Case Study On
Promoting Operational Efficiency through Internal Control in Meghna Bank

By

Nazmus Sakib Khan

ID: 21164019

MBA Program

A case study submitted to the Brac Business School in partial fulfillment of the requirements for the degree of
Master of Business Administration

Brac Business School
Brac University
December, 2023

Declaration

It is hereby declared that

1. The report submitted is my/our own original work while completing degree at Brac University.
2. The report does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The report does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. I/We have acknowledged all main sources of help.

Student's Full Name & Signature:

Nazmus Sakib Khan
Student ID: 21164019

Supervisor's Full Name & Signature:

Dr. Mohammad Enamul Hoque
Brac Business School
BRAC University

Letter of Transmittal

Dr. Mohammad Enamul Hoque

Brac Business School, BRAC University

Kha 224 Bir Uttam Rafiqul Islam Avenue, Merul Badda,

Dhaka 1212. Bangladesh

Subject: Letter of transmittal

Dear Sir,

I am hereby pleased to submit the case study on "Promoting Operational Efficiency through Internal Control in Meghna Bank". This report was prepared based on my observations during my employment at Meghna Bank for over 03 years. This report is focused to identify how Meghna Bank as a fourth-generation bank of Bangladesh is creating a compliance culture through addressing process loopholes and increasing it's operational efficiency by implementing structured policies and guidelines.

I sincerely hope, sir that you will enjoy reading this report. I would be very happy to provide any assistance in the interpretation of any part of the paper whenever necessary.

Sincerely yours,

____

Nazmus Sakib Khan

21164019

BRAC Business School

BRAC University

Date: April 22, 2024

Non-Disclosure Agreement

This agreement is entered into by Meghna Bank PLC and Nazmus Sakib Khan. The purpose of this agreement is to safeguard confidential information (as defined below) to which the intern may be exposed while seeking experience and training with the company.

1. **Confidential information:** This term refers to proprietary information related to company's business, including, but not limited to, intellectual property, security measures, financial records, proprietary data, new products or services, forecasts, or any other information that, if disclosed, could impact company's business.

2. **Non-disclosure undertaking:** The author hereby commits to refrain from

(a) revealing the confidential information to any external party unless granted written consent by the company beforehand; (b) Reproducing or permitting the replication of the confidential information; or (c) utilizing the confidential information for commercial pursuits.

3. **Return of confidential materials**: Upon the company's request, the author shall promptly return all original materials provided by the company, along with any copies, notes, or documents related to confidential information in the intern's possession.

4. **Term:** This agreement and the intern's obligation to maintain the confidentiality of confidential information shall remain in effect until the earliest of the following: (a) the company provides written notice releasing the author from this agreement, or (b) the confidential information disclosed under this agreement is no longer confidential.

5. **Notice of immunity from liability:** The Intern shall not be subject to criminal or civil liability under federal or state trade secret laws for the disclosure of a trade secret

made (i) confidentially to a government official or attorney for the purpose of reporting or investigating a suspected violation of the law; or (ii) in a sealed complaint or document filed in a lawsuit or other legal proceeding.

6. General clause:

(a) Separability: If any provision of this agreement is deemed invalid or unenforceable, the remaining provisions will be construed in a manner that most closely aligns with the intentions of the parties involved.

(b) Integration: This agreement represents a complete understanding between the parties regarding the subject matter and supersedes all prior agreements. Any amendments must be in writing and signed by both parties.

(c) Waiver: The failure to exercise any right provided in this Agreement shall not constitute a waiver of prior or subsequent rights.

Meghna Bank PLC By: **Shameul Islam** First Assistant Vice President & Head of Compliance & Monitoring Meghna Bank PLC Date:	Nazmus Sakib Khan By: **Nazmus Sakib Khan** MBA Program, Brac University Student ID: 21164019 Date:

Acknowledgement

The successful completion of this report is the result of the contribution and participation of a number of people, especially those who took the time to share their thoughtful guidance and suggestions to improve the report. I want to start by thanking Allah Ta'ala for bestowing upon me the capacity to work diligently under duress.

I have the deepest gratitude to my respectable supervisor and mentor Dr. Mohammad Enamul Hoque, Assistant Professor, BRAC Business School, BRAC University. I owe him a great deal for his guidance, encouragement, and suggestions as well as for giving me access to important material that was essential to finishing this study. Lastly, I would want to express my profound thanks to my friends, family, students, and coworkers who have supported me at all times. I want to express my gratitude to the following individuals for their support:

1. **Dr. Mohammad Enamul Hoque,** Brac Business School, BRAC University
2. **Mohammad Kaiser**, Former Head of Internal Control & Compliance Division & Senior Vice President, Meghna Bank PLC

Table of Contents

Executive Summary

Meghna Bank PLC (MGBL) is one of the fastest growing 4th generation digitalized banks in the country. There is no denying that corporate operations are altering as a result of digital transformation. Organizations have the ability to reinvent how they conduct business and interact with their consumers as they go from using traditional paper and spreadsheets to smart applications to manage their operations. To ensure customer satisfaction, its professionalism, its efficiency and corporate governance, the "Internal Control & Compliance Division (ICCD)" of the bank plays the vital role. It is immense responsibility for the ICCD to guide and monitor a massive portfolio. Therefore, this report contains case study on 03 operational issues with problem identification, reasons and recommendations.

In recent years MGBL is transforming digitally and converted to a centralized bank in terms of banking operations. Still there are some areas where centralization is yet to happen. Meanwhile the Business Operations team is implementing and designing Standard Operating Procedures aligned with Bangladesh Bank's guideline. During this transformation, Business Operations and ICCD teamed up to identify challenges and bring solutions to overcome process loopholes and setting control points.

The Internal Control Department has been reorganized to place more of an emphasis on Internal Control Mechanism and Regulatory Issues. The primary goal of this internal control function is to balance risk and return for the bank; no risk should be unidentified or illogical. The purpose of internal auditing is to offer value and enhance an organization's operations. It is an impartial, unbiased assurance and consulting activity. By applying a structured, methodical approach to assessing and enhancing the efficacy of risk management, control, and governance procedures, it aids a company in achieving its goals. Risk is the possibility of losing something valuable while also having a chance to earn something valuable.

Finally, based on the study and working experience in MGBL some findings along with the analysis are given. The analysis is in brief and simple so that it can be easily understand. At last some clear recommendations are given based on the findings of the study related to Regulatory Requirements, Risk of Fraud due to process lapses, Increasing Operational Efficiency through establishing compliance culture, Developing SOPs, Identifying Process Lapses and the overall analysis on the ICCD of MGBL.

According to the study's findings, ICCD does a job of minimizing risks through complying with relevant rules and regulations of banking services by regulatory bodies.

List of Acronyms

MGBL	Meghna Bank PLC
ICCD	Internal Control & Compliance Division
SOP	Standard Operating Procedures
GL	General Ledger
AML	Anti-money Laundering
BB	Bangladesh Bank
LOD	Liability Operations Department
HO	Head Office
KYC	Know Your Customer
CPV	Contact Point Verification
RBA	Risk Based Audit Guideline
DCFCL	Departmental Control Function Checklist
FAD	Financial Administration Division
BM	Branch Manager
BOM	Branch Operation Manager
CSO	Customer Service officer
PIN	Personal identification Number
CBS	Core Banking Solution

Chapter 1

Organization Background

Meghna Bank PLC began its operation from May 09, 2013 as a stable 4th generation scheduled commercial bank with a vision of "To be recognized as an essential institution for the unbanked through zealous participation in the financial inclusion process". Meghna Bank's Pay-Off line ***"Together We Sail"*** exemplifies the commitment to contribute building up an enlightened and prosperous nation. The Bank offers all kinds of commercial banking activities encompassing a wide range of services including accepting deposits, making loans and advances, card business, treasury management, internet banking, discounting bills, inland and international remittance services, foreign exchange transactions and other related services such as collections, issuing guarantees, acceptances and letters of credit, securities and custodial services etc.

1.1 About Meghna Bank

Vision & Mission

To be among the best service provider in the industry by ensuring complete customer satisfaction through the application of technology, professionalism & nursing.

Core Values

- To remain, at all times, a completely compliant financial institution and a responsible corporate citizen.
- To ensure a sustained growth of the Institution and meet the desired tangible as well as intangible expectations of the Shareholders.
- Customer needs customer care and customer satisfaction to be central to all our operating activities.

- To foster a healthy work-environment and a pleasant in-house culture in order that Meghna Bank is considered an ideal Institution to be associated with.

Establishment

Meghna Bank PLC was established in 2013. It is one of the newer banks in Bangladesh, which was formed with the aim of providing modern and technologically advanced banking services to the people of Bangladesh.

Ownership

Meghna Bank is a private sector bank in Bangladesh, and it is owned by a group of prominent local and international investors.

Services

Like other commercial banks, Meghna Bank offers a wide range of banking services, including retail banking, corporate banking, SME banking, and various financial products such as savings and fixed deposit accounts, loans, trade finance, and more.

Technology

Meghna Bank has emphasized the use of modern technology to enhance its banking services. This includes online and mobile banking, ATMs, and other digital channels to provide convenience to its customers.

Branch Network

As of my last update, Meghna Bank had a network of branches and ATM locations across various regions of Bangladesh. The bank has been expanding its presence gradually to serve more customers.

1.2 Financial position and performance of the Bank

Performance of the bank during 2022 was moderate. Various parameters reflect that the bank maintained to grow in all aspects. Some of the key indicators reflecting growth of the bank are summarized below;

BDT in Million

Particulars	2020	2021	2022
Total Assets	52,871	65,285	64,536
Loans & Advances	35,841	41,876	39,973
Deposits	43,330	52,738	49,535
Total Investments	9,464	15,592	13,796
Total Borrowing	559	2,105	1,620
Shareholder’s Equity	5,997	6,194	6,549
Total Regulatory Capital	6,374	6,740	8,634
Operating Profit	734	1,043	2,250
Net Profit After Tax	501	308	185
EPS	1.00	0.61	0.34
Return on Assets	0.98%	0.52%	0.29%
Return on Equity	8.80%	5.05%	7.66%
Non-Performing Loans	6.80%	5.60%	6.73%

Bank’s total asset and liability decreased by BDT 750 million showing a negative growth of 1% over year 2022. Major reason for the decrease was for decrease in investments in treasury bills, bonds and advances (Annual Report of MGBL, 2022).

Deposits and other accounts decreased by BDT 3.20 billion resulting 1% negative growth over year 2021. Shareholder’s equity increased from BDT 6.19 billion to BDT 6.54 billion in 2022. Also it is observed that, operating profit increased in every year but net profit of the company decreased each year. Major reasons for this are, recruiting employees in numbers for new branches and divisions and creating provision for classified loans.

Chapter 2

Introduction

In recent years, some common problems were identified by ICCD during internal audit at the branches. Those issues were reducing operational efficiency and most of the problems were occurring due to some process loopholes. Some of the issues were exposing the bank to fraud. Major identified issues are;

- Risks of Account Opening Process
- Non-compliance with Internal and External Guidelines
- Process Loophole in Fund Transfer Process

Hence, in the case study, reasons of these problems are explained and significance of the problems are highlighted. The paper also assesses the existing process and policies and compared with existing practice at operational level.

Case Overview

1. Risks of Account Opening Process

Since MGBL's inception, it is developing necessary SOPs for smooth operation and increasing operational efficiency. Though there was guidelines for opening accounts at the branch level, employees were reluctant to comply with those guidelines. As a result internal audit team identified some accounts which had no actual beneficial owner. Each year during audit, these types of accounts were reported in audit reports and referred to business operation team to take initiative. Some accounts were in the names of its customers without their knowledge or consent.

2. Non-compliances with internal & external guidelines

During branch audit, the audit team identified several issues regarding non-compliances with both internal & external guidelines. Since the banking operation has to be operated under the guideline on Bangladesh bank’s instructions, not complying with those guidelines and instructions may lead to expose the bank to disciplinary actions or even penalty.

3. Process Loophole in Fund Transfer Process

A type of payment fraud known as funds transfer fraud occurs when a fraudster starts or reroutes a money transfer from another user such that they receive the funds. While assuming another person's identity or stealing money in the middle of a transfer, the fraudster gives false instructions to a financial institution. Usually fund transfers are occurred by both bank employees and external fraudsters. Fund transfer fraud committed by bankers can occur due to a range of unethical or illegal actions taken by bank employees. These actions can result from the exploitation of their positions and access to financial systems.

Rationale of Study

The purpose of internal auditing is to offer value and enhance an organization's operations. It is an impartial, unbiased assurance and consulting activity. By applying a systematic, disciplined approach to review and enhance the efficacy of risk management, control, and governance procedures, it aids a company in achieving its goals.

Internal control has grown in importance for all organizations in recent years. It aids in the evaluation of our performance at work. Internal control is especially important for banking organizations because they handle other people's money when performing activities. For this internal control, Bangladesh Bank provides some instructions. In this study main concentration is given to the "Promoting Operational Efficiency through Internal Control in Meghna Bank". One of the economic sectors in Bangladesh with the quickest growth is commercial banking. Both the general advancement of society and the advancement of the nation are significantly influenced by commercial banks (Rahman, 2022). As a result, customers now have higher expectations than ever before. Banks, particularly commercial banks, are working to improve their daily, quarterly, monthly, and annual performance in light of the current situation. Bangladesh Bank has published a guideline to guarantee proper governance, prevent corruption, and ensure seamless banking operations. In order to adopt relevant rules and regulations, "GUIDELINES ON INTERNAL CONTROL & COMPLIANCE IN BANKS, September, 2015” acts as bible. Every commercial bank is required to perform its internal control functions in accordance with this guideline as well as their own operation manual and SOPs (Standard Operating Procedure).

Objective

The overall goal of the study is to determine how effective internal control is in Meghna Bank in promoting Operational Efficiency through Internal Control. To do this, it will employ resource-based theory to look at both internal and external factors that affect internal audit effectiveness. While internal variables are those under their control, external factors are those beyond the control of ICCD.

Objectives of the Study

Without well stated objectives, a work cannot be progressed accurately. To be able to concentrate on what one is doing, goals should be established in advance. Picking the objectives carefully is essential because they serve as a roadmap for the job. The following research goals and questions have been developed to achieve the study's objective:

Objective 1: Identifying the loopholes in existing process and policies.

Objective 2: Identifying functions that affect operational effectiveness in Meghna Bank.

Objective 3: Provide recommendation and solution.

Chapter 3

Research Methodology

We do research to either collect some new information about something or find an answer to a problem or to modify existing facts. Research is a big process which has many sections such as defining problems, creating hypotheses or gathering available solutions, organizing and estimating data, studying data, getting to a conclusion & lastly watching the results and verifying whether they fit in or not.

The study necessitates a methodical approach, from topic selection to writing the final report. Data sources need to be located and gathered in order to conduct the study. Key points must be identified and they must be systematically categorized, examined, interpreted, and presented. As a result, both primary sources and secondary sources were used to gather all the material. The majority of the relevant data was practically gathered by carrying out the internal control activity and other data from the bank and related sources.

Gap Analysis

A descriptive research study has been done for this study which has been designed to get the functions that affect operational effectiveness in Meghna Bank. Initially existing policies of Meghna Bank were reviewed and compared the process with actual work flow. If any loophole is identified in process then way out for improvement is suggested. If there is no process loopholes but operations are not running efficiently then establishing a control point is suggested. So, a gap analysis was conducted to identify the gap between actual performance and expected performance. Gap analysis is assessing the performance of a business operation to determine whether business requirements or objectives are being met and, if not, what steps should be taken to meet them. A gap analysis may also be referred to as a needs analysis, needs assessment or need-gap analysis (Jennings. 1999).

Primary Data

- Primary data was gathered base on my working experience in ICCD of MGBL.
- Internal audit & compliance report of MGBL.

Secondary Data

Internal and external sources for secondary data was used in this report and those are:

- Annual reports of MGBL
- Some brochures and related newspaper articles of MGBL;
- Publications obtained from the Internet and from the website of MGBL.

Scopes & limitations of study

By responding to all the research questions, this study has reached its goals. The study still has several shortcomings, though. First of all, the sample size was not very large, so the experiences, perceptions, and opinions given here may not represent the full spectrum of opinions on the efficacy of internal control in MGBL.

Scopes

- Risk based audit guidelines of MGBL.
- Annual audit plan if MGBL.
- Audit methodology of MGBL.
- MGBL operation manual.

Limitations

- This report is based on only the internal control activities of MGBL.

Internal Control & Fraud Management

Internal control is the process, designed to provide reasonable assurance regarding the achievement of objectives in the effectiveness and efficiency of operations, the reliability of financial reporting and compliance with applicable laws, regulations, and internal policies (*GUIDELINES ON INTERNAL CONTROL & COMPLIANCE IN BANKS*, September, 2015).

Internal Control System

An internal control system oversees the entire process in relation to the laws, regulations, tasks, behaviors, and other aspects of a banking company to facilitate its effective and efficient operation by allowing it to appropriately respond to significant business, operational, financial, compliance, and other risks to achieving its goals. The foundation of good and safe banking is strengthened by effective internal controls (*GUIDELINES ON INTERNAL CONTROL & COMPLIANCE IN BANKS,* September, 2015).

Instead of being a structure, internal control is a process. The board of directors and management at all levels within an organization plan, carry out, and track a continuous set of activities. Regarding the accomplishment of the organization's goals, it only offers reasonable confidence, not full assurance.

Internal Control Environment

The board's and management's general attitudes, understanding of the need of internal control, and behavior are all reflected in the control environment. It serves as the basis for the design, implementation, and monitoring of internal controls. It includes of the systems and agreements that protect the bank company from both internal and external threats.

Integrity, moral principles, and competency of the employee are control environment variables, as are the management's working philosophy, the way power is delegated, how responsibility is organized, and how human resources are developed.

Applicable Regulatory Guidelines

Different hazards are involved in the diverse and multifaceted financial activity of banking. In order to guarantee the banking sector operates smoothly, it is crucial to address concerns such as an effective internal control system, sound governance, transparency of all financial transactions, and accountability to stakeholders and regulators. Increased effectiveness in risk management procedures and smooth operation of the banking sector require robust internal control and compliance systems. Internal audit is frequently associated with internal control, but this association is not entirely accurate. By itself, internal control recognizes the risks connected to the process and implements a countermeasure. Internal Audit, on the other hand, is a component of the internal control system that, via routine examination, strengthens the control system. Therefore, internal control is a procedure used by financial firms to offer an acceptable level of confidence in relation to the following main business goals:

- Compliance with policies, plans, procedures, rules, and regulations; the confidentiality, dependability, and integrity of data and information; the protection of its investments and assets.
- the prudent and effective use of resources
- the achievement of stated objectives and programs' or operational goals

Internal controls, in the opinion of the Bank for International Settlement (BIS), can be seen as proactive steps to stop unauthorized charges and guarantee compliance. The structure for the ICCD functions of a bank should be based on *GUIDELINES ON INTERNAL CONTROL &*

COMPLIANCE IN BANKS, September, 2015. In addition to existing concerned legislation, under mentioned manuals are to be meticulously followed by the ICCD people in discharging their responsibilities:

1. Credit Policy Manual
2. Operation Manual
3. Finance and Accounting Manual
4. Treasury Manual
5. HR Policy Manual
6. Internal Control Manual
7. IT Audit Manual
8. Payment System Manual
9. Anti Money Laundering Guidelines
10. Agent Banking Manual
11. Green Banking Manual
12. Guidelines for Foreign Exchange Transactions
13. Basel Core Principles
14. International/Bangladesh Accounting Standard (FRSB)/IAS/BAS
15. Guidelines of Auditing and Accounting Organization for Islamic Financial Institution (AAOIFI)
16. Manual of Islamic Financial Services Board (IFSB)
17. BB Guidelines on Islamic Banking
18. Bank Company Act-1991

Applicable Internal Guidelines

- MGBL Branch Operation Manual, 2022.

- Fraud Detection and Management Policy, July 2019.
- MGBL Internal Control & Compliance Manual, 2014.

Fraud

Fraud is any attempt to cause loss involving deception, this includes but should not limited to: counterfeit, forged or false documents, false or misleading representations or statements or any other act intended to cause loss to the bank, it's employees or customers (MGBL Fraud Detection and Management Policy, 2019). Instances are;

- ATM Fraud
- Cyber crime
- Counterfeit currency
- False accounting
- Fictitious account set up
- Alteration of document
- Fraudulent payments
- Cash theft
- Loan frauds

Fraud Management

Fraud management refers to the processes, strategies, and technologies implemented by organizations to detect, prevent, and mitigate fraudulent activities. Fraud can take many forms, including financial fraud, identity theft, cyber-attacks, and more. Effective fraud management is crucial for protecting an organization's assets, reputation, and the interests of its customers or clients (Aghghaleh, 2014). Here are key components of fraud management:

Detection

Identifying fraudulent activities is the first step in fraud management. Organizations use various methods and tools to detect anomalies, irregular patterns, or suspicious behavior that may indicate fraud. This can include monitoring financial transactions, analyzing customer behavior, and employing fraud detection algorithms.

Prevention

Fraud prevention measures aim to stop fraudulent activities before they occur. This includes implementing security protocols, access controls, and authentication methods to safeguard sensitive data and systems. Educating employees and customers about security best practices is also a vital aspect of prevention.

Investigation

When fraudulent activities are suspected or detected, organizations often conduct investigations to gather evidence and determine the extent of the fraud. This may involve collaborating with law enforcement agencies and forensic experts.

Risk Assessment

Evaluating and assessing the risks associated with different types of fraud is essential. Organizations need to understand their vulnerabilities and take proactive steps to mitigate these risks.

Data Analytics

Advanced data analytics and machine learning techniques are increasingly used for fraud management. These technologies can analyze vast amounts of data to identify patterns and anomalies associated with fraud.

Compliance

Organizations must adhere to legal and regulatory requirements related to fraud prevention and management. Compliance with laws such as the Sarbanes-Oxley Act, Payment Card Industry Data Security Standard (PCI DSS), and Anti-Money Laundering (AML) regulations is essential.

Customer Education

Educating customers and clients about potential fraud risks and how to protect themselves is crucial. This can involve providing guidance on safe online practices, warning signs of scams, and reporting procedures for suspicious activities.

Collaboration

Collaboration with industry peers and sharing of information related to emerging fraud trends can be valuable. Industry-specific organizations and associations may facilitate such collaboration.

Technology Solutions

Various software and technology solutions are available for fraud management, including fraud detection systems, anti-phishing tools, and identity verification services. These technologies can help automate fraud detection and prevention processes.

Continuous Improvement

Fraud management is an ongoing process. Organizations need to continually update and improve their strategies and tools to stay ahead of evolving fraud tactics.

Effective fraud management is essential for protecting an organization's finances, reputation, and the trust of its stakeholders. It requires a multifaceted approach that combines technology, processes, and vigilance to detect, prevent, and respond to fraudulent activities.

Impact of Fraud

Fraud can have significant and far-reaching impacts on individuals, businesses, and society as a whole. These impacts can encompass financial, legal, reputational, and emotional consequences. Here are some of the key impacts of fraud:

Financial Losses

The most immediate impact of fraud is often financial loss. Victims of fraud can suffer direct monetary losses, including stolen funds, unauthorized charges, or financial damages resulting from fraudulent investments or schemes.

Reputation Damage

Fraud can severely damage the reputation of individuals, businesses, and organizations. When customers or clients perceive that an entity cannot protect their assets or personal information, they may lose trust and take their business elsewhere.

Legal Consequences

Committing fraud is illegal, and perpetrators can face legal consequences, including criminal charges, fines, and imprisonment. Additionally, victims of fraud may pursue civil lawsuits to recover their losses.

Emotional Distress

Fraud can cause significant emotional distress for victims. The feeling of being violated, betrayed, or taken advantage of can result in stress, anxiety, depression, and other mental health issues.

Economic Impact

Widespread fraud can have a negative impact on the economy as a whole. It can erode consumer confidence, disrupt financial markets, and lead to increased regulatory and compliance costs.

Identity Theft

One common form of fraud is identity theft, where a person's personal and financial information are used without their consent. Identity theft victims may spend significant time and effort restoring their identity and financial records.

Loss of Opportunities

Fraud can limit opportunities for individuals and businesses. For example, a business that has been a victim of fraud may struggle to secure loans or partnerships, while individuals with compromised credit may face challenges in obtaining financing or housing.

Cybersecurity Risks

Many frauds, especially in the digital age, involve cyberattacks and data breaches. These incidents can expose sensitive information, including personal data and financial details, leading to a heightened risk of further cybercrimes and identity theft.

Regulatory and Compliance Burden

Organizations that fall victim to fraud may face increased regulatory scrutiny and compliance requirements. This can result in additional costs and administrative burdens.

Loss of Time and Productivity

Dealing with the aftermath of fraud, including reporting the crime, recovering stolen assets, and implementing security measures, can consume a significant amount of time and resources for both individuals and organizations.

Impact on Trust

Fraud can erode trust not only between individuals but also between businesses and their customers, suppliers, and partners. Rebuilding trust can be a lengthy and challenging process.

Social Costs

Fraud has broader societal costs, as it diverts resources away from productive activities and towards prevention, investigation, and recovery efforts. These costs can ultimately affect economic growth and prosperity.

In summary, fraud has a wide range of negative impacts that extend beyond financial losses. It can harm individuals' well-being, damage the reputation of businesses and organizations, and undermine trust within communities and the broader society. Preventing and addressing fraud is essential to mitigate these far-reaching consequences.

Type of Fraud

Usually following types of frauds are seen in banking industry;

- Fraudulent fund transfer
- Misappropriation of Assets
- Corruption
- Fake account opening

Chapter 4

Findings of the study

As a 4th generation bank, MGBL is incorporated in the market for only 10 years. Which is comparatively a new bank. As a new bank in the market, MGBL is still in the process of designing new process and policies. For the purpose of study, I have to consider the existing process and policies to identify the deviations between the guidelines and the existing work procedure. I considered the following documents and methods to find the problems and identifying solutions;

1. Review of Investigations report prepared by internal audit team.
2. Review of Branch audit reports.
3. Review of Division and departmental audit reports.
4. Study of Meghna Bank's Branch Operation Manual.
5. Study of Internal Control & Compliance Guideline by Bangladesh Bank.

From the review and study of above-mentioned documents, it was apparent that MGBL has insufficient policies in some cases. Even if there is a policy for a specific operation, employees did not follow the policy. Moreover, a number of investigations were conducted where process is designed and communicated but employees committed fraud by finding loopholes in the processes. So, after designing a process it should be communicated with the end users and employees should be well trained about the new process and policies.

Problem Analysis

In recent past, MGBL's management was experiencing some frauds regarding some products and services which were creating difficulties, losses, excessive operating costs, client security concerns etc. These can make it impossible for a business to carry out its strategy and achieve its goals. When specific conditions apply, Business difficulties put a company's long-term survival in jeopardy. Frauds like fake account opening, issuance of fake bank guarantees, fund transfers without authorization, swindling of funds by employees and fake loans were hindering to achieve organizational goals and also MGBL had to incur losses for these incidents.

As a 4th generation bank, occurring frequent frauds makes it tough to stick with organizational goals and implementing new strategies.

4.1 Risks of Account Opening Process

After conducting several investigations, it was identified that the following issues were working as the *pressure* during account opening process as per Wells' Fraud Triangle;

i. **Business Target**

   While analyzing the natures of frauds, it was apparent that huge business targets were majorly responsible to engage in fraudulent activities. Not meeting business targets are considered as poor performance and this has an impact on yearly performance appraisals. So the employees sometimes want to meet targets by any means.

ii. **Influence from fraudsters**

   Scammers and fraudsters are always searching to take away bank's money through the process loopholes. Sometimes large groups are involved in a financial scam. Usually scammers went to a branch as a customer and submit fake documents to open an account. Moreover they also influence some bankers to work with them.

iii. **Money Laundering**

   Money laundering has 03 stages, Placement, Layering and Integration. Placement is the initial entry of black money in to a financial system. Usually depositing money in a fake accounts is a type of placement. Layering is creating multiple layers of transactions through fund transfers within several accounts. This process requires helps of financial systems and money launderers make some bankers to involve in money laundering activities.

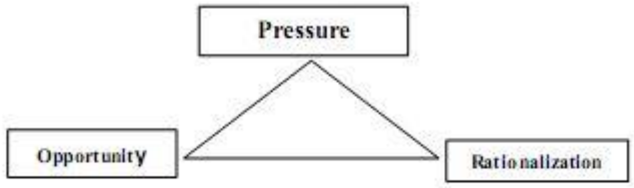

Fig. 1: Wells' Fraud Triangle, Wells, J. T., 2005.

Principles of fraud examination. Hoboken, New York: John Wiley and Sons

For a bank, reputational damage can have serious and far-reaching repercussions. One of a bank's most significant assets is its reputation, and damage to that reputation can have a variety of unfavorable effects, such as:

Regulatory Scrutiny: Regulators frequently keep a careful eye on institutions with a bad reputation. More stringent oversight, fines, and penalties may result from increased regulatory inspection, which might be expensive and time-consuming for the bank.

Legal Liability: Litigation and legal claims may result from reputational difficulties. Customers might file lawsuits in an effort to get paid if they feel they were wronged by the bank's conduct or negligence, for instance.

Employee Morale and Retention: A damaged reputation can affect employee morale and job satisfaction. Employees may become demotivated or worried about job security, leading to increased turnover.

Difficulty in Attracting Talent: Banks with a tarnished reputation may struggle to attract top talent. Highly skilled professionals may be reluctant to join a bank with a history of misconduct or unethical behavior.

Impact on Business Relationships: Reputational damage can strain relationships with business partners, suppliers, and other stakeholders. Counterparties may be hesitant to engage in transactions with the bank, affecting its business operations.

Credit Rating Downgrades: A bank's credit rating can be downgraded if its reputation is seriously damaged. This can increase the cost of borrowing and limit the bank's ability to access capital markets.

Loss of Business Opportunities: A damaged reputation can result in missed business opportunities, as potential clients and partners may choose to work with more reputable institutions.

Long-Term Brand Damage: Rebuilding a tarnished reputation can take years of consistent effort and investment in marketing and public relations. In some cases, the damage may be irreversible.

Mitigation

To mitigate reputational risk, banks must prioritize ethical conduct, compliance with regulations, and transparency in their operations. They should also have crisis management and communication strategies in place to respond effectively to reputational challenges when they arise. Additionally, banks should monitor social media, news, and public sentiment to detect and address emerging reputational threats promptly.

4.2 Non-compliances with internal & external guidelines

While investigation was conducted to identify the reasons behind non-compliances with internal and external guidelines it was observed that, banks fail to comply with internal and external guidelines for a variety of reasons, including organizational weaknesses, inadequate controls, and human errors (Al-Thiban, 2021). Usually auditors observe non-compliances in the following areas at branch level;

i. Management Control
ii. Cash & Cash Area Management
iii. ATM Operations
iv. Customer Service & Reputation
v. Account Opening Procedure
vi. Security Item reconciliation, delivery & destruction
vii. Clearing & Pay order
viii. Credit onboarding
ix. Anti-Money Laundering activities

For the purpose of study, some recurring incidents are identified which had severe impact on bank's overall reputation and financial performances;

a. Onboarding Fake Loan
b. Fraud mortgage
c. Issuance of fake bank guarantee
d. Opening corporate account without Contact Point verification
e. Unauthorized fund transfers from customers' account
f. Money laundering attempts

After analyzing these non-compliances and fraud events, major reasons were identified and those were actually common ways in which banks can fall short of compliance:

I. Inadequate Internal Controls

Lack of clear policies and procedures: Banks may not have well-defined and documented internal guidelines, making it difficult for employees to understand and follow the rules (Rikhardsson, 2021).

Weak monitoring and oversight: Inadequate supervision and oversight can result in employees not adhering to guidelines or taking shortcuts.

II. Human Error

Mistakes in data entry: Errors in data entry can lead to inaccurate reporting or transactions that do not comply with guidelines.

Misinterpretation of guidelines: Employees may misinterpret internal guidelines, leading to non-compliance.

Lack of training: Inadequate training of employees can result in them not fully understanding or being aware of compliance requirements.

III. Cultural Issues

A culture that prioritizes profit over compliance: When banks prioritize profit at the expense of compliance, employees may feel pressure to engage in unethical or non-compliant behavior.

A culture of complacency: In some cases, banks may have a culture of complacency where employees assume that existing controls are sufficient and do not proactively identify and address compliance gaps.

IV. Technology Failures

Outdated or inadequate systems: Legacy IT systems can struggle to keep up with changing compliance requirements, resulting in technology-related non-compliance.

IT glitches or system failures: Technical issues can disrupt processes and lead to non-compliance.

V. External Factors

Evolving regulations: Regulatory requirements can change frequently, and banks may struggle to keep up with the latest rules and guidelines.

Geopolitical and economic events: External events, such as economic crises or changes in government, can impact a bank's ability to comply with guidelines.

VI. Complex Financial Products:

Complex financial products and transactions: Banks may engage in complex financial products and transactions that are difficult to monitor and assess for compliance.

Lack of transparency: Lack of transparency in these products can make it challenging to ensure compliance.

VII. Incentive Structures

Inappropriate incentive structures: Compensation structures that reward risky behavior or short-term gains can incentivize employees to engage in non-compliant activities.

VIII. Outsourcing and Third-Party Risk:

Reliance on third-party vendors: Banks may outsource certain functions to third-party vendors, and if these vendors do not meet compliance standards, the bank can be held responsible.

Mitigation

To address these challenges and improve compliance, banks typically need to invest in robust internal controls, ongoing training and education, effective risk management, and a strong compliance culture. Regular audits, reviews, and assessments can help identify and rectify non-compliance issues. Additionally, staying informed about changing regulations and adapting systems and processes accordingly is crucial for banks to remain compliant with both internal and external guidelines.

4.3 Process Loophole in Fund Transfer Process

ICCD conducted several forensic audit to review and analyze the fund transfer frauds. After analyzing the natures of fund transfer frauds, it is apparent that fund transfer frauds can be categorized in two (02) types;

i. **Unauthorized Fund transfer from customers' account**

These type of frauds can be initiated by both internal and external influence. In phishing scams, fraudsters send emails, text messages, or even phone calls that appear to be from legitimate sources like banks, government agencies, or reputable organizations. These messages typically contain urgent requests for personal or financial information, leading victims to unwittingly share sensitive data or make fund transfers to the scammers.

On the other hand employees sometimes are involved in such type of unauthorized fund transfers. This can take place when both the transaction maker and authorizer are agreed to commit such fraud, in other case either of them took control of both transaction ID to initiate such transaction. Bankers

ii. Unauthorized Fund Transfers from Bank's GL Balance

Unauthorized fund transfer from bank's GL account is only possible when employees of the bank is involved. On that case two or more employees come together with a plan to commit such a fraud. Banks have so many GLs with idle money. Fraudsters target those GLs to transfer those GL balance to an individual or several customers' accounts. To make such type of transactions, both maker and authorizer have to get involved. Later, they withdraw the money from that account.

Mitigation

To protect a bank from fund transfer frauds, individuals and organizations should exercise caution, verify the identity of the other party, avoid sharing personal and financial information unsolicited, and conduct due diligence before making any financial transactions, especially wire transfers (Roy, 2022). Education and awareness are critical in recognizing and avoiding these scams. Additionally, reporting any suspected fraud to relevant authorities can help prevent others from falling victim to similar schemes.

Chapter 5

MGBL's Response to Mitigate Risks & Establish Control Points

Based on the above discussed cases, MGBL management launched some projects and developed Policies and SOPs to implement control point as the first line of defense against these frauds based on the risk appetite capability. Risk appetite refers to an organization's or individual's willingness and ability to accept and tolerate various degrees of risk in pursuit of its objectives or goals. It is a crucial concept in risk management and decision-making processes. Risk appetite helps establish the boundaries within which an entity is comfortable operating regarding risk exposure.

Addressing the risks of fraud in Account Opening Process

Based on the reported issues by ICCD, the management of MGBL took some initiative to mitigate risks of fraud in Account Opening Process. The management's initiatives are;

1. Establishment of Liability Operations Department
2. Implementation of Account Opening & Closing Guideline by LOD

MGBL established the LOD to set control points in account opening process in 2020. LOD implemented an SOP for Account opening and closing guideline and as per the guideline branch had to take approval from LOD to open a bank account. Before that, bank account can be opened in the branch without any HO approval. So, the required documents were not collected in some cases. After establishment of LOD, the branch collects all required documents from customers and send to LOD for approval. Meantime the customer's account status will be locked to “Debit Freeze”. Which means customer cannot withdraw money from his account until he/she submits all required documents to the bank. LOD confirms the KYC and CPV being done properly, AML guideline has been followed to open the account and after satisfaction they enable the account to do all types of transactions.

Addressing the Risk of Non-compliance with internal & external guidelines

Based on the nature of non-compliances found at the branch level and requirement by regulatory authority (BB), ICCD developed a Risk Based Audit Guideline to conduct audit with an intention to mitigate the risk. Risk Based Audit (RBA) Guideline is developed considering the Risks, Impacts and Likelihood of non-compliant issues. Moreover, ICCD developed and reviewed the RBA guideline each year based on the changes of business processes. Based on the RBA guideline, ICCD gives a rating to the branches. Branch rating depends on the type of non-compliant issues found at the branches. Non-compliance issues are categorized in 03 risk levels, which are High, Medium and Low. ICCD also implemented the DCFCL (Departmental Control Function Checklist) at the branch level and head office divisions to make someone responsible for each banking operations. DCFCLs are designed for daily, weekly, monthly and quarterly jobs. DCFCL not only works as a part of internal control, it is also effective as a reminder.

Addressing the Risk of Fund Transfer Fraud

Since MGBL experiences that, employees were engaged in fund transfer frauds, a detail SOP was developed in response to those fraud. To stop unauthorized transactions from GL accounts, the management determined ownership of some GL and one GL account cannot be accessed from other cost centers.

ICCD also instructed the cost centers to generate day-end user-wise transaction listing on each day before closing, to check whether any unauthorized transactions occurred either from customer's account or GL account of the branch. Both Branch Manager (BM) and Branch Operation Manager (BOM) are responsible to verify the transactions made by the CSOs.

In response to a fraud related to fund transfer using debit card of customers, ICCD recommended to establish more security measures to prevent such frauds. Later, debit cards were delivered to the customer directly and no document for PIN number was generated. As per new policy, customer will receive debit/credit card over courier and should make a call from registered number to customer care to set the PIN.

The management also developed a Fund transfer guideline to prevent account to account fraud transfer. Customers now must have cheque leaf to do any kind of fund transfer within MGBL.

ICCD also identified some issues which had a connection for such occurrences, like Human Resource constraints, maintaining workload balance and independent reviewer. Usually each transactions must be checked by one checker and one authorizer. Due to human resource constraints, transactions at the branch level are authorized by the checker only. So, if a maker and checker of a transaction agrees, then fraud can take place.

Since human resource constraints is a common problem all over the organization, workload balance cannot be maintained. As a result, dependency on a single employee is increased and chances of fraud are also exposed. To set a control point, ICCD recommended to appoint an independent reviewer for all transactions and engage concurrent audit where applicable. So that, every transactions will be scrutinized by two different persons.

Chapter 6

Conclusion

The first step for the responsible authorities to do in order to handle these concerns is to establish strict monitoring. Any transaction must be authenticated by the makers-checkers-authorizers in order to be cleared.

The transaction procedure depends heavily on the officials who perform these duties. The transaction is started, the transaction check is then authenticated, and then the transaction is authorized. If those three individuals control the entire procedure, illegal money transactions won't be initiated. It is crucial to keep an eye on each officer's activity because of this. One or two officers managing the entire procedure as opposed to the recommended three usually results in a loophole (Rahman, 2022).

Utilizing the CBS, monitoring is possible through Audit Trails or User-wise transaction report. The security operating system has the ability to track transactions involving large sums of money, defined as those involving more than BDT 1,000,000. Step-by-step verification of the bank-to-bank transaction by designated officers is required. Otherwise, any error will lead to a host of issues. How to check transactions involving sizable sums of money is described in the Money Laundering Prevention Act and various Bangladesh Bank recommendations. There is a chance that fraud will occur if officials disobey the rules and grant check clearance without verification.

What would be perfect to do? A simple phone call to the account holder should be enough for the transaction initiator to determine whether the instruction is legitimate or not. By carrying out the necessary verification, banks must guarantee the accuracy of KYC information. In the verification process, the maker-checker-authorizer concept is used. The likelihood of fraud is zero provided the verification standards are strictly adhered to.

Since Bangladesh is now a digital country, it is logical that our financial services would move to a digital platform. The deployment of ETF through EFTN and RTGS is a solid step in the direction of a fully digital banking system. However, it is important to carefully evaluate the risk considerations related to online banking. Digital banking obviously carries greater hazards than traditional banking. Electronic banking can be highly beneficial if its hazards are accurately identified and reduced, but it can also be risky if the correct controls are not in place (Rahman, 2022). Meghna Bank would advise branches to have proper control while using fund transfers and should revisit this complex service.

Creating a compliance culture in a bank is essential to ensure that the institution adheres to regulatory requirements, ethical standards, and best practices. A strong compliance culture helps minimize risks, maintain trust with customers, and avoid legal issues (Rahman, 2022). Here are steps to create and promote a compliance culture in a bank:

Leadership Commitment: Start at the top. Senior management and the board of directors should demonstrate a strong commitment to compliance and ethics. Leaders should set the tone by consistently following and promoting compliance principles.

Clear Policies and Procedures: Develop comprehensive policies and procedures that outline the bank's compliance expectations. Ensure that employees understand and have access to these documents. Regularly update them to reflect changes in regulations.

Training and Education: Provide ongoing training and education for all employees, including new hires and existing staff. Training should cover not only regulatory requirements but also ethical behavior and the importance of compliance.

Communication: Maintain open and transparent communication channels regarding compliance matters. Encourage employees to report compliance concerns or violations without fear of retaliation. Establish anonymous reporting mechanisms if necessary.

Risk Assessment: Regularly assess the bank's compliance risks. Identify potential vulnerabilities and develop strategies to mitigate them. This includes monitoring changes in regulations that may affect the bank's operations (Wilks, 2005).

Testing and Monitoring: Implement a system for ongoing compliance testing and monitoring. Conduct regular internal audits and reviews to ensure that policies and procedures are being followed and that compliance requirements are met.

Consequences for Non-Compliance: Clearly define consequences for non-compliance with policies and regulations are to be communicated with employees. Ensure that these consequences are consistently applied to all employees, regardless of their position.

Incentives for Compliance: Consider implementing a reward or recognition system for employees who consistently adhere to compliance standards. Positive reinforcement can reinforce the importance of compliance.

Customer Focus: Emphasize the importance of customer protection and satisfaction. Compliance efforts should be seen as a way to protect customers' interests and maintain their trust.

Continuous Improvement: Encourage a culture of continuous improvement in compliance. Regularly review and update policies and procedures to adapt to changing regulatory environments and emerging risks.

External Engagement: Establish relationships with regulators and industry associations. Participate in discussions and collaborate with external parties to stay informed about industry best practices and regulatory developments.

Whistleblower Protection: Ensure that whistleblowers are protected from retaliation and that their concerns are thoroughly investigated. Create a safe environment for employees to report wrongdoing.

Transparency and Accountability: Hold individuals and departments accountable for their compliance responsibilities. Transparency in reporting and accountability for compliance performance are critical.

Lead by Example: Management should lead by example and demonstrate a strong commitment to compliance in their own actions and decisions.

Creating a compliance culture is an ongoing process that requires dedication and vigilance (Roy, 2022). It should become an integral part of the bank's values and operations, instilling a sense of responsibility and commitment to compliance throughout the organization.

References

1. MGBL Fraud Detection & Management Policy, July 2019.
2. Annual Report of Meghna Bank PLC, 2020.
3. Annual Report of Meghna Bank PLC, 2021.
4. Annual Report of Meghna Bank PLC, 2022.
5. Meghna Bank's Branch Operation Manual Version 2.0, 2022.
6. Account Opening & Closing Documents guideline, November 2021.
7. MGBL Tender Security Financing Scheme, 2021.
8. GUIDELINES ON INTERNAL CONTROL & COMPLIANCE IN BANKS, September, 2015.
9. Jennings, Michael D. (1999, March 10). Gap analysis: concepts, methods, and recent results. National Gap Analysis Program, U.S. Geological Survey, 530 S. Asbury St., Suite 1, Moscow, Idaho 83843, USA
10. Aghghaleh, S F. (2014, February 14). Fraud Risk Factors of Fraud Triangle and the Likelihood of Fraud Occurrence: Evidence from Malaysia, Universiti Kebangsaan Malaysia, Malaysia.
11. Kassem, R. and Higson, A.W., 2012. The new fraud triangle model. Journal of Emerging Trends in Economics and Management Sciences, 3 (3), pp. 191 – 195.
12. Wilks, T. Jeffrey (2005). Decomposition of Fraud Risk Assessments and Auditors.
13. Rikhardsson, P., Rohde, C., Christensen, L., & Batt, C. E. (2021). Management Controls and Crisis: Evidence from the Banking Sector. Accounting, Auditing and Accountability Journal, 34(4), 757-785. https://doi.org/10.1108/AAAJ-01-2020-4400.
14. Al-Thiban, M., Tayachi, T., Why Banks Fail?, Palarch's Journal of Archaeology of Egypt/Egyptology 18(13), 560-568. ISSN 1567-214x

15. Rahman, S. (February 06, 2022), Bank fraud: No loopholes in the system, problem lies with people, The Business Standard. https://www.tbsnews.net/interviews/bank-fraud-no-loopholes-system-problem-lies-people-367057
16. Roy, N. (March 30, 2022), Electronic fund transfer needs additional control, The Financial Express. https://thefinancialexpress.com.bd/views/views/electronic-fund-transfer-needs-additional-control-1648565949

Appendix

List of questions and answer from interview:

The interview was conducted with Mr. Mohammad Kaiser, SVP & Head of ICCD and Mr. Md. Mohsin Rony, Principal Officer from Monitoring Unit.

Q1. How does ICCD detect process loopholes?

While ICCD is looking for process loopholes, they focus on some things namely; Risk Assessment, Documents review, Process observation, data analysis, test of controls, benchmarking, continuous monitoring, fraud analysis, follow-up audits. ICCD checks and monitor CBS generated Audit trails for customers' account and GL related transactions. ICCD also confirms that, at the branch level, these monitoring is practiced by the BOM/BM.

Q2. What is the reporting structure of ICCD?

The Head of the internal control is responsible for the both compliance and control related tasks which include compliance with laws and regulation, audits and inspection, monitoring activities and risk assessment. The Head of internal control reports directly to the MD and also have an indirect reporting line to the Audit Committee of the Board.

The Division is comprised of the following three Departments:

i) Internal Audit & Inspection Department

ii) Monitoring Department

iii) Compliance Department

Q3. How does ICCD officials conduct inspections?

Internal audit monitors the functions of the Branches and various Departments / Divisions of the Bank periodically on regular basis. Depending on the requirement Internal Audit will carry out inspection, surprise inspection in order to help avoiding any fraudulent activities which in turn strengthens the Bank to set up sound structural base.

Q4. How does ICCD promote the operational guidelines?

Audit Team will primarily focus on the Process Audit instead of transaction based audit. It will assess the existing work procedure /work flow of each desk of each Department, if the operational activities are done as per MGBL Branch Operation Manual and other applicable internal guidelines and try to find out the efficiency of the procedure, note the lapses if any and suggest measures to be taken to make the process more efficient to overcome the lapses.

Q5. How does ICCD implement the fraud detection process?

Audit Team will emphasize on the Risk Based Audit instead of previous practice of auditing of all the vouchers of each desk irrespective of propensity of inherent risks in the relevant fields. For Risk Based Audit format has been developed and marks have been allowed for related risks depending on their magnitude. A criterion for awarding marks has been mentioned in the format. RBA will determine the risk to which the Branch is exposed.

Q6. How does ICCD conduct the fraud reporting process?

If required, there will be special audit on specific areas of operation in the Branch/HO any time in addition to the routine audit program and there will be special investigation on any issue as and when needed, in any Branch/Division/Department of the Bank.

Q7. How does ICCD set the control points?

ICCD determines the impact and likelihood of an identified issue and based on that, they give recommendations in their report suggesting the effective control points to be established as per best practice.

Q8. What are the ICCD's activities regarding prevention of fraud?

ICCD initiates surprise visit, scheduled audit, spot audit, offsite supervision, GL transaction monitoring, employees' bank account monitoring, follow-up of identified audit issues to prevent fraud and determines the responsible parties for fraud when an investigation is conducted.

Q9. How ICCD identified the risks of Account Opening Process?

ICCD conducts audit at each branch and each divisions once in every year. At the time of branch audit, ICCD officials conducted some verifications of documents relating to account opening forms. From those verifications, fake accounts were identified.

Q10. How those risks were addressed by the bank?

The bank formed a division named Liability Operations division and a policy for account opening with a centralization concept. As per new policy, branches cannot open a bank account by themselves, but they can upload account opening documents in ERP and liability operations division approves an account after getting satisfaction from reviewing documents. Before approval, the account will be inoperative and debit freeze mode.

Q11. How does fake account opening process affect the bank?

Fake account opening exposes the bank for a risk of money laundering and other frauds. Which may lead to financial loss and regulatory penalty.

Q12. What are the main reason for frauds in Account Opening?

Business target, influence from fraudsters and money laundering are the major reason for fraud account opening.

Q13. What are the main reasons for Non-compliances with internal & external guidelines?

Inadequate human resource, lack of training, not circulating the risks of non-compliances to the employees and cultural issues are the main reasons for non-compliances.

Q14. What can be done to establish a compliance culture within the bank?

Banks typically need to invest in robust internal controls, ongoing training and education, effective risk management, and a strong compliance culture. Regular audits, reviews, and assessments can help identify and rectify non-compliance issues. Additionally, staying informed about changing regulations and adapting systems and processes accordingly is crucial for banks to remain compliant with both internal and external guidelines.

Q15. How fund transfer fraud is done?

Usually fund transfers are occurred by both bank employees and external fraudsters. Fund transfer fraud committed by bankers can occur due to a range of unethical or illegal actions taken by bank employees. These actions can result from the exploitation of their positions and access to financial systems.

Q16. What types of fund transfers are common in the bank?

After analyzing the natures of fund transfer frauds, fund transfers can be categorized in two (02) types;

i. Unauthorized Fund transfer from customers' account

ii. Unauthorized Fund Transfers from Bank's GL Balance

Q17. What can be done to mitigate fund transfer fraud?

People and organizations should use prudence, confirm the other party's identification, refrain from disclosing personal or financial information without permission, and carry out due diligence before completing any financial transactions, especially wire transfers, in order to safeguard banks from money transfer frauds. To identify and stay away from these scams, awareness and education are essential. Additionally, you can help stop others from becoming victims of scams similar to yours by reporting any suspected fraud to the appropriate authorities.