out of total cash	5	
	Found nil	0	
Sl	**Checking and preservation of prize bond draw result sheet**	**Allotted Score**	**Score obtained**
6	Checking and preservation not done by the branch	10	0
	Partially checked and preserved by the branch	5	
	Found checked and preserve by the branch	0	
Sl	**Deposit scheme exceeding expiry date/prematured encashment of deposit scheme but not marked as closed**	**Allotted Score**	**Score obtained**
7	More than ten cases	10	0
	Up to ten cases	5	
	In no cases	0	
Sl	**FDR/ Deposit account & products rate/tenor variance with approved rate sheet.**	**Allotted Score**	**Score obtained**
8	More than five cases	10	0
	Up to five cases	6	

	In no cases	0	
Sl	**Excise duty/ service charge/other charges/fees/commission/rent/security deposit including VAT (where applicable) not deducted from deposit/ loan account**	**Allotted Score**	**Score obtained**
9	More than five cases	10	0
	Up to five cases	6	
	In no cases	0	
Sl	**Voucher stitching**	**Allotted Score**	**Score obtained**
10	Pending more than 15 days	10	0
	Pending more than 05 days but less than 15 days	7	
	Pending more than 01 day & up to 05 days	5	
	Found not pending	0	
Sl	**Audit Trail prints**	**Allotted Score**	**Score obtained**
11	Found not checked and signed by branch DM/BM	10	0
	Found partially checked and signed by branch DM/BM	5	
	Found checked and signed by branch DM/BM	0	
Sl	**Daily mandatory output (supplementary sheet/ statements of affairs/clean cash book/ vouchers/etc.)**	**Allotted Score**	**Score obtained**
12	Found not checked and signed by branch DM/BM	10	0
	Found partially checked and signed by branch DM/BM	7	
	Found checked and signed by branch DM/BM	0	
Sl	**Payment made against advance dated or against stale cheque**	**Allotted Score**	**Score obtained**
13	More than five cases	10	0
	Up to five cases	7	
	In no cases	0	
Sl	**Reversal of contra entries**	**Allotted Score**	**Score obtained**
14	Expired contra entries found not reversed more than five cases	10	0
	Expired contra entries found not reversed up to five cases	8	
	Expired contra entries found reversed	0	
Sl	**Balance confirmation letter**	**Allotted Score**	**Score obtained**
15	Preceding half yearly BC not sent by the branch	10	0
	BC sent by the branch but not in all cases (partially sent)	5	
	BC regularly sent by the branch	0	
Sl	**Thanks letter**	**Allotted Score**	**Score obtained**
16	Thanks letter not sent by the branch	10	

	Thanks letter sent by the branch but not in all cases	5	0
	Branch is in practice of sending thanks letter	0	
Sl	**Officials in the branch working in the branch more than 3 years.**	**Allotted Score**	**Score obtained**
17	100% cases	10	0
	80%-<100% cases	8	
	30%-<80%	5	
	Less than 30%	3	
	No such instances	0	
Sl	**User shut down his work station, power off the printer and UPS at the end of the day**	**Allotted Score**	**Score obtained**
18	No (for any instances and any single cases)	10	0
	Yes	0	
Sl	**Loan disbursed but accepted sanction advice not obtained**	**Allotted Score**	**Score obtained**
19	More than 10 cases	10	0
	06 to10 cases	8	
	Up to 05 cases	5	
	No such case found	0	
Sl	**Sanction advice was not prepared according to CHO approval.**	**Allotted Score**	**Score obtained**
20	More than 10 cases	10	0
	06 to 10 cases	5	
	Up to 05 cases	4	
	No such case found	0	
Sl	**Charge document not obtained/ found blank/ without stamp**	**Allotted Score**	**Score obtained**
21	More than 10 cases	10	0
	06 to 10 cases	5	
	Up to 05 cases	4	
	No such case found	0	
Sl	**Lien of security instruments**	**Allotted Score**	**Score obtained**
22	Pending any instances	10	0
	Done in all applicable cases	0	
Sl	**Execution of Registered Mortgage and IGPA**	**Allotted Score**	**Score obtained**
23	Pending any instance	10	0
	Done in all applicable cases	0	
Sl	**Obtainment of original title deed/certified true copy along with SRO token/deed ticket for registered mortgaged property.**	**Allotted Score**	**Score obtained**

24	Pending any instance	10	0
	Done in all applicable cases	0	
Sl	**Obtainment of land related documents/chain documents**	**Allotted Score**	**Score obtained**
25	Pending more than 15 cases	10	0
	Pending up to 15 cases	8	
	Pending up to 05 cases	5	
	No such case found	0	
Sl	**Monthly basis stock report as per CHO sanction**	**Allotted Score**	**Score obtained**
26	Pending more than 15 cases	10	0
	Pending up to 15 cases	8	
	Pending up to 05 cases	5	
	No such case found	0	
Sl	**Insurance coverage not taken properly/policy expired/insurance policy not found**	**Allotted Score**	**Score obtained**
27	More than 10 cases	10	0
	06 to 10 cases	8	
	Up to 05 cases	5	
	No such cases found	0	
Sl	**Non-Preservation of LDCL in respective loan file**	**Allotted Score**	**Score obtained**
28	More than 10 cases	10	0
	06 to 10 cases	8	
	Up to 05 cases	5	
	No such cases found	0	
Sl	**Maintenance of safe-in and safe-out register**	**Allotted Score**	**Score obtained**
29	Not maintained	10	0
	Maintained but not up to date	5	
	Maintained properly and found up to date	0	
Sl	**Comments of Bangladesh Bank Audit team regarding core risk areas (CRM,AML,ICT & ICC)**	**Allotted Score**	**Score obtained**
30	Not satisfactory	10	0
	Partial satisfactory	5	
	Satisfactory	0	
	(If not audited by Bangladesh Bank score will be zero)		
	Total	**300**	**0**
	Percentage (%)		-
	Branch Rating		

Annexure-C: Departmental Control Function Checklist (DCFCL)

a. Departmental Control Function Checklist (DCFCL): "Daily"

Bank Name:……..

Branch Name:…….

DEPARTMENTAL CONTROL FUNCTION CHECKLIST (DCFCL): "DAILY" **FOR THE MONTH OF:**

Sl	Process	Function	Responsibility	Initial																														
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	A. General Banking Activities:																																	
1	**Branch premises Cleanliness**	**Ensure Cleanliness of branch premises.**	DM/BM																															
2	**Branch employees attendance**	**Ensure timely attendance of branch employees.**	DM/BM																															
3		**Ensure 24/7 security guard duty & register maintenance.**																																
4		**Ensure gunman's duty.**																																
5	**Safety and premises Security**	**a) Ensure 24/7 CC TV Coverage of full area of Branch & checked recording data regularly & preserved the same at least 1 year.**	DM/BM																															

		b) Ensure CCTV footage reviewed and recorded in register, as the previous day's CCTV footage is already available. In addition, the three month's CCTV footage must be sent to ICCD, CHO.																																				
6		**Ensure adequate Fire Extinguisher and smoke detector on Branch premises.**																																				
7		**Ensure generator backup/ Log Book register maintenance.**																																				
8	**Compliance of CHO Instructions**	**Ensure Bank's dress code compliance.**	DM/BM																																			
9		**Ensure Bank's etiquette and service compliance.**																																				
10		**Ensure Bank's code of conduct compliance.**																																				
11		**Ensure Customer Compliance acceptance Policy.**																																				
12		**Ensure Bank Anti Harassment Policy compliance.**																																				
13	**Regulatory Compliance**	**Ensure timely submission of compliance report of B Bank, Internal & External Audit and Inspection team.**	DM/BM																																			

14		**Ensure display in the branch premises "Forged note Notice".**																																				
15		**Ensure display "Cheque returns Notice".**																																				
16		**Ensure display "Bank's profit rates on Deposit and Credit/investments".**																																				
17		**Ensure display updated "Bank charges schedule".**																																				
18		**Ensure display "Bank's Complaint Cell No. and BB Hot line No."**																																				
19		**Ensure that School Banking a/c & No Frill A/c. information & related programmed photograph are displayed.**																																				
20	**Cash in hand Local Currency**	**Ensure Daily cash received and payment made including online payment.**	Dealing officer																																			
			Cash In-charge																																			
			DM/BM																																			
21		**Confirm review teller's cash sheet with evidence & Register.**	Cash In-charge																																			
			DM/BM																																			
22		**Confirm physical Cash balance with daily cash book, vault register and daily affairs.**	Cash In-charge																																			
			GB In-charge																																			
			DM/BM																																			

23		**Ensure cash transaction and cash holding of the branch within insured limit.**	Cash In-charge																																
			GB In-charge																																
			DM/BM																																
24		**Ensure Mutilated notes separately kept and recorded in the separate register.**	Cash In-charge																																
			DM/BM																																
25		**Fly leaf are used each and every bundle of currency notes.**	Cash In-charge																																
			DM/BM																																
26	**Cash in hand Foreign Currency (For AD Branch)**	**Ensure Selling and Buying of Foreign Currency and recording in the register under dual control.**	Cash In-charge																																
			In-charge GB																																
			In-charge FEX																																
			DM/BM																																
27		**Confirm physical cash of Foreign Currency balance with daily cash book, vault register and daily affairs.**	Cash In-charge																																
			In-charge FEX																																
			DM/BM																																
28	**ATM (For ATM Branch)**	**Ensure loading of cash in ATM after counting previous balance.**	Cash In-charge																																
			DM/BM																																
29		**Ensure Passing necessary entries soon after loading, unloading of cash of ATM**	Cash In-charge																																
			DM/BM																																

30	**Stamps in hand**	**Ensure Stamps in hand are recorded and maintained under dual control.**	Dealing officer																															
			Cash In-charge																															
31		**Confirm physical stamp in hand and balance with GL register.**	GB In-charge																															
			DM/BM																															
32	**Account opening activities**	**Ensure before Opening new deposit accounts Contact Point Verification (CPV) is done.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
33		**Ensure all necessary formalities are completed at the time of New A/C Opening and New A/C Listing is tallied with A/C Opening Form (AOF).**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
34		**Ensure upload data in CBS after getting approval from Branch Manager.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
35		**Ensure Send thanks letter for new deposit accounts to the account holder to verify the address.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
36	**Standing Instructions**	**Ensure checking and verify Standing instruction issue list.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															

37		**Ensure provide AML/CFT information leaflets to the customers.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
38		**Ensure regularly monitor and review TP and KYC**	GB In-charge																																
			DM/BM																																
39	**Anti Money Laundering activities (AML)**	**Ensure monitoring of High Risk Client**	Dealing officer																																
			GB In-charge																																
			BAMAL CO																																
40		**Ensure checking, verify CTR, STR and report the same to DM/BM if any abnormality seen.**	Dealing officer																																
			GB In-charge																																
			BAMAL CO																																
41	**Cheque Books**	**Ensure requisition, receive & deliver of cheque books by maintaining register under dual control.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
42	**Printing stationery & Security stationery (MTDR, PO etc.)**	**Ensure requisition and receive printing/ security stationery by maintaining register under dual control.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
43	**Balancing of Instruments**	**Ensure physical (both Issued & non Issued) balancing of MTDR/FDR/ PO/ Scheme Term**	Dealing officer																																
			GB In-charge																																

		Deposit Receipts etc. with the system regularly at the close of the business each day to protect the missing of Leaves/Book.	DM/BM																																	
44	**Locker Account (If locker services available)**	**Ensure maintaining of locker register under dual control.**	Dealing officer																																	
			GB In-charge																																		
			DM/BM																																		
45		**Ensure maintaining of Master keys of locker under dual custodians.**	Dealing officer																																		
			GB In-charge																																		
			DM/BM																																		
46		**Ensure realization of security deposit and rent of Locker.**	Dealing officer																																		
			GB In-charge																																		
			DM/BM																																		
47	**Standing/ Stop Payment instruction**	**Ensure maintenance of standing /Stop Payment instruction register under dual control.**	Dealing officer																																		
			GB In-charge																																		
			DM/BM																																		
48	**Debit Card and Credit Card (fresh and renewal)**	**Ensure receiving card application & forwarded to Card Division, CHO for approval.**	Dealing officer																																		
			GB In-charge																																		
			DM/BM																																		
49		**Ensure maintaining of card (Receiving, delivered& undelivered card) by**	Dealing officer																																		
			GB In-charge																																		

		dual custodian.	DM/BM																															
50	**Bangladesh Automated Clearing House (BACH) Outward**	**Ensure scanning image of received instruments.**	Dealing officer																															
			DM/BM																															
51		**Ensure posting of cheque series, routing number, a/c number, transaction number and amount of the instruments in BACH.**	Dealing officer																															
			DM/BM																															
52		**Ensure marking of BACH in High value and regular value.**	GB In-charge																															
			DM/BM																															
53		**Ensure release reprocess to Central Clearing Department (CCD).**	DM/BM																															
54		**Ensure checking settlement position of BACH.**	GB In-charge																															
			DM/BM																															
55		**Ensure inform returned instruments information to the client.**	Dealing Officer																															
			GB In-charge																															
			DM/BM																															
56	**Bangladesh Automated Clearing House (BACH) Inward**	**Ensure BACH delegation (receiving and printing) Scrutiny of BACH (cheque series, routing no. a/c no., transaction no., amount, manual & e-endorsement of both high value and regular value instruments.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															

57		**Debit customer a/c as per positive payment advice from customer's properly.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
58		**Ensure checking & verify Outward and Inward Bills & Remittance Registers outstanding balance with GL Heads.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
59		**Ensure issuance and encashment of PO, Pay Slip recording in the register under dual control.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
60	**Bills and Remittance**	**Ensure that Payment Order amount has been deposited along with Commission & Vat.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
61		**Ensure the Payment Order must be printed to deliver customer, also confirmed that hand written Payment Order are not issued.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
62		**Ensure Issuing Payment Order to a walk-in customer, KYC, NID & Cell No. must be obtained.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															

63		**Confirm for issuance or encashment of a Payment Order exceeding Tk.50,000/-, it is maintained a linked CASA a/c.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
64		**Ensure balancing the leaf of security blocks on regularly basis.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
65	**Reconciliation**	**Ensure reconciliation of online GL transaction with other branches and CHO.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
66		**Ensure reconciliation of balance of deposit a/c maintained with other bank.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
67	**Activities of Accounts Department**	**Ensure different Charges, profit, Depreciation and VAT & AIT realized.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
68		**Ensure profit paid to deposit account.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
69		**Ensure confirm Monthly provision made against expenses.**	GB In-charge																																
			DM/BM																																

70		**Ensure debit all a/c (sundry creditor's a/c, sundry debtors a/c, advance against employee a/c, advance against suppliers a/c suspense a/c etc.) with the approval of branch manager and reviewing the same & adjusted within 15 days.**	Dealing officer																														
			GB In-charge																														
			DM/BM																														
71		**Ensure check Sundry/ Suspense Balance Difference, if any mismatch is found, dissolved immediately.**	GB In-charge																														
			DM/BM																														
72	**Activities of Accounts Department**	**Ensure reversal/ Deleted Transactions & report to the same to DM/BM.**	Dealing officer																														
			GB In-charge																														
			DM/BM																														
73		**Ensure verify all register balance tallied with related GL Heads and any negative balance in Income & Expenditure.**	Dealing officer																														
			GB In-charge																														
			DM/BM																														
74		**Ensure checking and review of Profit/ Interest product sheet.**	Dealing officer																														
			GB In-charge																														
			DM/BM																														

75		**Ensure balances of different Heads of Statement of Affairs are matched with Summary Situation Report.**	DM/BM																																
76		**Ensure checking & verify remote Transaction Report to ensure correctness of the Transaction.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
77		**Ensure monitoring of Dormant and imperatives a/c and maintaining the same.**	GB In-charge /DM																																
78		**Ensure monitoring of Voucher Record Register/ Voucher Movement Register under joint signature.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
79		**Ensure printing user wise transaction listing (GL & Client) and verify with related transaction vouchers.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
80		**Ensure printing Clean Cash Report and verified with GL and Client Supplementary Summary.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
81		**Ensure checking Modification Log report.**	GB In-charge																																
			DM/BM																																

82		**Ensure all voucher Cash, Clg, Trf (both Client & GL) and any other instruments are signed and acknowledged by a/c holder/ customers must be preserved in hard form.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
83		**Ensure all original copies of vouchers and related transaction listing and supplementary must be stitched under Voucher Cover with Gala Sealed & preserved in safe custody in the next working day.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
84	**Voucher preservation**	**Ensure number of vouchers must be written on the Voucher Cover with initiated jointly signature.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
85		**Ensure duly filled in Voucher Record Register must be maintained jointly signature.**	Dealing officer																																
			GB In-charge																																
			DM/BM																																
86		**Ensure daily original vouchers are kept in Steel Trunk/Vault in day, month and year -wise, sequentially under lock & key in**	Dealing officer																																
			GB In-charge																																

		joint custody.	DM/BM																															
87		**Branch must sent vouchers to Central godown in consultation with CSD.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
88	**Reports/ Returns/Statements on General Banking**	**Ensure timely submission of all returns & statements to Head Office, B. Bank and Regulatory bodies.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
89	**Refrain from Password Sharing**	**Ensure no official share their login credential (ID & password) with any other officials under any circumstances.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
90	**Awareness relating ICT Security Policy**	**Ensure all officials are aware of the latest ICT Security Policy & its Implications in our Bank**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
91	**Allow transaction where Valid Phone Number Exists in Account**	**Ensure transaction in an account where a valid phone number is present.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
92	**Functional Antivirus**	**Ensure Trend Micro antivirus agent is installed in all the branch PCs an Real-time Scanning is enabled.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															

93	**Email Security**	**Ensure officials do not open emails from unknown Domain, unknown Senders, suspicious email links**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
94	**Updating Web Browsers**	**Ensure web browsers are updated with the latest stable version to avoid common vulnerabilities.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
95	**Physical Security of IT Room**	**Ensure IT room is kept locked , AC is running and backup available, Displayed "Entry Restricted" sign & a List of Authorized Officials to Access IT room, IT Room Access Log is maintained properly, Emergency Contract Numbers shown, etc.**	Dealing officer																															
			GB In-charge																															
			DM/BM																															
	B. Credit/ Investment Department Activities:																																	
96	**Credit/ Investment Operations**	**Ensure preparation of Loan/Investment proposal and sending to CHO for approval upon complying relevant policy and procedure of the bank in due time.**	Dealing Officer																															
			Credit-In-charge																															
			DM/BM																															

97		**Ensure prepare up to date Credit Rating/ICRRS of the client.**	Dealing Officer																																
			Credit-In-charge																																
			DM/BM																																
98		**Ensure checking all Loan/ Investment a/c through Exception Credit/investment Listing.**	Dealing Officer																																
			Credit-In-charge																																
			DM/BM																																
99		**Ensure tally Net Loan/Investment balance of Loan/Investment Listing with balance of Statement of Affairs.**	Dealing Officer																																
			Credit-In-charge																																
			DM/BM																																
100		**Ensure obtaining up to date clean CIB report.**	Credit-In-charge																																
			DM/BM																																
101		**Ensure receiving CHO sanction letter, issue duplicate sanction advice to client & preserve with client's acceptance.**	Credit-In-charge																																
			DM/BM																																
102	**Credit/ investment Operations**	**Ensure prepare LDCL/ IDCL and send to CHO for Authority for Disbursement.**	Dealing Officer																																
			Credit-In-charge																																
			DM/BM																																

##		**Ensure the Credit/investment charge documents executed/ to be executed must be read out to the Loan/ Investment Client, Guarantor/ relevant 3rd party. In additional to obtaining their signatures, thumb impressions of both hands must be taken and verified with the NID database before acceptance.**	Dealing Officer																																			
			Credit-In-charge																																			
			DM/BM																																			
104		**Ensure maintaining safe-in and safe-out register under dual control.**	Dealing Officer																																			
			Credit-In-charge																																			
			DM/BM																																			
105		**Ensure maintaining due date diary for renewal of Loan/ Investment/ Insurance /SRO token.**	Credit-In-charge																																			
			DM/BM																																			
	C. Trade Finance and Foreign Exchange Transactions:																																				
106	**Loan/Investment approvals for trade transactions**	**Ensure obtaining approvals for trade transactions from CHO.**	Dealing officer																																			
			In-charge FEX																																			
			DM/BM																																			

107	**Loan/Investment a/c opening and limit loading**	**Ensure opening Credit/investment a/c and loading of Loan/Investment limit after complete proper IDCL formalities.**	Dealing officer																																
			DM/BM																																
108	**Timely recovery of Loan/Investment**	**Ensure timely recovery of outstanding /overdue /expired Loan/Investment.**	Dealing officer																																
			DM/BM																																
109	**Cash Transactions**	**Ensure realizing commission and charges (e.g. advising charges) from non customers.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
110	**Stamps in Hand**	**Confirm stamp in hand stock agreed with register.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
111	**Collecting Bill of Entries and EXP forms**	**Ensure collecting all Bill of Entries within 15(fifteen) days from the date of release of imported consignment for onward reporting to BB.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
112		**Ensure collecting all EXP forms within 10 (ten) days from the shipment date of the export consignment for onward reporting to BB.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
113	**Storage of Files and**	**Ensure master file of the customer is**	Dealing officer																																

	Register	**maintained at branch level.**	In-charge FEX																																	
			DM/BM																																	
114	**Cash Incentive and Duty Draw back**	**Ensure claiming Cash Incentive to BB through CHO and paid to client by following all applicable rules and regulations.**	Dealing officer																																	
			In-charge FEX																																	
			DM/BM																																	
115		**Ensure accurate cash incentive calculation sheet.**	Dealing officer																																	
			In-charge FEX																																	
116		**Ensure collected PRC and other related certificates / documents on time and file.**	Dealing officer																																	
			In-charge FEX																																	
117	**Central Payment Unit(CPU)**	**Ensure timely Submission of Payment Instructions (PI) and Reimbursement Authorizations (RA).**	Dealing officer																																	
			In-charge FEX																																	
118	**Reports/ Returns/Statements on Foreign Trade**	**Ensure timely submission of all returns & statements to Head Office, B. Bank and Regulatory bodies.**	Dealing officer																																	
			In-charge FEX																																	
			DM/BM																																	
119	**Import**	**Ensure opening of LC by obtaining stipulated margin/cash security.**	Dealing officer																																	
			In-charge FEX																																	
			DM/BM																																	
120		**Ensure LC commission**	Dealing officer																																	

		/vat/charge realized properly.	In-charge FEX																																		
			DM/BM																																		
121		**Ensure LC opened with valid IRC/ other related papers and documents.**	Dealing officer																																		
			In-charge FEX																																		
			DM/BM																																		
122		**Ensure L/C opened by obtaining buyers' /supplier s' credit report.**	Dealing officer																																		
			In-charge FEX																																		
			DM/BM																																		
123		**Ensure Importer's signature verified in Pro-forma Invoice / Indent / LC application form etc.**	Dealing officer																																		
			In-charge FEX																																		
			DM/BM																																		
124		**Ensure original shipping documents / import documents keeping until liability adjusted.**	Dealing officer																																		
			In-charge FEX																																		
			DM/BM																																		
125		**Ensure readable copy (4th copy) of LCAF sent to CCI & E in due time.**	Dealing officer																																		
			In-charge FEX																																		
			DM/BM																																		
126		**Ensure PAD register and other register relating to Import, properly maintained by the Branch.**	Dealing officer																																		
			In-charge FEX																																		
			DM/BM																																		

127		**Ensure collection Bill of Entry/Custom certified invoice from the client and Matching done with IMP in due time.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
128	**Export**	**Ensure EXP issued by the branch with valid ERC/other related papers and documents.**	Dealing officer																																
			DM/BM																																
129		**Ensure Exp register properly filled by the branch.**	Dealing officer																																
			DM/BM																																
130		**Ensure Clean export documents purchased.**	In-charge FEX																																
			DM/BM																																
131		**Ensure submission of 2nd copy of EXP form to B Bank within 14 days from the date of shipment.**	Dealing officer																																
			In-charge FEX																																
132		**Ensure submission of 3rd copy of Exp form to B Bank within the month of proceed realized against Exp.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
133		**Ensure reporting to B Bank against un-realized Export Proceeds over 120 days.**	In-charge FEX																																
			DM/BM																																
134		**Ensure compliance of other terms and conditions as per CHO sanction letter.**	In-charge FEX																																
			DM/BM																																

135	**Foreign Remittance**	**Ensure Foreign remittance realized & credited to the respective a/c under dual control.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
136		**Ensure making payment all Foreign Remittance (Inward Remittance) with F.C a/c.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
137		**Ensure encashment Certificate issued against foreign remittance as per client request.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
138		**Ensure payment miscellaneous outward remittance under dual control.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
139	**Others**	**Confirm correspondence via SWIFT with Foreign correspondence formiscellaneous Purpose.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
140		**Ensure proper open & maintain Foreign Currency A/c & ERQ A/c upon complying relevant rules and regulation of the Bank.**	Dealing officer																																
			In-charge FEX																																
			DM/BM																																
141		**Confirm Settlement International Credit Card Bill in due time properly.**	Dealing officer																																
			In-charge FEX																																

			DM/BM																															
142		**Confirm cash Dollar endorsement & prepare TM form to report BB under dual control.**	Dealing officer																															
			In-charge FEX																															
			DM/BM																															
143		**Ensure proper open and maintain student file upon complying relevant rules and regulation of the Bank.**	Dealing officer																															
			In-charge FEX																															
			DM/BM																															
144		**Ensure prepare and maintain L/C Operational Check List (if any open) Properly.**	Dealing officer																															
			In-charge FEX																															
			DM/BM																															

b. Departmental Control Function Checklist (DCFCL): "Weekly"

Bank Name:……..

Branch Name:…….

DEPARTMENTAL CONTROL FUNCTION CHECKLIST (DCFCL): "WEEKLY" **FOR THE MONTH OF:**

Sl	Process	Functions	Responsibility	1st WEEK		2nd WEEK		3rd WEEK		4th WEEK	
				Initial	Date	Initial	Date	Initial	Date	Initial	Date
1	Compliance of Head Office Instructions	Ensure full compliance of all Guidelines, Manual, and Insurances & Circulars.	DM/ BM								
2	Compliance of Regulatory Instructions	Ensure display bank's profit rates on various deposit and Investment products.	DM/ BM								
3		Maintain Complain Box in a visible place properly.	DM/ BM								
4		Ensure Display up to date schedule of charges of the bank.	DM/ BM								
5		Ensure surprise visit record Register holiday/night is being maintained properly.	DM/ BM								
6	Account opening	Ensure opening of all deposit accounts as per Head Office Circular and In-put information in CBS.	Desk officer								
			GB In-charge								
			DM/ BM								
7	Bills and Remittance	Ensure leaf balancing of security blocks on regular basis.	Desk officer								
			GB In-charge								
			DM/ BM								
8	Reports/ Returns/ Statements on General Banking	Ensure timely submission of all weekly returns& statements to Head Office, BB and Regulatory bodies.	Desk officer								
			GB In-charge								
			DM/ BM								
	Loan/ Investment										
9	Loan/ Investment Operations	Ensure execution of Mortgage & other formalities; obtain required papers and documents as per Head Office sanction.	Desk officer								
			Credit In-charge								
			DM/ BM								
10	Monitoring, follow up and supervision	Follow up the overdue and NPL properly.	Credit In-charge								
			DM/ BM								
11		Ensure monitoring and follow up of all court cases.	Credit In-charge								
			DM/ BM								

c. Departmental Control Function Checklist (DCFCL): "Monthly"

Bank Name:……..

Branch Name:…….

DEPARTMENTAL CONTROL FUNCTION CHECKLIST (DCFCL)- "MONTHLY" **FOR THE MONTH OF:**

Sl	Process	Functions	Responsibility	Date of Checking	Signature
1	Compliance of Head Office Instructions	Ensure full compliance of Bank Compliance Manual.	DM/BM		
2		Ensure full compliance of Customer Acceptance Policy.	DM/BM		
3	Compliance of Regulatory Instructions	Ensure compliance of Bangladesh Bank, Internal and External Audit and Inspection Report.	DM/BM		
4	Compliance of Anti Money Laundering activities	a) Ensure holding of BAMLCO meeting regularly.	BAMLCO		
		b) Ensure review and reporting of CTR & STR and maintaining hard copy thereof.	DM/BM		
5	Cheque Books	Ensure generate undelivered cheque books list and ensure necessary compliance as per CHO Circular.	Desk officer		
			GB In-charge		
			DM/BM		
6	Card (Debit & Credit)	Ensure generate undelivered Card (Debit & Credit) list and ensure necessary compliance as per CHO Circular.	Desk officer		
			GB In-charge		
			DM/BM		
7	Printing stationery, Security stationery	Ensure physical verification of printing and security stationery is to be done.	Desk officer		
			GB In-charge		
			DM/BM		
8	Locker Account	Ensure realization of locker rent & security deposit as per HO instructions.	Desk officer		
			GB In-charge		
			DM/BM		
9	Maturity Log	Ensure review Time Deposit / Scheme Deposit Maturity log on a regular basis.	Desk officer		
			GB In-charge		
			DM/BM		

10		Ensure generate Time Deposit Maturity/ Scheme Deposit Maturity List on 1st working day of each month and properly inform the client about the up-coming maturity of the related Scheme Deposit Account.	Desk officer		
			GB In-charge		
			DM/BM		
11		Ensure generate Monthly Scheme Deposits Defaulter List.	Desk officer		
			GB In-charge		
			DM/BM		
12	Accounts Department	Confirm physical verify of Payment Order, Demand Draft, MTDR, MIS stock with GL register monthly under dual control.	Desk officer		
			GB In-charge		
			DM/BM		
13		Ensure charging of profit, service charge, fees, commission and depreciation.	Desk officer		
			GB In-charge		
			DM/BM		
14		Ensure realization of VAT and AIT as per instructions of concerned Government office.	Desk officer		
			GB In-charge		
			DM/BM		
15		Ensure profit paid to deposit account and accrued accordingly.	Desk officer		
			GB In-charge		
			DM/BM		
16		Ensure monthly provision made against expenses.	Desk officer		
			GB In-charge		
			DM/BM		
17		Ensure review and reversal of contra entries.	Desk officer		
			GB In-charge		
			DM/BM		
18		Ensure checking and review of Profit product sheet.	Desk officer		
			GB In-charge		
			DM/BM		
19	Reports/ Returns/ Statements on General Banking	Ensure timely submission of all returns& statements to Head Office, BB and Regulatory bodies.	Desk officer		
			GB In-charge		
			DM/BM		

	Loan/Investment				
20	**Monitoring, follow up and supervision**	**Ensure collected monthly basis clients stock report.**	**Credit In-charge**		
			DM/BM		
21		**Ensure verified of rent, khatian of mortgaged property including Digital Khatian through QR Code scanning.**	**Credit In-charge**		
			DM/BM		
22		**Ensure reverse the timely Expired contingent liability BG /PG/Bai-Salam/APG etc.**	**Desk Officer**		
			Credit In-charge		
			DM/BM		
23		**Ensure follow up the overdue and NPL regularly.**	**Credit In-charge**		
			DM/BM		
24		**Ensure monitoring, supervision and follow up of all court cases (if any).**	**Credit In-charge**		
			DM/BM		
25		**Ensure timely renewal of loan/Investment limit.**	**Credit In-charge**		
			DM/BM		
26		**Ensure rescheduling of classified loan/ Investments accounts (if any) as per BRPD circular of BB.**	**Desk Officer**		
			Credit In-charge		
			DM/BM		
27		**Ensure prepare of CL Statements as per BRPD circular of BB.**	**Desk Officer**		
			Credit In-charge		
			DM/BM		
28	**Integrated Supervision System (ISS) Reporting**	**Ensure collect the relevant information for ISS Reporting and correctly fill up the fields of ISS Reporting Format.**	**ISS Reporting Official(s)**		
29		**Get the report checked by the concerned officials properly.**	**ISS Reporting Official**		
			DM/BM		
30		**Submit the same to the Manager for confirmation and upload in the Bangladesh Bank's Web Portal on or before 10th of the following month properly.**	**DM/BM**		
31		**Ensure Checking the Integrated Supervision System (ISS) of the branch.**	**Credit In-charge**		
			DM/BM		
32		**Ensure Deficiency, if detected, report to concerned division/department of CHO.**	**Credit In-charge**		
			DM/BM		

33		Ensure Uploading the Integrated Supervision System (ISS) Report to Bangladesh Bank's Web Portal and submit back-up copy (Excel Sheet) to Group ICC within 10th of the following month.	ISS Reporting Official		
			DM/BM		
34	Reports/ Returns/ Statements on Investment	Ensure timely submission of all returns& statements to Head Office, B. Bank and Regulatory bodies.	Credit In-charge		
			DM/BM		
	Foreign Trade				
35	Monitoring, follow up and supervision	Ensure PAD/MIB Register is being maintained.	Desk Officer		
			Fex In-charge		
			DM/BM		
36		Ensure Export performance register has properly been maintained.	Fex In-charge		
			DM/BM		
37		Ensure All Commission, Vat& others Charges are realized.	Desk Officer		
			Fex In-charge		
			DM/BM		
38		Ensure Timely Expired contingent liability LC, ABP Reverse.	Desk Officer		
			Fex In-charge		
			DM/BM		
39	Reports/ Returns/Statements on Foreign Trade	Ensure timely submission of all returns& statements to Head Office, BB and Regulatory bodies.	Desk Officer		
			Fex In-charge		
			DM/BM		

d. Departmental Control Function Checklist (DCFCL): "Quarterly"

Bank Name:……..

Branch Name:…….

DEPARTMENTAL CONTROL FUNCTION CHECKLIST (DCFCL): "QUARTERLY" FOR THE QUARTER ENDED:

Sl	Process	Functions	Responsibility	1st quarter		2nd quarter		3rd quarter		4th quarter	
				Date	Initial	Date	Initial	Date	Initial	Date	Initial
1	Safety, Security, measures and premises protection	Ensure adequate Fire Extinguisher in branch premises.	DM/ BM								
2		Ensure checking of electrical wires by qualified electrician.	DM/ BM								
3		Ensure adequate smoke detector in Branch.	DM/ BM								
4		Ensure emergency contact number i.e. Police station, Fire station, RAB, Hospital etc. are available in branch.	DM/ BM								
5	Compliance of Regulatory Instructions	Ensure checking the validity of Bank's License.	DM/ BM								
6		Ensure checking the validity of all insurance policy of the Branch.	DM/ BM								
7		Display up-to date financial statements with highlights Properly.	DM/ BM								
8		Display leaflets containing the salient points of AML and CFT properly.	DM/ BM								
9	Self Assessment of Anti- Fraud Internal Control (SAFFIC)	Ensure checking the internal control system of the branch.	DM/ BM								
10		Ensure deficiency, if detected report to concerned division / department of Head Office.	DM/ BM								
11		Submit SAFFIC Report to Respective Division within 10th of the following months of the quarter ended and preserved in the file properly.	Desk officer								
			GB In-charge								
			DM/ BM								
12	Accounts Department	Generate Fixed Asset Register report and verify with Physical Position & Statement of Affairs properly.	Desk officer								
			GB In-charge								
			DM/ BM								
13	Quarterly Operation Report (QOR)	Ensure submission of QOR to Head Office within 10th of the following months of the quarter ended and preserved in the file.	Desk officer								
			GB In-charge								
			DM/ BM								

14	Returns , statements and reporting on General Banking	Ensure timely submission of all quarterly returns & statements to Head Office, BB and Regulatory bodies.	Desk officer								
			GB In-charge								
			DM/ BM								
15	Updating ICT Assets inventory of the Branch	Ensure physical ICT assets are matched with the record of ICT assets in the Fixed Asset inventory list of the Bank's CBS.	Desk officer								
			GB In-charge								
			DM/ BM								
16	Review of User Lists of Different Applications	Ensure timely review of all user list of different applications running in the branch, such as CBS, BACH, BEFTN, RTGS, eGP, SMS Registration, RMS, CIB, Card Requisition, Email Group, Agent Banking, e-Challan, e-Account etc.	Desk officer								
			GB In-charge								
			DM/ BM								
17	Undelivered Card	Ensure no undelivered card stays at the branch after 6 months. Send those cards to Card Division with a list to destroy those Cards timely.	Desk officer								
			GB In-charge								
			DM/ BM								
	Loan/Investment										
18	Monitoring, follow up and supervision	Ensure collected clients stock report, trade license, copies of income tax return, financial statement.	Desk officer								
			Credit In-charge								
			DM/ BM								
19	Reports/ Returns/ Statements on loan/Investment	Ensure timely submission of all quarterly returns & statements to Head Office, BB and Regulatory bodies.	Desk officer								
			Credit In-charge								
			DM/ BM								
	Foreign Trade										
20	Monitoring, follow up and supervision	Follow up over due bill of Entry, EXP. Properly.	Desk officer								
			Fex In-charge								
			DM/ BM								
21		Follow up overdue PAD/MIB, LTR/MPTIR properly.	Desk officer								
			Fex In-charge								
			DM/ BM								
22		Follow up overdue LDBP/IDBP, FDBP & PC properly.	Desk officer								
			Fex In-charge								
			DM/ BM								

23		**Ensure Export performance register has properly been maintained.**	**Desk officer**								
			Fex In-charge								
			DM/ BM								
24	**Reports/ Returns/ Statements on Foreign Trade**	**Ensure timely submission of all quarterly returns & statements to Head Office, BB and Regulatory bodies.**	**Desk officer**								
			Fex In-charge								
			DM/ BM								

Annexure-D: Quarterly Operations Report (QOR)

Bank Name

QUARTERLY OPERATIONS REPORT (QOR)

Date :

From : Branch Manager, _____ Branch, _____

To : Head of Internal Control & Compliance Division (IC&CD)

Copy : Head of Banking Operations Division (BOD)

Subject : Quarterly Operations Report for the quarter ended on ……..

(A) POLICIES, PROCEDURES AND CONTROLS

1. **BANGLADESH BANK INSPECTION:**

The Branch/Centre was last audited by Bangladesh Bank on ……..

We confirm that adequate corrective actions have been initiated to remove the deficiencies excepting the followings:

Audit Paragraph's Number	Original Target Date of Rectification	Revised Target Date (If applicable)

2. **BANK'S INTERNAL CONTROL:**

The Branch's/Centre's operational functions were also last audited by the Internal Control & Compliance Division on _____. We confirm that adequate corrective actions have been initiated to remove the deficiencies excepting the followings:

Audit Paragraph's Number	Original Target Date of Rectification	Revised Target Date (If applicable)

3. **OTHER THAN BANGLADESH BANK:**

We confirm that regulatory requirements as outlined by other than BB has been complied with except the following(s):

Audit Paras Number	Target Date of Rectification	Revised Target Date (If applicable)

4. **CLOSED CIRCUIT TELEVISION (CCTV):**

We confirm that operations and recording of day's activities in CCTV installed in the branches and ATM's where applicable have been checked regularly. The recorded cassettes are being controlled as per instructions from Head office.

Exception (if any):

No. of CC Camera	No. of Inoperative Camera	Recording (Yes/No)	Remarks

5. **COMPUTER ACCESS**:

a. We confirm that a full review of "Access Levels" is made to ensure that no conflicts exist and no official is holding both IDs to input transactions and authorize such transactions.

Exception (if any):

No. of IDs	Name of the Officers	Type of Transactions

b. We also confirm that Administrator Passwords are held in dual custody and the both custodians review the Administrator Journal Report and the Audit Trail Report (which reports all user access maintenance) and investigate all activities on a daily basis.

Exception (if any):

Date	Name of the Officers	Type of Reports

6. **CUSTOMER SERVICES STANDARDS:**

The Customer Services Standards of all departments have been checked and documented as per guidelines from Head Office/ Regional Office. The shortfalls detected during the last quarter have been/will be removed within the target set.

Exception (if any):

Date	Name of the Departments	Remarks

7. **DEPARTMENTAL CONTROL FUNCTIONS CHECK LISTS:**

a. The DCFCLs were completed and documented as per Head Office Guidelines by the concerned departments which are being/have been verified by the designated independent officials on _____

b. We confirm that no shortfalls have been identified by the Independent Reviewer and/or the shortfalls identified by him/her are being rectified and will be completed by _____ under advice to Head of Compliance.

8. **INTERNAL CHECKS:**

We confirm that all Internal Checks as per Head Office Guidelines applicable to us are being undertaken by the Independent officials designated in writing. All papers and the reviewer's certificates are retained under the control of the Unit Head/Branch Manager/Designated official for future review by the Bangladesh Bank audit team/ Internal Control Team.

_____	_____	_____	_____
GB In-charge	Inv- In-charge	FEX- In-charge	Deputy Manager/ Manager

9. **LOAN/ INVESTMENT SECURITY DOCUMENTS:**

We confirm that "Loan/ Investment Documentation Check List" for all Investment/ Advances is being sent to the Loan/Investment Administration Division/ Concern Department/ Internal Control Team Head office for review and all Loan/Investment Security Documents is retained as per HO Sanction.
We confirm that:

Sl	Particulars	Yes/No	Remarks
1	Safe In Safe Out Resister maintained properly		
2	Document Jacket maintained properly		
3	Stamp on Charge documents affixed properly		
4	Internal Investment Risk Rating System (IIRRS) done in all applicable cases		
5	Environmental & Social Due Diligence (ESDD) done in all applicable cases		

_____ _____
Credit In-charge Deputy Manager/ Manager

10. **TREASURY/ ID OPERATIONS:**

We confirm that all required processes related to Treasury Operations/ID (e.g. LC Opening, Export-Import Documentation, Foreign Remittance Documentation etc.) have been duly completed by the designated officer(s). All papers/documents are retained under the control of the Unit Head/Branch Manager/Designated official for future review by the Bangladesh Bank Inspection Team/ Internal Control Team.

_____ _____
FEX- In-charge Deputy Manager/ Manager

11. **COMPLAINTS:**

We confirm that complaint letters received from Customers were dealt with in terms of Head office guidelines. All complaints in the form of statement including pending complaints of previous quarter have been forwarded to Complain Cell for review.

_____ _____
GB In-charge Deputy Manager/ Manager

12. **RECOVERY OF COSTS:**

We confirm that the costs of swift and other charges have been recovered from the Customers/Correspondents where applicable and credited to the appropriate Recoveries Accounts under Expenses Head.

13. **FRAUDS, FORGERIES & OPERATING LOSSES:**

Following transaction(s) involving Frauds/Forgeries/Other Operating Losses has/have been detected during the quarter ended on _____ and reported to Head Office/ Concerned Division/ Bangladesh Bank / Internal Control & Compliance Division

Date	Nature of Fraud/Forgeries/ Operation lapses	Remarks

14. **RETURNS:**

We confirm that returns to Head Office /Zonal Office/ Bangladesh Bank including those under Calendar of Returns have been submitted within the schedule dates except the following:

Title of Return	Due Date	Reasons for Delay	Sent on

15. **LEGAL:**

We confirm that legal matters are being monitored by us as per Legal Unit, Head Office/Zonal Office/ Internal Control Units. Return for this quarter has been submitted to Concerned Division on ……

16. **COMMUNICATIONS:**

Following meetings were held during this quarter to improve communication among the members of Officer/Staff. We enclose a copy of the minutes of the meetings held for information and record.

Date & Time	Subject of discussions/ or Agenda in brief	Suggestions/Outcome/ Recommendations

17. **FIXED ASSETS:**

We confirm that:

a) All items of Fixed Assets deployed to the branch have been included in the respective departmental lists and physical check of all departmental Fixed Assets has been undertaken and verified with the departmental inventories.

b) The entries passed through Profit and Loss A/c in respect of sale of Fixed Assets for the half year ended ---------- have been reviewed to ensure that no entry is outstanding in the books.

c) Returns as on----------showing the Fixed Assets sold during the quarter have been prepared & reviewed for tax purposes

d) Fixed Assets of the Branch as on ---------- have been physically checked by the independent officers designated by Branch.

(B) PROTECTION OF VALUABLES

18. **CHANGE OF KEYS:**

We confirm that the Key Register is being maintained as per prescribed procedure and keys were changed with the duplicates as under-

Lastly Changed Date	Bank Name /Branch Name	Remarks

19. **SAFE CUSTODY:**

We confirm that Safe Custody items are being maintained under dual custody and the Last complete independent physical verification of Safe Custody items as per Head Office/ instructions was undertaken on ……. We enclose a copy of the certificate received from the designated reviewer(s).

CUSTODIAN – 1	**CUSTODIAN – 2**	**CUSTODIAN– 3**
Name:	Name:	Name:
Designation:	Designation:	Designation:

20. **SAFE DEPOSIT LOCKERS (Applicable to the branches where lockers are installed):**

We confirm that keys to unrented lockers are kept in sealed envelopes under dual control and spare locks and surrendered keys pending change of locks and keys are controlled by two independent custodians who have no access to locker custodian's key(s)

We confirm that Half Yearly and Yearly Internal Checks are conducted at the prescribed Frequencies by the independent designated officials.

We also confirm that security Money & yearly charges have realized from the Customers and credited to the appropriate Accounts Head.

Exception (if any):

Name of the Customers	Security Money	No. of overdue years	Overdue Amount	Remarks

CUSTODIAN – 1	**CUSTODIAN– 2**
Name:	Name:
Designation:	Designation:

(Item 3 applies to branches/centers where lockers are installed)

21. **CONTROLLED/ SECURITY STATIONERY:**

All Controlled /Security Stationery are being kept under dual custody and Bulk/Working Stocks are being verified as per instructions from Head Office / Zonal Office

22. **CASH/ FOREIGN MONEY etc. :**

Cash (Local/Foreign Moneys) are being dealt with as per requirements – Physical verifications also being carried out at the frequencies prescribed.

23. **CHEQUE BOOK:**

Balancing of Cheque Books are verified during the quarter

24. **PAYMENT ORDER:**

Leaf Balancing of Payment Orders are verified during the quarter.

(C) COMPUTER AND SOFTWARE MAINTENANCE:

25.

Sl	Particulars	Details	Yes / No
1	Computers:	Physically checked and found in order.	
2	Software Maintenance	Checked through system for any deviation	
3	Computer Logs and others	Checked as described in the ICT Guideline of the Bank	

* (if there is anything to report should be prescribed.)

(D) PROOFS / VERIFICATIONS:

26. All accounts in General Ledger (GL)/ Subsidiary Ledger were proved and verified during the quarter except the following accounts.

Title of GL/ SL Account	Difference Amount	Date Last Reconciled	Target Date/ Date Reconciled

We confirm that all outstanding entries in General Suspense (Assets & Liabilities) are being followed up for early liquidation. We enclose the statements of General Suspense Accounts as on ---------- for your perusal.

27. **DIFFERENCE ACCOUNTS:**

We enclose a summary showing the outstanding in Difference Accounts. The entries relating to differences are being investigated. All unresolved entries will be adjusted in terms of approval of Head Office.

28. **BRANCH MANAGER APPROVAL:**

We confirm that all kind of A/C's opened duly approved by Branch Manager & Deputy Manager & no pending issues in this quarter.

Exception (if any):

No. of A/Cs	Reason	Remarks

_____ _____

Deputy Manager Branch Manager

29. **THANKS LETTER:**

We confirm that letter of thanks issued to all A/c holders & Introducers after opening of A/c and acknowledgement thereof is received & no pending issues in this quarter as per Head Office Guidelines.

30. **BALANCE CONFIRMATION CERTIFICATE:**

We confirm that Balance Confirmation Certificate Provided to all A/c holders during the half year ended June and December and acknowledgement thereof is received as per Head Office Guidelines.

Exception (if any):

No. of A/Cs	Reason	Remarks

(E) PERSONNEL & SUPERVISION

31. Following transfers/movements were affected during the quarter (**both Officers and Unionized Staff).**

Name	From (Dept./Br.)	Period worked In this department/Br.	Transferred To (Dept./Br.)	W.E.F. (Date)

32. **LEAVE PROGRAMMES**

a) Officers/staff are being granted leave as per leave programme. (Exception are given below):

Name	Category of Staff	Numbers of days accumulated

b) Arrangements have been made to allow all employees including management staff to avail of 10 days uninterrupted leave or half of annual leave entitlement, whichever is the lesser in terms of service rules.

33. **TRAINING PROGRAMME:**

Following Officers / staffs are undergoing training / have undergone training during the quarter

Name Participant	Name of Course attended	Duration of Course	Course Conducted by

(F) PREMISES MANAGEMENT

34. **FIRE/SAFETY STANDARDS:**

a) Following items have been checked during the quarter ended ----------.

Sl	Particulars	Standard Achieved/ Shortfalls detected
1	Fire Extinguisher-	
2	Burglary Alarm	
3	Intruder Alarm	

b) Half-yearly Self Audit of Fire/Safety Standards was undertaken and the return submitted to you for the period ended ---------- by a separate letter on …….

c) We confirm that:

SL	Particulars	Yes/No	Remarks
1	Fire Drill was carried out half-yearly in terms of Emergency Evacuation Standards of Fire / Safety procedures		
2	Security Drill was carried out regarding Audible Tellers Counter Alarm Protective System and documented		
3	Recording of the arrival and departure time of all personnel occupying the Premises outside working hours and after banking hours are being documented/reviewed on the Registers maintained for these purposes.		
4	Cartridge (Gun) was tested (Supported by certificate) on ……..		
5	Telephone numbers of the local Police Station, the nearest Fire Brigade Office, Branch Manager, Deputy Manager and Cash In charge are noted in a small board & hung in a convenient place within the Branch Premises.		
6	Notice Board is placed in a conspicuous place in the branch and Bank's latest financials, rate of profit on different Deposit & Scheme A/c are shown through the Notice Board.		
7	Signboard of Bank, ATM Booth, Locker facility are displayed at conspicuous place of Branch in good condition.		
8	Buying and selling rates of foreign currencies are displayed.		
9	"Complaint" Box is set in the appropriate place of the branch		
10	Business hours and time is displayed at conspicuous place of Branch.		

d.) All electric wiring were checked by M/s …..…on …..…during the quarter ------- and certificates kept in file for future audit / inspection. We enclose a copy of the certificate for our record.

e). The premises were inspected on holidays by the officers on rotation. Immediate action was taken on shortfalls detected through the checklist maintained which is retained after taking appropriate action as applicable for future audit/inspection.

Confirmation on Regulatory Compliance

(G) REGULATORY COMPLIANCE:

35. **Regulatory Compliance:**

We confirm that regulatory requirements in Bangladesh as outlined by Bangladesh Bank / other Govt. Body have been complied with except the following:

Sl.	Subject of Regulatory Compliance	Legislation	Reasons for Non Compliance	Compliance Risk	Remarks

36. Following issues /objects have been checked during the quarter ended ----------.

Sl.	Particulars	Yes/ No	Remarks
1	Existing IT System Security-		
2	IT System Utilization and Operation Capacity-		
3	Payment System Security Monitoring (ATM & Mobile Banking)-		
4	Inclusion Banking Monitoring (SME, Female Entrepreneurship and Green Banking related -compliance monitoring)-		
5	Branch Anti Money Laundering Reporting/ Monitoring -		
6	Investment Monitoring Report-		
7	CL Checking-		

_____ _____

Deputy Manager **Branch Manager**
Name – Name –
Designation- Designation

Annexure-E: Loan/ Investment Documentation Checklist (LDCL)

LOAN/ INVESTMENT DOCUMENTATION CHECKLIST (LDCL)

Client:	:	
Registered Address:	:	
STATUS:	:	Individual / Proprietorship / Partnership / Limited Company
A/C No.	:	

First obtain General Documents. Then identify the Collaterals, Facility (ies) and obtain specific documents listed hereunder: Leave out documents not mentioned in Credit/Investment Approval and Sanction Letter.

Sl. No	Description	Reqd. (√)	Date of Doc.	Date Received	Expiry	Original Doc Located In	Taka Amount
A.	**General Documents**						
1.	Letter of Loan/Investment Client requesting for new facilities / renewal						
2.	Authority for availing of Loan/Investment facility(ies) (Letter of authority from partners in case of Partnership concern and resolution in case of Limited company) – with list of Partners/Directors						
3.	Form XII certified by RJSC regarding list of existing Directors for Limited company						
4.	Facilities Advice Letter: accepted unconditionally by Loan/Investment Client						
5.	Demand Promissory Note						
6.	Letter of Continuity						
7.	Deed of Partnership (for Partnerships; Loan/Investment Client / third party), By-Laws etc.						
8.	Memorandum and Articles of Association (for limited company Loan/Investment Client / third party) with Certificate of Incorporation						
9.	Letter of Arrangement						
10.	Letter of Disbursement						
11	Revival Letter (Form I & II)						
B.	**Lien of Account**						
1.	Resolution to lien account proceeds (Third Party partnerships and Ltd Companies.)						
2.	Letter of Lien and Set- Off (Pledge Agreement)						

Sl. No	Description	Reqd. (√)	Date of Doc.	Date Received	Expiry	Original Doc Located In	Taka Amount
C.	**Pledge of Deposit Receipts**						
1.	Resolution to deposit (for Third Party partnerships and Limited company)						
2.	Term Deposit Receipts						
3.	Letter of Guarantee by depositor (if the deposit stands in the name of Third Party)						
4.	Letter of Lien and Set Off (Pledge Agreement)						
5.	Letter of Authority for encashment of TDR						
D.	**Pledge of demat Shares**						
1.	No Objection Certificate (NOC) from the competent authority of the Company whose shares are to be pledged						
2.	Pledge Request Form (PRF) i.e., Form 17-1 and Form 17-2 duly filled in and signed by the Pledgor and the Pledgee						
3.	Confiscate Request Form (CRF) i.e., Form 19-1 duly filled in and signed by the Pledgor and the Pledgee						
E.	**Pledge of Inventory**						
1.	Letter of Pledge / Pledge Agreement						
2.	Letter of Disclaimer (if required)						
3.	RJSC Search Report (for limited company partnerships; Loan/Investment Client / third party)						
4.	RJSC Form 18, and receipt of filing with RJSC						
5.	Certificate of registration from RJSC						
6.	Modification of Letter of Pledge / Pledge Agreement of Inventory						
7.	RJSC Form 19, and receipt of filing with RJSC						
8.	Insurance Policy with SJIBPLC as jointly insured						
F.	**Hypothecation of Inventory**						
1.	Resolution to hypothecate inventory (for Third Party partnerships and Limited companies.)						
2.	Letter of Hypothecation of Inventory / Hypothecation Agreement						

Sl. No	Description	Reqd. (√)	Date of Doc.	Date Received	Expiry	Original Doc Located In	Taka Amount
3.	RJSC Search Report (for Limited company. partnerships; Loan/Investment Client/third party)						
4.	RJSC Form 18, and receipt of filing with RJSC						
5.	Certificate of registration from RJSC						
6.	Modification of Letter of Hypothecation of Inventory						
7.	RJSC Form 19, and the Receipt of filing with RJSC						
8.	Insurance Policy - jointly insured						
G.	**Trust Receipt**						
1.	Trust Receipt Agreement						
H.	**Hypothecation of Receivables/Book Debts**						
1.	Resolution to hypothecate receivables / book debts (for Third Party partnerships and limited company)						
2.	Letter of Hypothecation of Receivables / Book Debts (Hypothecation Agreement)						
3.	RJSC Search Report (for limited company/registered partnerships; Loan/Investment Client/third party)						
4.	RJSC Form 18, and receipt of filing with RJSC						
5.	Certificate of registration from RJSC						
6.	Modification of Letter of Hypothecation of Receivables						
7.	RJSC Form 19, and receipt of filing with RJSC						
	I. Hypothecation of Machinery and Equipment						
1.	Resolution to hypothecate inventory (for Third Party partnerships and Limited companies)						
2.	Letter of Hypothecation of Machinery and Equipment / Hypothecation Agreement						
3.	RJSC Search Report (for Limited company. partnerships; Loan/Investment Client/third party)						
4.	RJSC Form 18, and receipt of filing with RJSC						
5.	Certificate of registration from RJSC						

6.	Modification of Letter of Hypothecation of Machinery & Equipment						
7.	RJSC Form 19, and receipt of filing with RJSC						
8.	Latest list of machinery & equipment						
9.	Insurance Policy with SJIBPLC as jointly insured						
J.	**Assignment of Receivables**						
1.	Resolution to assign receivables (for Third Party partnerships and Limited companies)						
2.	Deed of Assignment of Receivables						
3.	Notification and acknowledgement of assignment and confirmation of receivables from the debtor						
K.	**Mortgage**						
1.	Letter of nomination of third party mortgagor from Loan/Investment Client with attested specimen signature of mortgagor						
2.	Resolution to mortgage and guarantee (for Third Party partnerships and limited company)						
3.	Copy of valid ID (for Third Party individual mortgagor)						
4.	Personal Guarantee from Third Party mortgagor						
5.	Original title deeds of mortgagor and previous owners (Bia- Deed)						
6.	C.S., S.A. and R.S. Parchas						
7.	Mutation Parchas in mortgagor's name, certified by Assistant Commissioner of Land						
8.	Duplicate carbon receipt for mutation case						
9.	Letter of No Objection of Lessor for mortgagor to mortgage (for leasehold property)						
10.	Land development tax receipts of the immediately preceding Bangla year						
11.	Municipal holding tax receipts for property in municipalities						
12.	Building/factory plan with letter of approval						
13.	Real Estate Appraisal / Valuation report						

14.	RJSC Search Report (for limited company/registered partnerships; Loan/Investment Client/third party)						
15.	Memorandum of deposit of title deeds (for equitable mortgages) with legal counsel's approved draft.						
16.	Mortgage Deed and registration receipt endorsed by mortgagor (for legal/Registered mortgage) along with Power of Attorney						
17.	RJSC Form 18, and receipt of filing with RJSC if property in the name of ltd cos.						
18.	Certificate of registration from RJSC						
19.	Modification of Memorandum of deposit of title deeds						
20.	RJSC Form 19, and receipt of filing with RJSC						
21.	Income Tax Clearance Certificate as required for Registration						
22.	Non Encumbrance Certificate from Land Registrar						
L.	**Guarantee**						
1.	List of Directors/Partners with specimen signatures, certified by company secretary or Chairman, or Managing Partner (for Limited company and partnerships)						
2.	Resolution to guarantee (for Limited company and partnerships)						
3.	Net Worth Statements (NWS) for individuals/guarantors						
4.	Letter of Guarantee						
5.	Letter of Counter Indemnity						
M.	**Term Loan/Investment Agreement**						
1.	Term Loan/Investment agreement between Loan/Investment Client and the Bank						
2.	Draft Term Loan/Investment Agreement approved by Head of Credit Risk Management Division and Legal Counsel.						
N.	**Security Sharing Agreement**						
1.	Security Sharing Agreement						
2.	Draft Security Sharing Agreement approved by Head of Credit Risk Management Division and Legal Counsel.						

O.	**Syndication**						
1.	Accepted Mandate Letter						
2.	Accepted Term Sheet						
3.	Information Memorandum						
4.	Participation letters						
5.	Facilities Agreement						
6.	Powers of Attorney of participants						
7.	Accepted Fee Letter						
8.	Legal counsel's opinion						
9.	Head of Credit Risk Management and Legal Counsel approval of documents.						
P.	**Other Documents**						

		Name	**Date**	**Signature**
Credit In-charge	:			
Deputy Manager/RM	:			
Manager/CAD	:			

Annexure-F: Sample Annual ICMS Report on Health of the Bank

Health Grading Score Sheet
As on December 31, 20..

90 & Above Excellent
80-89 Very Good
70-79 Good
60-69 Satisfactory
Below 60 Marginal

Total Score Obtained	**80**
Result	**Very Good**

Sl. No.	Particulars	Parameter Range	Actual Parameter	Assigned Value	Score Obtained
I)	**Earning Success**				
	Operating Profit Growth	25% &Above 20%-25% 15%-20% Below 15%		10 8 6 3	
	Net Interest Income Growth	20% & Above 15%-19% 10%-14% Below 10%		5 4 3 2	
	Non-Interest Income Growth	40% & Above 30%-39% 20%-29% Below 20%		5 4 3 2	
	Return on Asset (ROA)	2%-3% 1%-2% Less than 1%		5 3 1	
	Return on Average Equity (ROAE)	25% & Above 20%-24% 15%-19% Below 15%		5 4 3 2	
		Total Earning Success Score (out of 30)			
II)	**Liquidity Health**				
	CRR and SLR	Above 17%* (9.5%**) 17%* (9.5%**) Below 17%* (9.5%**)		2 3 0	
	A-D Ratio and Interbank Dependency	Above 85% (above 92.0%**) 80%-85% (87-92%**) 70%-79% (82-86%**) Below 70% (below 82%**)		0 2 1.5 1	
		Total Liquidity Score (Out of 5)			

III)	**Solvency**				
	Core Capital to RWA ratio (As per Basel-III)	Above 10% 7%-10% 4.5%-7% Bellow 4.5%		5 4 3 0	
	Capital Adequacy Ratio (As per Basel-III)	Above 10% 8%-10% 6%-8% 4%-6%		3 2 1 0	
	Growth of Capital/ Shareholders' Equity	20% & Above 10%-20% Bellow 10%		2 1 0	
		Total Solvency Score (Out of 10)			

Sl. No.	Particulars	Parameter Range	Actual Parameter	Assigned Value	Score Obtained
IV)	**Deposit Health**				
	Deposit Growth	25%-30% 20%-24% 15%-19% Less than 15%		5 4 3 2	
	Deposit Mix (% of High Cost Deposit)	100%-86% 85%-71% 70%-56% 55%-31%		1 3 4 5	
	Cost of Fund	12%-14% 10%-12% 8%-10% 6%-8%		4 6 8 10	
	Core Deposit to Total Deposit	81%-100% 71%-80% 60%-70%		5 3 1	
		Total Deposit Score (Out of 25)			
V)					
	Loans and Advance Growth	25%-30% 20%-24% 15%-19% 10%-14% 5%-<10%		5 4 3 2 1	
	Segment-wise Concentration (% of concentration (LTR+PAD) to total Loans and Advances)	10%-15% 16% - 21% 20% - 25% Above 25%		5 4 3 2	

	Sectoral Diversification (As a % of Industrial/Manufacturing Loan to Total Loans & Advances)	25%-34% 35%-44% 45%-54% Above 54%		5 4 3 2	
	Concentration of Loans (Large Loan to Total Loans and Advances)	Above 60% 56-60% 50-55% Below 50%		2 3 4 5	
	Asset Quality (NPL Management)	5% & Above 3%-5% 0%-3%		2 6 10	
		Total Loans & Advances Score (Out of 30)			
				Total Score	

* CRR and SLR are subject to change as per Bangladesh Bank directives from time to time.

** CRR, SLR and ID Ratio for Islami Banking

Annexure-G: Sample of Shariah non-Compliance Risk Rating:

Sl. No.	Category of Risk Factor	Allocated Marks
1	2	3
1	For 2 types of Major Violations	(16x2/2)=16
2	For 5 types of other Major Violations	(6x5)=30
3	For 18 types of Minor Violations	(2x18)=36
4	For 2 types (Employee + Client) lacking motivational activities	(3x2)=6
5	For 2 types lacking other activities related to Shariah	(2x3)=6
6	For 6 types lacking other activities	(1x6)=6
	Total	**100**

1) Score 16 (8x2) @ 8 for each kind of non compliance of 2 types Major Shariah violations (See structure 1 for scoring):

Sl. No.	Types of Shariah Non-Compliance	Allocated Marks for violation	Allocated Marks as per doubtful income	Allocated Marks as per volume of violation	Score
		Score out of 16 (always gets full marks)	Score out of 16	Score out of 16	Average
1	*2*	*3*	*4*	*5*	*6*
1	Cash Facility Provided in Bai Murabaha and BaiMuajjal. [Except Buying Agency]				
2	Old investment liability adjusted by creating new investment A/C. [Including Conversion]				
	Total				

2) Score 30 (5x6) @ 6 for each kind of non-compliance of 5 types of others Major Shariah violations (See structure 2 for scoring):

Sl.No.	Types of Shariah Non-Compliance	Allocated Marks for violation	Allocated Marks as per doubtful income	Allocated Marks as per volume of violation	Score
		Score out of 6 (always gets full marks)	Score out of 6	Score out of 6	Average
1	2	3	4	5	6
1	Cash memo obtained in the name of the investment client				
2	Existence of the supplier not found				
3	Investment given on the Shariah prohibited item				

Sl.No.	Types of Shariah Non-Compliance	Allocated Marks for violation	Allocated Marks as per doubtful income	Allocated Marks as per volume of violation	Score
4	Charging of rent on the asset before it becomes usable/ rentable				
5	Amount of cash memo is less than the investment				
Total					

3) Score 36 (18x2) @ 2 for each kind of noncompliance of 18 types Minor Shariah violations (See structure 3 for scoring):

Sl.No.	Types of Shariah Non-Compliance	Allocated Marks for violation	Allocated Marks as per doubtful income	Allocated Marks as per volume of violation	Score
		Score out of 2 (always gets full marks)	Score out of 2	Score out of 2	Average
1	*2*	*3*	*4*	*5*	*6*
1	Client received the goods instead of the Branch from the sellers directly				
2	No record of possession of goods by the branch				
3	Cash memo/Bill/Challan/Transport receipt not found				
4	Letter of Authority not taken in case of MPI				
5	Letter of Authority not taken in case of dealership				
6	Post purchase inspection report by the Branch not found				
7	Delivery of asset was not made to the client in case of HPSM				
8	Charging of profit at agreement stage in case of Bai Salam				
9	Selling of Bai Salam goods through the client without engaging him as selling agent				
10	Amount of cash memo exceeds the investment				
11	Agreement kept blank				
12	Post dated cash memo obtained				
13	Investment Client himself is applicant of TT/DD/PO				
14	Engagement of buying agent in Bank's unapproved item				
15	Investment made to the client without engagement of buying				

Sl.No.	Types of Shariah Non-Compliance	Allocated Marks for violation	Allocated Marks as per doubtful income	Allocated Marks as per volume of violation	Score
		Score out of 2 (always gets full marks)	Score out of 2	Score out of 2	Average
	agent				
16	Engagement of buying agent in case of local and single supplier				
17	Cash memo not taken from actual seller or supplier				
18	Back dated cash memo obtained				
	Total				

4) Score 6 (3x2) @ 3 for each kind of noncompliance of 2 types of lacking in motivational activities(Employee + Client) (See structure 4 for scoring) :

Sl.No.	Types of Shariah Non-Compliance	Allocated Marks for violation	Allocated Marks as per number of program	Allocated Marks as per attendee of program	Obtained score
		Score out of 3 (always gets full marks)	Score out of 3	Score out of 3	Average
1	*2*	*3*	*4*	*5*	*6*
1	Lacking in Shariah motivational program for the employees				
2	Lacking in Shariah motivational program for the clients				
	Total				

5) Score 6 (2x3) @ 2 for each kind of non-compliance of 2 types of other Shariah activities (See structure 5 for scoring):

Sl.No.	Types of Shariah Non-Compliance	Allocated Marks for violation	Allocated Marks as per measure of violation	Obtained score
		Score out of 2 (always gets full marks)	Score out of 2	Average
1	*2*	*3*	*5*	*6*
1	Lacking in Offer and Acceptance with the Supplier			
2	Lacking in sending officials to the spot (outside of the branch) to receive/inspect (in case of buying agency) the goods and handover to the client			
3	Lacking in collecting Cash Memos directly by the branch from the suppliers			
	Total			

6) Score 6 (1x6) @ 1 for each kind of Non-Compliance of 6 types of other activities (See structure 5 for scoring):

Sl.No.	Types of Shariah Non-Compliance	Allocated Marks for violation	Allocated Marks as per measure of violation	Obtained score
		Score out of 1 (always gets full marks)	Score out of 1	Average
1	*2*	*3*	*5*	*6*
1	Lacking in giving or/and taking Inter-branch co-operation			
2	Lacking in establishing separate queue or counter for the Woman Clients			
3	Lacking in establishing an effective and efficient purchase cell in the branch			
4	Lacking in conducting dars regularly			
5	Lacking in housekeeping & discipline			
6	Lacking in performing salat in congregation timely			
	Total			

Calculation of Risk related to non-Compliance of Shariah:

Structure: 1

Score will be calculated as below in case of non-Compliance of 2 types major Shariah principles (Sl. No. 1):

Sl.No.	Amount of doubtful income	Score	Number of Shariah violation (Investment A/C Number)	Score
1	2	3	4	5
1	Tk 1-50,000	2	1-3	2
2	Tk 50,001-100,000	4	4-6	4
3	Tk 100,001-300,000	6	7-9	6
4	Tk 300,001-500,000	8	10-12	8
5	Tk 500,000-1,000,000	10	13-15	10
6	Tk 1,000,001-1,500,000	12	16-18	12
7	Tk 1,500,001- 2,000,000	14	19-21	14
8	Tk 2,000,001 and above	16	22 and above	16

Structure: 2

Score will be calculated as below in case of non-Compliance of 5 types other major Shariah principles (Sl.No. -2):

Sl.No.	Amount of doubtful income	Score	Number of Shariah violation (Investment A/c Number)	Score
1	2	3	4	5
1	Tk 1-50,000	2	1-5	2
2	Tk 50,001-100,000	4	6-10	4
3	Tk 100,001 and above	6	11 and above	6

Structure: 3

Score will be calculated as below in case of non-Compliance of 18 types minor Shariah principles (Sl.No-3):

Sl.No.	Amount of doubtful income	Score	Number of Shariah violation (Investment A/c Number)	Score
1	*2*	*3*	*4*	*5*
1	Tk 1-50,000	1	1-5	1
2	Tk 50,001-100,000	1.5	6-10	1.5
3	Tk 100,001 and above	2	11 and above	2

Structure: 4

Score will be calculated as below in case of non-Compliance of 2 types of lacking in motivational activities (Sl.No. -4):

Sl.No.	Number of the program	Score	volume of Shari`ah violation	Score
1	*2*	*3*	*4*	*5*
1	0 (zero)	3	1-49%	3
2	1	2	50-80%	2
3	2-3	1	81-95%	1

Structure: 5

Score will be calculated as below in case of non-Compliance of 2 types of other Shariah principles(Sl. No.-5):

Sl.No.	Percentage of Shariah violation	Score
1	*2*	*3*
1	50% and above	2
2	1-49%	1

Structure :6

Score will be calculated as below in case of non-Compliance of 2 types of other activities (Sl.No. -6):

Sl.No.	Percentage of Shariah violation	Score
1	*2*	*3*
1	50% and above	1
2	1-49%	0.5

Annexure-H: Risks and Opportunities of Virtual Audit Techniques

This annexure provides illustrative examples of key **risks and opportunities** associated with commonly used **virtual audit techniques**. These examples shall assist Audit Team Leaders in selecting appropriate audit methods under a **Risk-Based Internal Audit (RBIA)** framework.

1. Video Call – Synchronous

(e.g. Zoom, Webex, MS Teams, Google Meet)

ICT Tool	Potential Use	Key Risks	Key Opportunities
Video Conferencing	• Audit interviews • Opening & closing meetings • Guided branch / unit walkthroughs	• Risk of data leakage or unauthorized recording • Difficulty in confirming identity if video is not used • Poor audio/video quality affecting understanding • Limited auditor control over camera movement during walkthroughs • Reduced ability to observe behavioral cues	• Enables interviews with staff working remotely or in distant branches • Effective for multi-location audits • Reduces travel time and cost • Suitable where physical observation is not critical

2. Documentary Review with Auditee Participation (Live Sharing)

ICT Tool	Potential Use	Key Risks	Key Opportunities
Screen Sharing / Live Document Review	• Review of policies, vouchers, reports • Walkthrough of system reports	• Risk of data manipulation or selective disclosure • Delays in document availability • Reduced audit depth due to time constraints • Weak interaction compared to on-site review	• Suitable when physical visit is not feasible • Useful for follow-up audits and low-risk areas • Supports multi-branch audits without physical presence • Saves travel cost and time

3. Online Surveys / Applications

(e.g. Google Forms, Internal Survey Tools)

ICT Tool	Potential Use	Key Risks	Key Opportunities
Online Surveys / Questionnaires	• Internal control self-assessment • Preliminary risk identification • Process understanding	• Authenticity of responses cannot be fully ensured • Requires advance preparation and structured questionnaires • Risk of incomplete or inaccurate responses	• Helps understand branch/unit operations before audit • Useful during audit planning stage • Supports focused on-site or virtual audit testing • Enables auditees to prepare for audit

4. Document & Data Review – Asynchronous

(e.g. secure portals, DMS, core banking reports)

ICT Tool	Potential Use	Key Risks	Key Opportunities
Secure Document Access	• Review of SOPs, MIS, system reports • Off-line analysis of records	• Risk of unauthorized access or data leakage • Time-consuming navigation of systems • Limited opportunity for immediate clarification • Auditee may lack visibility of audit scope	• Allows flexible audit scheduling • Enables deeper and independent analysis • Facilitates involvement of specialist auditors • Provides strong audit trails for interviews

5. Live Video Observation (Synchronous)

(e.g. CCTV feed, live stream, controlled camera use)

ICT Tool	Potential Use	Key Risks	Key Opportunities
Live Video / CCTV	• Observation of high-risk operations • Vault, cash counter, ATM activities	• Limited field of view and image quality • Dependence on auditee-controlled camera • Risk of misrepresentation of actual conditions	• Enables observation without physical presence • Useful where safety or access restricts auditor presence • Enhances sampling in high-risk processes • Complements on-site audit activities

6. Recorded Video / Audio – Asynchronous

(e.g. CCTV recordings, call center logs, training videos)

ICT Tool	Potential Use	Key Risks	Key Opportunities
Recorded Media	• Review of past activities • Call center monitoring • Process verification	• Risk of data tampering • Confidentiality concerns • Limited context of surrounding conditions • Incomplete representation of processes	• Enables selective review of key events • Useful for hard-to-reach or remote locations • Improves audit efficiency and sampling • Supports post-event analysis

Note:
Where recorded media contains highly sensitive data or does not meet Confidentiality, Security & Data Protection (CSDP) requirements, such review shall be deferred to on-site audit.