Operational Risk Management in Islamic Banks: Best Practices and Evaluation

Banking Research Series 2025

Keynote Paper of Research Workshop of BIBM

Issue No. 02

Dr. Md. Mahabbat Hossain CIPA, CSAA, DIB
Md. Alamgir CIPA, CSAA
Md. Rabiul Karim CIPA, CSAA
Md. Atiqur Rahman Khan Khadem CERM, CSAA
Md. Emon Arefin

Published by

Bangladesh Institute of Bank Management

BIBM
Bangladesh Institute of Bank Management
Since 1974

Banking Research Series-2025

Keynote Paper on Research Workshop of BIBM
Issue No. 02

Operational Risk Management in Islamic Banks: Best Practices and Evaluation

Research Team

Dr. Md. Mahabbat Hossain CIPA, CSAA, DIB
Associate Professor, BIBM

Md. Alamgir CIPA, CSAA
Professor and Director (Certification), BIBM

Md. Rabiul Karim CIPA, CSAA
Additional Director, IBRPD, Bangladesh Bank

Md. Atiqur Rahman Khan Khadem CERM, CSAA
Senior Vice President and Head of Financial Institutions, IBBPLC

Md. Emon Arefin
Lecturer, BIBM



Bangladesh Institute of Bank Management (BIBM)
Mirpur, Dhaka-1216, Bangladesh

Operational Risk Management in Islamic Banks: Best Practices and Evaluation

Editorial Advisor : **Dr. Md. Ezazul Islam**
Director General, BIBM

Editor : **Dr. Mohammad Tazul Islam**
Professor and Director (Training), BIBM

Research Team : **Dr. Md. Mahabbat Hossain CIPA, CSAA, DIB**
Associate Professor, BIBM
: **Md. Alamgir CIPA, CSAA**
Professor and Director (Certification), BIBM
: **Md. Rabiul Karim CIPA, CSAA**
Additional Director, IBRPD, Bangladesh Bank
: **Md. Atiqur Rahman Khan Khadem CERM, CSAA**
SVP and Head of Financial Institutions, IBBPLC
: **Md. Emon Arefin**
Lecturer, BIBM

Support Team : **Md. Al-Mamun Khan**
Senior Officer (PPR), BIBM
: **Md. Habibur Rahman**
Assistant Senior Officer (General), BIBM
: **Md. Morshadur Rahman**
Officer (PPR), BIBM
: **Mst. Shamsun Naher Sumi**
Junior Officer (General), BIBM

Graphics & Illustration : **Azizur Rahman,** *Junior Officer (IT/ICT), BIBM*

Published : January 2026

Copyright©BIBM 2026

The views in this publication are of authors only and do not necessarily reflect the views of the institutions involved in this publication.

Forewords

It gives me great pleasure to present this research report titled *Operational Risk Management in Islamic Banks: Best Practices and Evaluation*. This study arrives at an important moment for the Islamic banking industry in Bangladesh, when Islamic banking industry is passing a critical situation with very high non-performing investment and merger of some banks. As a training, academic and research institute for the banking sector, BIBM has consistently emphasized the need for strong governance systems, disciplined risk cultures, and continuous capacity building to support a resilient and ethical financial system. This publication reflects that institutional commitment.

Operational risk has become one of the most challenging and consequential forms of risk for Islamic banks. Unlike conventional institutions, Islamic banks must manage not only process failures, human errors and system disruptions, but also the added dimension of Shariah compliance. A single lapse in documentation, contract execution or product structuring can lead to Shariah non-compliance, reputational damage and fiduciary consequences. This study provides a timely, evidence-based assessment of these realities and offers a structured analysis of how Islamic banks in Bangladesh are currently managing operational risk—where they are progressing, where gaps remain, and what reforms are necessary.

The research team has combined survey insights, case studies, Focus Group Discussions (FGDs), Key Informant Interviews (KIIs), and documentary reviews to deliver a comprehensive evaluation of the prevailing practices in the industry. Their findings highlight critical issues such as weaknesses in documentation standards, the need for better system integration of Shariah parameters, capacity constraints in internal Shariah audit, and the absence of an external Shariah review mechanism and fiduciary rating framework.

I firmly believe that this research will serve as a valuable reference for Islamic banks, regulatory bodies, policymakers, academics, and practitioners. It provides not only a diagnostic view of the current landscape but also strategic recommendations that can guide the development of stronger, more transparent, and more Shariah-aligned operational risk frameworks. As Bangladesh's Islamic banking industry continues to expand, embracing these recommendations will be crucial for safeguarding stakeholder trust and ensuring sustainable growth.

I commend the research team for their dedication, rigor and commitment to excellence. On behalf of BIBM, I extend my gratitude to all industry representatives, regulators, and participants who contributed their time, insights, and experience to enrich this study. I sincerely hope that the findings of this research will inspire continued dialogue and meaningful improvements across the Islamic banking sector of Bangladesh.

Dr. Md. Ezazul Islam
Director General
Bangladesh Institute of Bank Management (BIBM)

Acknowledgment

The research team gratefully acknowledges the support, guidance, and cooperation of all individuals and institutions that contributed to the successful completion of this study titled "Operational Risk Management in Islamic Banks: Best Practices and Evaluation." This work would not have been possible without the collective efforts of many stakeholders within the banking and financial sector of Bangladesh.

We express our sincere gratitude to Bangladesh Institute of Bank Management (BIBM) for providing the institutional support, research environment, and resources necessary to undertake this study. We are especially indebted to the Director General of BIBM, whose continuous encouragement and commitment to rigorous research have motivated us throughout the study.

The research team extends heartfelt thanks to the Bangladesh Bank, particularly officials from the Islamic Banking Regulations and Policy Department (IBRPD) for their valuable insights and cooperation during KIIs and FGD. Their perspectives greatly enriched the depth and relevance of the study.

We also convey our appreciation to the member of the Board, senior executives, Shariah Supervisory Committee members, Internal Shariah Audit units, and Risk Management Departments of various Islamic banks and Islamic branches/windows for participating in the survey, KIIs, and FGDs. Their openness in sharing operational experiences, challenges, and practical viewpoints significantly enhanced the empirical strength of this research.

Special recognition is due to the Distinguished Discussants and participants who contributed thoughtful comments during the research workshop. Their critical observations and constructive feedback helped refine the findings and recommendations presented in this report.

We gratefully acknowledge the administrative and logistic support provided by the BIBM Research, Training, and Publication Divisions. We extend our thanks to our colleagues and staff members who assisted in data collection, coordination with banks, workshop arrangements, and document preparation at various stages of the study. A special appreciation to Mr. Abdullah His Saad, Assistant Director, Bangladesh Bank and MBM Graduate of BIBM for assisting in collecting data for the study.

Finally, the research team expresses deep appreciation to all respondents, participants, and stakeholders whose cooperation made this work possible. Their contributions reflect a shared commitment to strengthening operational risk management practices and reinforcing the integrity of Islamic banking in Bangladesh.

Dr. Md. Mahabbat Hossain CIPA, CSAA, DIB

Md. Alamgir CIPA, CSAA

Md. Rabiul Karim CIPA, CSAA

Md. Atiqur Rahman Khan Khadem CERM, CSAA

Md. Emon Arefin

Table of Contents

Chapter 1: Introduction	01
1.1 Background of the Study	01
1.2 Objectives of the Study	04
1.3 Methodology of the Study	04
1.4 Structure of the Report	05
Chapter 2: Conceptual and Theoretical Framework	06
2.1 Concept of Risk (Mukhatarah) and Risk Management	06
2.2 Shariah Viewpoints on Risk (Mukhāṭarah) and Risk Management	07
2.3 Theoretical Foundations of Operational Risk in Islamic Finance	09
2.4 Key Operational Risk Categories in Islamic Banks	10
2.5 Relationship between Operational Risk and Shariah Risk	11
2.6 Interdependencies of Operational Risk with Major Risks in Banking	11
2.7 Basic Features of Operational Risk in Banks	12
2.8 Calculation of Capital Requirement for Operational Risk under Basel	13
Chapter 3: Regulatory and Institutional Framework	15
3.1 Guiding Framework for ORM in Banks: International	15
3.2 Guiding Framework for ORM in Banks: Domestic	21
Chapter 4: ORM Practices in Banks of Bangladesh	27
4.1 ORM Practices in Banks in Bangladesh: Questionnaire Survey	27
4.2 Operational Risk in Banks of Bangladesh: Case Studies	29
Chapter 5: Findings and Data Analysis	33
5.1 Islamic Banking in Bangladesh	33
5.2 Summary of FGD and KII Outcomes	37
Chapter 6: Issues and Recommendations	51
6.1 Understanding Level of and Attention to ORM	51
6.2 Shariah Non-Compliance Risk as Integral Part of Risk Management Process	51
6.3 Proper Selection in Entry Level Officials and Development Subsequently	52
6.4 Introduction of External Shariah Review and Fiduciary Rating	52
6.5 Regulatory Initiatives and Updating Regulations	53
6.6 Shariah-Based KPI of Banks and Employees	53
6.7 Massive Shariah Awareness Programs	54
6.8 Independency of ISA and Pro-activeness of SSC	54
References	55
Appendix I: Industry Survey on Operational Risk Management in Banks	58
Appendix II: Case Study Collected from BIBM Study	60
List of Abbreviations	65

List of Tables

Table 5.1: Aggregated Balance Sheet of IBs (Amount in Billion BDT)	33
Table 5.2: Aggregated Income Statement of IBs (Amount in Billion BDT)	34
Table 5.3: Comparative Performance of Banking Industry and IBs (%)	35
Table 5.4: Comparative Capital Requirements of IBs and CBs in 2023	36

List of Box

Box 5.1: Relationship of Others Risks with Operational Risk of Islamic Banks	39
Box 5.2: Summary of Control Points for Operational Risk Management of Islamic Banks	44

List of Figures

Figure 5.1: Salient Operational Risk of Islamic Banks	38
Figure 5.2: Operational Risk Governance Framework of Islamic Banks	42
Figure 5.3: Optimal Risk Management Organogram	47

Executive Summary

Operational risk has emerged as a critical dimension of risk governance in Islamic banks, reflecting the combined challenges of process failures, human error, system deficiencies and external disruptions alongside the unique requirement of maintaining strict Shariah compliance. This study examines the operational risk management (ORM) frameworks of Islamic banks in Bangladesh, evaluates their effectiveness against international standards, and identifies the practical challenges and gaps that impede sound risk practices. Drawing on the Basel Committee's operational risk framework and the Islamic Financial Services Board (IFSB) standards—particularly IFSB-1 on risk management, IFSB-23 on capital adequacy and IFSB 30 on governance—the study provides an integrated assessment of the current readiness of Islamic banks to manage operational and Shariah-related risks.

The research employs a mixed-method approach combining questionnaire surveys, Key Informant Interviews (KIIs), Focus Group Discussions (FGDs), documentary analysis and case studies. Findings reveal that Islamic banks have made notable progress in establishing ORM structures, forming risk management units, and introducing policies mandated by Bangladesh Bank's Risk Management Guidelines (2018). However, significant weaknesses remain. These include inconsistencies in contract documentation, inadequate product structuring processes, manual interventions arising from system limitations, limited integration between Shariah supervisory bodies and risk management units, and insufficient capacity in internal Shariah audit functions. The study identifies Shariah non-compliance risk (SNCR) as the most prominent operational risk category for Islamic banks, as breaches not only cause financial loss but also trigger reputational damage and fiduciary concerns, making SNCR fundamentally different from typical operational risks in conventional banks.

Evidence shows that operational risk practices across Islamic banks are uneven and heavily dependent on institutional size, system automation and staff competencies. While some institutions have adopted Key Risk Indicators (KRIs), loss event databases, system-based controls and Shariah-compliant audit trails, others continue to rely on manual processes, limited audit coverage and fragmented governance practices. Industry participants emphasized the necessity of strengthening documentation standards, enhancing system integration for Shariah parameters, refining the role of Internal Shariah Audit (ISA), and increasing the capacity of Shariah Supervisory Committees (SSC) in technical and operational oversight. The absence of an external, independent Shariah review mechanism and fiduciary rating in Bangladesh was widely identified as a structural gap, unlike jurisdictions such as Malaysia and Bahrain where external Shariah assurance has become integral to ORM. The study concludes that Islamic banks require a more holistic and technology-enabled ORM culture that embeds Shariah considerations at every operational touchpoint—from product design and approval to execution, monitoring and reporting. Key recommendations include: establishing an external Shariah review and

fiduciary rating framework; strengthening ISA independence and audit coverage; ensuring system-based controls for contract execution; improving staff competency through specialized training on operational and Shariah risk; and updating regulatory guidelines to reflect emerging technology-driven risks, including cyber threats and digital delivery channels for Islamic banking. Strengthening ORM is essential not only for financial resilience but also for upholding the trust that stakeholders place in Islamic banks as Shariah-compliant institutions.

This research aims to support policymakers, regulators, and Islamic banks in enhancing operational resilience and harmonizing Shariah governance with modern risk management practices. By bridging global standards with the unique requirements of Islamic finance, the study contributes to building a stronger, more transparent and trustworthy Islamic banking sector in Bangladesh.

Operational Risk Management in Islamic Banks: Best Practices and Evaluation

Chapter 1: Introduction

1.1 Background of the Study

Operational Risk Management (ORM) has risen as a crucial pillar of risk governance in financial institutions. According to the Basel Committee on Banking Supervision (BCBS), operational risk refers to the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events (Jayahama, 2005; Habib et al., 2025). This risk category is broad and includes legal risk, though it excludes strategic and reputational risk (FDIC, 2023; IFSB 2021). In an era of rapid technological advancement, regulatory pressure, and heightened complexity, banks must build resilient operational risk frameworks (KPMG, 2022).

While conventional banks deal with operational risk in terms of process failures, cyber events, fraud, system outages, or human error, Islamic banks confront additional layers of complexity. They must integrate Shariah compliance into all operational processes, since violations may lead not only to financial losses, but also reputational damage and regulatory sanctions for failing to observe Islamic law. The unique features of Islamic financial contracts—such as Murabahah, Mudarabah, Musharakah, and Ijārah—introduce documentation risk, contract interpretational risk, and Shariah non-compliance risk (Reyazat, 2012). Islamic institutions therefore must ensure that their operational controls align not only with sound risk principles but also with Shariah governance frameworks.

Globally, the Islamic Financial Services Board (IFSB) has established guiding standards aimed at aligning risk practices with Islamic finance principles. Its Guiding Principles of Risk Management (IFSB-1, 2005) explicitly address operational, Shariah, and compliance risks, emphasizing that each institution must adopt a risk management architecture consistent with its business model and Shariah obligations (IFSB, 2005). The IFSB's work complements the broader international regulatory regime, including the Basel framework, thus allowing Islamic banks to adapt global rules while honoring their faith-based imperatives (IFSB-23, 2021).

In Bangladesh, Islamic banking forms a significant and growing part of the financial sector. Although all banks (conventional and Islamic) are bound by central bank guidelines on risk and capital requirements, Islamic banks operate under dual

requirements — they must comply with Bangladesh Bank's risk and capital regulations and Islamic jurisprudential norms. Prior studies highlight challenges in measurement, lack of standardized disclosure, and weak integration between Shariah governance bodies and risk units (Shakhatreh, Biancone & Radwan, 2016).

Hence, this research aims to explore Operational Risk Management in Islamic Banks with special emphasis on (a) identifying best practices, (b) evaluating existing frameworks in Bangladesh, and (c) proposing context-sensitive recommendations. This study aspires to fill gaps in the literature and support Islamic financial institutions in strengthening their operational resilience within Shariah boundaries.

Basel Committee on Banking Supervision (BCBS) has formulated the ORM given the humongous operational ambiguities (Ahmed, 2010). The ORM got the spotlight and is being considered diligently while keeping additional percentage of capital aside to manage the operational risk along with credit risk and market risk.

Due to the adherence to the shariah principle, unique contract and governance structure, Islamic banks are exposed to greater operational risk. The operational risk management standards offered by IFSB is considered as guiding principle for ORM. Particularly, capital and risk guidance framework offered by IFSB mentions Shariah non-compliance as operational risk (Archer & Karim, 2007). In Malaysia, Pakistan and Indonesian bank regulators have adopted standards from Basel/IFSB to manage operational risk in Islamic banks. Unique source of operational risk comprises documentation challenges arise from mistake in contract design, complex mechanism than conventional banks, additional steps for approval can be the source of operational risk (Hasan, 2019). To measure and manage the ORM both quantitative and qualitative method is followed. Qualitative methods include the assessment of risk, key risk indicators (KRIs) and training and development of the employees whereas the quantitative methods focus on the mathematical steps as suggested by IFSB and Basel committee. Internal control and compliance needed to be strengthened to inspect regulatory and shariah violation to combat Operational risks. Historically, large banks are seen to disclose the operational risk exposure in the annual reports as compared to the small Islamic banks. Added to that, a new form of operational risk has been triggered due to cyber-attack and system failure and natural calamities (Ali, 2021).

Despite significant threat posed by operational risk to Islamic banks, there remains a lack of literature thoroughly addressed issue regarding operational risk as compared to credit and market risk (Noman et all., 2020). The reason behind this gap may be

trace back to the gap of understanding and complexities of the origin of operational risk in Islamic banks. This is why the aspects of the operational risk management worth exploration from the context of Islamic banks of Bangladesh.

Empirical research in conventional banks shows that robust ORM systems enhance institutional stability and market confidence. Pakhchanyan (2016) and Ferreira, Nunes and Pereira (2019) argue that operational risk, once considered residual, now occupies a central position in enterprise-wide risk frameworks, integrating loss event databases, risk control self-assessments, and key risk indicators. Studies in Europe, the Middle East, and Asia—such as those by Cornwell et al. (2023) and Jadwani (2024)—confirm the shift toward data-driven, technology-enabled risk assessment under the revised Basel III standards.

Hassan (2016) highlight that non-compliance with Shariah rules—arising from errors in contract documentation or execution—can lead to both financial losses and reputational damage, thereby linking Shariah non-compliance risk intrinsically with operational risk. Conversely, some scholars such as Archer and Karim (2009) and Al-Musheifri (2021) suggest that Shariah non-compliance should be recognized as a distinct risk component, since its implications extend beyond operational failures to ethical and legal dimensions that affect investor confidence and systemic reputation. Therefore, the classification of Shariah non-compliance risk remains a conceptual divergence—treated as part of operational risk in the IFSB framework, yet addressed separately in some national regulation (Ahmed, 2009).

International studies further illustrate these dynamics. In Malaysia, a comparative study by Hassan (2011) found that Islamic banks integrate Shariah governance with operational risk functions through dual reporting lines between the risk management unit and the Shariah board. Similar approaches in the Gulf Cooperation Council (GCC) countries reveal that board-level oversight and Shariah audits serve as mitigating tools against both operational and compliance risks (Neifar & Jarboui, 2018). Research in Pakistan and Indonesia demonstrates that the lack of standardization in contract documentation and IT infrastructure contributes to process-related operational losses (Masood & Javaria, 2018). These findings collectively suggest that effective ORM in Islamic banks requires integrating conventional internal-control mechanisms with Shariah governance structures.

In the Bangladesh context, operational risk management in Islamic banks is still evolving. Although Bangladesh Bank's Guidelines on Risk Management for Banks (2018) prescribe comprehensive internal-control mechanisms, there is no standalone

directive on operational risk for Islamic banks. Empirical work by Habib et al. (2025) indicates that most Islamic banks follow conventional ORM templates, with limited incorporation of Shariah perspectives. Meanwhile, studies by Makiyan (2009) reveal that documentation errors, product mis-structuring, and manual contract execution are the most frequent operational lapses observed in Bangladeshi Islamic banks.

1.2 Objectives of the Study

Operational risk management (ORM) plays a vital role in maintaining the soundness, efficiency, and Shariah compliance of Islamic banking operations. As Islamic banks continue to expand within Bangladesh's dual banking system, they face increasing challenges stemming from both conventional operational risks and unique Shariah-related considerations. Understanding how these institutions identify, assess, and mitigate operational risks is essential to ensuring their long-term stability and adherence to Shariah principles. Against this backdrop, the study aims to evaluate the governance structures, frameworks, and practices of ORM in Islamic banks and to identify the key issues that influence their effectiveness. The specific objectives of the study are as follows:

1. to evaluate the operational risk management frameworks adopted by Islamic banks in Bangladesh;
2. to identify and analyze the key challenges Islamic banks encounter in managing operational risks in comparison with conventional banks;
3. to examine the roles and responsibilities of various stakeholders in mitigating operational risks within Islamic banks; and
4. to develop practical recommendations for strengthening ORM in Islamic banks to ensure both Shariah compliance and institutional sustainability.

1.3 Methodology of the Study

The present study is an extension of the earlier research conducted by the Bangladesh Institute of Bank Management (BIBM) titled "Governance and Practices of Operational Risk Management in Banks". Accordingly, several common findings and insights from that study (Habib et al., 2025) have been utilized as foundational references to ensure continuity and comparability between conventional and Islamic banking contexts.

To achieve the objectives of the current study, a mixed-method approach was employed, combining both qualitative and quantitative elements. Content analysis was conducted on relevant national regulatory frameworks issued by Bangladesh Bank, along with international standards and guidelines provided by institutions such

as the Islamic Financial Services Board (IFSB) and the Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI).

Primary data were collected through Focus Group Discussions (FGDs) and Key Informant Interviews (KIIs). The participants included officials from the Islamic Banking Regulations and Policy Department (IBRPD) of Bangladesh Bank, representatives from the Internal Control and Compliance Divisions (ICCD) of commercial banks, Internal Shariah Auditors, members of the Senior Management Team (SMT) of Islamic banks, and members of Shariah Supervisory Committees. These engagements provided critical insights into the practical dimensions of operational risk management in Islamic banks.

Secondary data were gathered mainly from the published annual reports and official websites of Islamic banks in Bangladesh and central bank. In addition, websites and reports of central banks and commercial banks from other countries were reviewed to identify and compare international best practices in operational risk management.

1.4 Structure of the Report

The main objective of the study is to address the ORM practices of Islamic banks operating in Bangladesh. Accordingly, the report is organized into six chapters. *Chapter 1* introduces the study by presenting the background, literature review, objectives and methodology. *Chapter 2* outlines the conceptual and theoretical framework, explaining the Islamic concept of risk (Mukhatarah), theoretical foundations of operational risk in Islamic finance, key categories of operational risk, and the relationship between operational and Shariah risks. *Chapter 3* describes the regulatory and institutional framework, covering domestic regulations given by Bangladesh Bank, international standards such as IFSB, AAOIFI, and institutional governance structures. *Chapter 4* discusses the operational risk management practices of Islamic banks in Bangladesh. *Chapter 5* presents empirical findings based on surveys, FGDs, and KIIs, followed by both quantitative and qualitative analyses to identify key trends and emerging issues. Finally, *Chapter 6* highlights the major issues, provides policy recommendations and explains Shariah governance implications.

Chapter 2: Conceptual and Theoretical Framework

2.1 Concept of Risk (Mukhatarah) and Risk Management

In Islamic finance, the idea of risk originates from the main sources of Shariah — the Qur'an and the Sunnah. The Arabic word Mukhatarah (**مخاطرة**) means exposure to danger or uncertainty. But in Islam, the meaning of risk is more balanced than in the conventional system. Conventional finance often tries to remove or reduce risk only to make more profit. On the other hand, Islamic finance accepts that risk is a natural and necessary part of trade and wealth creation and mobilization.

Islam teaches that profit and risk must go together. This is based on the saying of the Prophet (peace be upon him): "Profit comes with liability" (Al-Kharaj bi al-Daman, Ibn Majah). It means that if a person wants to earn profit, he must also be ready to bear loss. This rule ensures justice and fairness because no one should gain money without taking some responsibility for possible loss.

However, Islam does not allow all kinds of risk. It makes a clear difference between Gharar (excessive uncertainty) and normal business risk (Mukhatarah).

- Gharar happens when there is too much uncertainty in the basic terms of a contract, like the subject matter, price, or delivery. Such contracts are not allowed because they may lead to cheating or dispute.
- Mukhatarah, on the other hand, is the normal type of business risk — for example, the risk that a project may fail or that an asset may lose value. This type of risk is allowed as long as both parties understand and accept it clearly (Ayub, 2007).

The Maqasid al-Shariah (objectives of Islamic law) guide all Islamic economic activities, including risk management. The main goals are to protect faith (Din), life (Nafs), intellect (Aql), family (Nasl), and wealth (Mal). Among these, the protection of wealth is most related to risk management, as it teaches people to safeguard money and property from injustice, loss, or misuse (Chapra, 2008).

From these principles, Islamic finance applies the following ways to manage risk:

Risk Management Strategies	Objectives
Avoid Prohibited Risk (Gharar and Maysir)	Islam prohibits transactions involving excessive uncertainty and gambling. These are unfair and lead to unearned profit.
Transfer of Risk through Permitted Contracts	Certain Islamic contracts allow sharing or transfer of risk. For example, in a Salam contract, the seller faces production risk, and the buyer faces delivery risk. In Ijarah (leasing), the owner carries the ownership risk, and the user carries the usage risk.
Reduce Risk with collateral (Rahn)	Using collateral or a pledge helps reduce credit risk and ensures repayment.
Share Risk through Partnership Contracts	In Mudarabah and Musharakah, both parties share profits and losses. The investor provides the money, and the entrepreneur provides effort and management.

Source: *Iqbal & Mirakhor (2011)*

Thus, Islamic risk management is not only a technical task. It is a moral and religious duty that ensures fairness, trust, and stability in financial activities.

2.2 Shariah Viewpoints on Risk (Mukhāṭarah) and Risk Management

Contemporary scholars affirm that risk management is permissible and necessary within Shariah, as it aligns with the objective of safeguarding wealth (Hifẓ al-mal) and maintaining contractual fairness. This position is supported by several foundational texts. Quran 2:282 requires the documentation of debts, appointment of a just scribe and the use of witnesses—elements that are central to risk mitigation, transparency and operational discipline. The famous hadith reported in Jami al-Tirmidhi (no. 2517), where the Prophet (ﷺ) advised a man to "tie your camel and then rely on Allah," clearly establishes that Tawakkul must be accompanied by precaution and sound control measures. Islam also recognizes the inherent link between risk and return, expressed through the legal maxims Al-ghunm bil-ghurm (profit is justified only by bearing liability for loss) and Al-kharaj bi al-ḍaman (usufruct belongs to the one who bears responsibility). Profit in Islamic finance is therefore legitimate only where real business risk is borne, underscoring the centrality of operational, asset-based and transactional risk in Shariah-compliant contracts.

The Quran further acknowledges uncertainty as an intrinsic feature of human life. Verses such as Quran 31:34 emphasize that only Allah possesses perfect knowledge of future events, thereby underscoring the need for prudent anticipation, planning and responsible conduct within economic activities. Likewise, Quran 12:67 records the counsel of Prophet Yaqub (AS) advising his sons to diversify their entry into Egypt while recognizing that ultimate outcomes are in Allah's hands—an early example of prudent diversification combined with Tawakkul. Shariah also prohibits unjust consumption of wealth, as in Quran 4:29, which forms the basis for rejecting risk structures involving exploitation, deception or excessive speculation. Moreover, the narrative in Quran 12:46–49, where Prophet Yusuf (AS) interprets the king's dream and advises a strategy of storing grain during abundant years to mitigate future famine, demonstrates forward-looking risk identification and contingency planning comparable to modern risk management practices.

Several prophetic traditions reinforce this orientation toward disciplined risk-taking. The instruction to invest the wealth of orphans to prevent erosion by Zakah highlights the obligation to avoid certain loss through prudent financial action. Likewise, the contractual conditions imposed by Abbas ibn Abd al-Muṭṭalib (RA) in Muḍarabah—such as prohibiting his agent from crossing the sea or engaging in inherently risky trade routes, conditions later approved by the Prophet (PBUH)—illustrate early Islamic principles of risk allocation, contractual covenants and specification of operational limits. Classical jurists such as Ibn Taymiyyah and Ibn al-Qayyim distinguish between productive commercial risk, which is inherent and necessary in trade, and prohibited forms of risk associated with gambling (Maysir) and excessive uncertainty (Gharar faḥish). This distinction underpins modern Islamic finance, wherein value-adding risk is permissible and even required, while speculative, zero-sum or unjust risk structures are rejected.

From the perspective of Maqaṣid al- Shariah, risk management is closely tied to the objectives of protecting faith, life, intellect, lineage and wealth. Effective operational and financial controls prevent unjust loss, promote economic stability and protect stakeholders from harm, thereby fulfilling Shariah's higher intents. Consequently, risk in Islamic finance can be categorized into three groups: (i) permissible risk, which is inherent in legitimate commercial activity and essential for Shariah-compliant contracts; (ii) prohibited risk, associated with unjust, speculative or exploitative practices that violate Quranic injunctions; and (iii) tolerable but avoidable risk, which is incidental and should be minimized through Shariah-compliant mitigation tools such as proper documentation, Shariah-based controls, takaful arrangements and robust internal governance. Overall, Shariah endorses proactive management of uncertainty, emphasizing prudence, justice and accountability in all financial dealings.

In the context of Islamic banking, these principles form the conceptual foundation for integrating Shariah governance with operational risk management, ensuring that risk mitigation is both professionally rigorous and religiously compliant.

2.3 Theoretical Foundations of Operational Risk in Islamic Finance

The Basel Committee on Banking Supervision (BCBS, 2011) defines operational risk as the possibility of loss resulting from inadequate or failed internal processes, people, systems, or external events. Similarly, the Islamic Financial Services Board (IFSB, 2021) describes it as the risk of loss arising from deficiencies in internal processes, human resources, technology, or external factors, including legal, cyber, and Shari'ah non-compliance risks. According to the IFSB, operational risk excludes strategic and reputational elements.

Islamic banks encounter unique operational risks beyond those of conventional institutions, the most significant being Shariah non-compliance risk—losses arising from failure to adhere to Shariah rules and principles (IFSB, 2005). Any deviation can cause financial penalties, reputational damage, and income purification requirements. Complex contracts like Murabahah, Mudarabah, and Ijarah involve multi-step processes and detailed documentation, heightening exposure to human or procedural errors. Variations in Shariah interpretation and a shortage of professionals with both banking and Shariah expertise further increase such risks. To mitigate these, Islamic banks integrate robust internal control systems, Shariah audits, and automated compliance mechanisms within their core banking systems. Regular staff training, process audits, and maintenance of risk registers strengthen compliance, promote accountability, and ensure early detection of operational weaknesses.

The theory of operational risk in Islamic banking can be understood from three main perspectives — agency theory, stakeholder theory, and the unique nature of Islamic contracts.

Agency Theory and Information Asymmetry

Agency theory explains the relationship between a principal (the one who gives authority) and an agent (the one who manages on behalf of the principal). In Islamic banks, this relationship is more complex because of the two-tier Mudarabah system. In the first level, depositors are the principals, and the bank acts as their agent (Mudarib). In the second level, the bank becomes the investor and gives funds to entrepreneurs.

This layered structure may create problems such as moral hazard (when one side takes hidden risks) and adverse selection (choosing bad investments). For example, the bank

may favor its shareholders over depositors or may not check a project properly, causing losses (Sundararajan & Errico, 2002).

Stakeholder Theory and Responsibility

Islamic banks are responsible not only to shareholders but also to depositors. This makes their duties broader and more moral in nature. Any failure in their internal system that leads to a Shariah violation can damage both reputation and trust. Therefore, reputation risk is part of operational risk in Islamic banks (Grais & Pellegrini, 2006).

Nature of Islamic Contracts

Each Islamic finance contract brings its own operational challenges. In case of Mudarabah/Musharakah, risk of incorrect profit calculation or weak monitoring is pertinent. For Murabahah, risk of not taking real ownership of assets or documentation mistakes is very common Shariah non-compliance. Whereas, HPSM or Ijarah poses the risk of poor maintenance or calculation errors in lease payments. In regard to Salam/Istisna'a, risk that the supplier may not deliver on time or as agreed upon.

In short, operational risk in Islamic banks is wider and more complex than in conventional banks because it involves many types of contracts and moral responsibilities.

2.4 Key Operational Risk Categories in Islamic Banks

Islamic banks experience operational risks similar to those outlined by Basel and the IFSB (2005), though their nature and implications are often shaped by Shariah requirements. Internal fraud may occur through dishonest acts by employees, such as bypassing contract procedures, embezzling funds, or manipulating profit-sharing calculations. External fraud involves criminal acts by third parties, including cyberattacks, forgery, theft or manipulation of accounting record by the partner. Employment and workplace-related risks arise from breaches of employee rights, discrimination, or unsafe working conditions. Risks linked to clients, products, and business practices are particularly critical in Islamic finance, as they include Shariah non-compliance (e.g., failure to take ownership in a Murabahah transaction), fiduciary breaches (such as mixing clients' and shareholders' funds), mis-selling of complex investment products, and product errors like documentation mistakes in Sukuk structures. System failures, including IT breakdowns or disruptions in online platforms, can halt essential banking operations, while process management failures—such as neglecting to insure leased assets or register ownership—may lead to financial and reputational losses. Managing these risks demands both conventional control mechanisms, such as internal audits and IT safeguards, and specialized

Shariah controls embedded within the Shariah Governance Framework to ensure compliance and operational integrity.

2.5 Relationship between Operational Risk and Shariah Risk

The Arabic word **خَطَر (Khatar)** means *danger, risk, or exposure to loss*. While it refers to operational risks in banking specially in Islamic banking it is termed as- مخاطر **التشغيل في المصارف الإسلامية** (*Makhāṭir al-Tashghīl fī al-Maṣārif al-Islāmiyyah*) i.e. o*perational risks in Islamic banks. Actually,* **تشغيل** (*Tashghīl)* means *to cause something to work or operate*, and in finance, **مخاطر التشغيل** refers to risks arising from the functioning or operation of the bank (Wehr, 1994).

Operational risk—commonly defined as the risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events—poses major challenges for banks. Islamic banks operate under broadly the same categories of operational risk as conventional banks, but they also face unique exposures because of Shariah-governance requirements, product contract structures (such as Murabahah, Mudarabah, Ijarah), and the involvement of depositors.

In Islamic banking, operational risk and Shariah risk are deeply interconnected. The IFSB (2005) defines Shariah risk as the possibility that a bank fails to comply with Islamic rules and principles. In practice, most Shariah non-compliance incidents stem from weaknesses in internal processes, human error, or system deficiencies—making it a subset of operational risk. A simple procedural lapse, such as an officer neglecting to take ownership in a Murabahah transaction, can render the deal invalid under Shariah, resulting in both financial loss and reputational harm. The implications extend beyond the transaction level; any violation may lead to contract cancellation and erosion of public trust (Hasan, 2011). Shariah risk also infuses all functions of an Islamic bank—from product structuring to reporting—necessitating a robust Shariah Governance Framework (BNM, 2019) to ensure compliance at every stage. Furthermore, differences in scholarly interpretation (Ikhtilaf) across jurisdictions can pose additional challenges for international Islamic banks. Ultimately, operational and Shariah risks are mutually reinforcing: a failure in operational control can trigger Shariah breaches, while weak Shariah supervision can expose operational vulnerabilities. Hence, effective risk management in Islamic banks must integrate both operational safeguards and strong Shariah oversight mechanisms.

2.6 Interdependencies of Operational Risk with Major Risks in Banking

Essentially, operational risk covers a wide range of non-financial risks that stem from deficiencies in people, systems, or procedures, making it closely intertwined with other core risks in banking. Operational risk and credit risk are mutually reinforcing. Weak internal controls or process failures can lead to poor credit assessments,

mismanagement of financing portfolios, and eventual defaults. Conversely, large-scale investment defaults can trigger operational strain through legal disputes, documentation backlogs, or system overloads (Kelliher et al., 2020). Market risk also interacts with operational risk—failures in internal monitoring or valuation systems can cause market losses, as seen in the Barings Bank collapse. Similarly, extreme market volatility can expose hidden weaknesses in a bank's operational systems (FDIC, 2006).

Operational disruptions can swiftly evolve into liquidity problems. For instance, fraud, cyberattacks, or system outages can erode depositor confidence, limiting access to funding and creating liquidity stress (BCBS, 2008). Reputational risk is another by-product of operational failures. Incidents such as customer data breaches, compliance violations, or ethical lapses not only damage a bank's public image but also amplify credit, market, and liquidity risks (Management Solutions, 2021).

Operational and compliance risks are also closely linked, as many compliance breaches stem from weaknesses in operational processes. Regulatory penalties, anti-money laundering violations, and reporting errors often result from internal control failures, showing that compliance risk is effectively a subset of operational risk (IMF, 2023). Finally, Operational Risk Management (ORM) forms a vital component of Enterprise Risk Management (ERM). ORM supports ERM through tools like Key Risk Indicators (KRIs), scenario analysis, and risk control self-assessments, aligning operational insights with broader strategic goals. In turn, ERM frameworks rely on ORM data—such as loss events and incident trends—to enhance resilience, ensure regulatory compliance, and guide risk-based decision-making across the institution.

2.7 Basic Features of Operational Risk in Banks

In essence, operational risk encompasses the broad array of non-financial risks that arise from failures or disruptions in the business functions of banks. Commercial banks' operational risk arises for a variety of reasons, and their complex features and natures may be placed under four topologies, as demonstrated by Lu Jin (2024).

One, operational risk is complex and often difficult to isolate from other core banking risks such as credit and market risks, as these risk categories frequently overlap in practice. For instance, a breakdown in credit assessment processes may lead to both credit and operational losses, while market volatility can expose weaknesses in valuation systems—demonstrating how these risks are interconnected and difficult to segregate.

Two, operational risk is broad and multidimensional, arising from diverse sources such as human error, internal control failures, information technology disruptions, and

external shocks like natural disasters or cyber incidents. Its scope varies widely across institutions depending on their size, complexity, technological dependency, and regulatory environment. A global bank with multiple subsidiaries faces different operational challenges than a small domestic bank due to differences in governance structures and operational processes.

Three, another defining feature of operational risk is its unpredictability and dynamic nature. It can originate from any business unit and is influenced by management quality, staff discipline, institutional culture, and overall governance standards. As banking operations increasingly depend on digital platforms and outsourced services continue to emerge, making traditional static models inadequate for capturing these vulnerabilities.

Four, operational risks often stem from human factors rather than system errors. Lapses in judgment, ethical misconduct, or negligence can cause significant financial and reputational harm. However, such risks can be mitigated through continuous staff training, a culture of accountability, robust internal controls, and regular system enhancements. Investing in technology-driven monitoring tools, automation, and process redesign further strengthens resilience and reduces the likelihood of human or procedural failures.

2.8 Calculation of Capital Requirement for Operational Risk under Basel

Adequate capital is the key to risk abortion, and Basel III introduced several methods to estimate capital requirements for operational risks to be practiced by the banks.

Basic Indicator Approach

Capital Requirement = 15% × Average Annual Gross Income (over the last 3 years)

Standardized Approach

Capital = sum of capital charges for each business line [Gross income of each business line; Assigned factor (12–18%) per business line]

Advanced Measurement Approach

Internal models based on: (i) Internal loss data; (ii) External data; (iii) Scenario analysis; (iv) Business environment and internal control factors, subject to supervisory approval.

Bangladesh Bank Guidelines

Under the Guidelines on Risk Based Capital Adequacy (Revised Regulatory Capital Framework for Banks in line with Basel III) issued by Bangladesh Bank (2014), the capital charge for operational risk is calculated in accordance with the methodologies recommended by the Basel Committee.

Bangladesh Bank prescribes two permissible methodologies for computing the operational risk capital requirement: (i) the Basic Indicator Approach (BIA) and (ii) the Standardized Approach (TSA). These methods are arranged along a continuum of increasing sophistication and risk sensitivity. Banks are encouraged to progressively migrate toward more advanced approaches as their operational risk management frameworks, internal systems, and data capabilities mature. Once a bank is approved to adopt a more advanced method, it cannot revert to a simpler approach without explicit supervisory approval.

However, if Bangladesh Bank determines that a bank no longer satisfies the eligibility conditions for its existing approach—such as deficiencies in loss data collection, weak governance, or non-compliance with methodological standards—it may require the bank to return temporarily to a simpler approach for some or all of its activities. Reinstatement to the advanced method is permitted only after the bank demonstrates full compliance with the supervisory conditions prescribed by Bangladesh Bank.

Chapter 3: Regulatory and Institutional Framework

Operational risk, unlike credit or market risk, demands a multidimensional and integrated management approach because it cannot be mitigated through a single, uniform solution. As a core pillar of Enterprise Risk Management (ERM), operational risk often acts as an underlying trigger for other risk categories and manifests across every operational segment of a bank. Ineffective management of this risk can undermine institutional credibility and erode public confidence in the banking system. In acknowledgement of its systemic significance, international standard-setting bodies and regulatory agencies have introduced comprehensive global standards and guidelines aimed at strengthening operational risk governance, enhancing resilience, and safeguarding financial stability.

3.1 Guiding Framework for ORM in Banks: International

Basel Principles for ORM in Banks

The Basel Committee on Banking Supervision (BCBS) issued a set of revised Principles for the Sound Management of Operational Risk (PSMOR) in 2021 to address gaps in implementation and to capture emerging sources of operational risk. The updated framework consists of 12 principles covering governance, the operational risk management framework (ORMF), ICT risk, business continuity, and disclosure. These principles apply to all banks but must be tailored to the institution's size, complexity, and risk profile.

The framework underscores the central role of the Board in promoting a strong risk culture, approving key policies, and overseeing the ORMF. Senior management is responsible for implementing these policies, ensuring that staff, processes, and systems reflect the bank's operational risk appetite. The principles emphasize comprehensive identification and assessment of operational risks across all products and activities, supported by tools such as event data, self-assessments, control monitoring, and scenario analysis.

These principles highlight the importance of structured change management, robust risk monitoring and reporting, and maintaining an effective internal control environment with clear segregation of duties. ICT risk receives heightened attention, with banks required to ensure the resilience, security, and integrity of their systems. Business continuity planning is integrated into the ORMF, requiring forward-looking scenario analysis and regular updates. Disclosure expectations focus on transparency without compromising security or creating new vulnerabilities.

Supervisors are expected to assess the adequacy and effectiveness of banks' ORMFs, identify deficiencies, and require timely corrective action. Overall, the 2021 PSMOR places strong emphasis on integrated governance, risk culture, operational resilience, and technology-related risks to strengthen the stability of the global banking system.

Basel Framework for Capital Adequacy of Banks

Basel III reinforces the global treatment of operational risk by shifting the framework toward stronger capital adequacy, enhanced risk coverage, and improved governance—factors directly relevant for Islamic banks. Under Basel III, operational risk is recognized as a core component of total risk-weighted assets besides credit and market risk which requires banks to maintain sufficient high-quality capital to absorb losses arising from failures in people, processes, systems or external events. The framework replaced the earlier Basic Indicator and Standardized Approaches with the more risk-sensitive methodologies, emphasizing the use of robust loss data, scenario analysis, and control environment assessments. Basel III also strengthens the linkage between operational resilience and capital buffers through the capital conservation buffer, countercyclical buffer, leverage ratio, and stringent disclosure requirements. The overarching objective is to ensure that operational losses—whether from fraud, cyber incidents, documentation errors, system breakdowns, or process failures—do not compromise solvency. For Islamic banks, this has important implications because operational lapses often trigger Shariah non-compliance. Consequently, the Basel III regime demands more disciplined governance, stronger internal control systems, documented processes, and integrated risk-data systems—aligning well with Shariah governance requirements and reinforcing the need for Islamic banks to embed operational risk management deeply within both their business processes and their Shariah compliance mechanisms.

IFSB Standards

The Islamic Financial Services Board (IFSB) has developed a comprehensive suite of prudential standards to strengthen the resilience, governance, and stability of the Islamic financial services industry. These standards complement global regulatory frameworks such as Basel III, while addressing the unique contractual and Shariah-specific characteristics of Islamic finance.

IFSB-1, *Guiding Principles of Risk Management* was issued in 2005. This standard establishes foundational risk-management expectations for Islamic banks. It recognizes that Islamic financial institutions face conventional risks – credit, market, liquidity, operational – alongside Shariah-specific risks. Fifteen principles are organized across six risk categories, emphasizing comprehensive risk identification, measurement, monitoring, and reporting. Crucially, IFSB-1 embeds Shariah

compliance as an integral component of operational and fiduciary risk, requiring strong governance structures, proper asset allocation to investment account holders (IAH), effective controls, and transparent reporting.

Under IFSB-1, Islamic financial institutions must recognize operational risk as a broad and multidimensional category encompassing losses arising from weaknesses or failures in internal processes, human resources, information systems, or external events. For Islamic banks, this risk extends beyond conventional dimensions to include potential losses triggered by Shariah non-compliance and breaches of fiduciary duties. Shariah non-compliance risk (SNCR) represents a critical subset of operational risk. It arises when an institution fails to adhere to the Shariah rules and principles established by its Shariah Supervisory Board (SSB) or by the national Shariah authority. Given that Islamic banks exist to provide Shariah-compliant financial solutions, any breach can invalidate contracts, render income illegitimate, necessitate purification, and severely damage the institution's credibility. Because depositors and investors select Islamic banks primarily on the basis of Shariah adherence, even a perceived lapse can trigger withdrawals, reputational erosion, and sustained loss of business opportunities. Consequently, Shariah compliance sits at the highest tier of operational risk priorities.

Fiduciary risk arises when an Islamic bank fails to fulfil the explicit and implicit trust placed upon it by fund providers, including current account holders and Investment Account Holders (IAH). Failure to exercise due care in managing investment funds, misallocation of earnings, or operational weaknesses that impair investment performance can lead to forgone profits, losses to IAH, and, in extreme cases, institutional insolvency. An inability to meet withdrawal demands or protect investor interests undermines confidence and directly threatens the sustainability of the institution.

IFSB-12, *Liquidity Risk Management* was issued by the Board in 2012. The IFSB-12 provides 23 guiding principles covering institutional, interbank, and supervisory aspects of liquidity management. It recognizes structural constraints faced by Islamic banks—limited Shariah-compliant instruments, underdeveloped money markets, and inadequate central bank facilities.

The Board released IFSB-23, *Revised Capital Adequacy Standard* in 2021, establishing the most comprehensive and Basel III–aligned capital framework for Islamic banks to date. The standard replaces and significantly expands IFSB-15 by introducing granular, instrument-specific capital requirements for all major Shariah-compliant contracts, including Murabaḥah, Ijarah, Musharakah, Muḍarabah, Salam, Istisna'a, and Wakalah. It formalizes Shariah-compliant definitions and eligibility

criteria for CET1, AT1, and Tier-2 capital instruments, and provides a structured methodology for the treatment of Profit-Sharing Investment Accounts (PSIAs), incorporating the alpha factor and displaced commercial risk. IFSB-23 strengthens the calculation of RWAs across credit, market, and operational risks and embeds macroprudential components such as the capital conservation buffer, countercyclical buffer, and leverage ratio. It recognizes the SNCR is one of the important components of operational risk of Islamic financial institutions. The standard achieves regulatory parity with conventional Basel III requirements while fully accommodating the contractual and risk-specific features of Islamic finance.

The IFSB issued the *Revised Corporate Governance Principles* (IFSB-30) in 2023, introducing a significantly upgraded governance framework for Islamic banks that reflects contemporary global regulatory reforms. The standard reinforces the Board's central role in shaping institutional culture, ethical values, and risk appetite, while ensuring that Shariah governance is fully integrated into the broader corporate governance architecture. It strengthens oversight of senior management, risk management and compliance functions, internal audit, and Islamic window operations. IFSB-30 provides clearer protections for Investment Account Holders (IAHs), enhances expectations on transparency and disclosure, and broadens accountability requirements across the institution. It also incorporates emerging regulatory priorities including climate-related financial risks, ESG considerations, and long-term sustainability. While aligned with AAOIFI governance standards, BCBS governance principles, OECD governance benchmarks, IFSB-30 directly addresses governance gaps unique to Islamic finance, thereby elevating the resilience, integrity, and credibility of Islamic banking institutions. Besides, IFSB 30 recognizes the concept of "three lines of defense".

IFSB-31, *Effective Supervision of Shariah Governance*, issued in 2025, establishes a dedicated supervisory framework to ensure consistent, credible, and enforceable Shariah governance across jurisdictions. The standard articulates clear expectations for regulators in overseeing the full Shariah governance ecosystem, including supervisory authority, enforcement powers, and systemic oversight responsibilities. It defines the roles and obligations of boards and senior management in upholding Shariah compliance, and sets rigorous benchmarks for the structure, independence, and competency of Shariah Supervisory Boards (SSBs). The standard advances a risk-based supervisory approach to Shariah non-compliance, outlining requirements for escalation, corrective actions, reporting, and alignment with market-conduct supervision. It also provides direction on supervising Islamic windows, complex group structures, and outsourced Shariah functions to prevent gaps or arbitrage in compliance. By harmonizing supervisory expectations and strengthening regulatory

oversight, IFSB-31 enhances systemic confidence in the integrity of Shariah governance.

Taken together, the suite of IFSB standards forms a coherent prudential architecture for Islamic financial institutions—integrating Shariah governance, risk management, liquidity and capital adequacy, corporate governance, and supervisory practices. This unified framework ensures institutional resilience, global comparability, and strict adherence to Shariah principles, reinforcing the stability and credibility of the Islamic banking system.

AAOIFI standards

AAOIFI has revised it governance standard *GS 1: Shari'ah Governance Framework* in 2024. GS-1 establishes a comprehensive and institutionalized Shariah governance framework designed to ensure that Islamic financial institutions operate in strict adherence to Shariah principles. The standard lays out clear responsibilities for the board of directors, senior management, Shari'ah Supervisory Boards (SSBs), and internal control units, emphasizing accountability, independence, transparency, and competence. It strengthens the governance architecture by mandating structured processes for Shariah pronouncements, their implementation, and continuous monitoring to prevent Shariah non-compliance risk (SNCR). The standard embeds stronger expectations for risk integration, disclosure, and internal oversight, aligning governance practices with emerging global regulatory norms and the growing complexity of Islamic financial operations.

AAOIFI GS 9, *Shari'ah Compliance Function,* outlines the institutional requirements for an effective Shariah compliance function within Islamic financial institutions. It specifies the policies, processes, and internal structures required to ensure day-to-day adherence to Shariah rulings issued by the SSB. The standard mandates dedicated Shariah compliance units, internal review processes, real-time monitoring, and comprehensive documentation systems to prevent, detect, and rectify Shariah non-compliance. GS 9 strengthens the defensive line of Shariah governance by embedding compliance controls into operational activities, thereby reducing operational and reputational risks.

AAOIFI GS 10: *Shari'ah Compliance and Fiduciary Ratings for Islamic Financial Institutions* integrates the assessment of both Shariah compliance and fiduciary responsibility, providing a holistic framework for rating Islamic financial institutions. It evaluates the institution's capacity to manage SNCR, uphold fiduciary duties toward fund providers, and maintain sound governance and control environments. The standard blends qualitative and quantitative indicators—such as board oversight, internal control robustness, disclosure quality, and operational reliability—to produce

an independent rating that enhances transparency and strengthens stakeholder confidence. It is particularly relevant for jurisdictions seeking to institutionalize external Shariah review and performance benchmarking.

AAOIFI GS 11: *Internal Shari'ah Audit* formalizes the requirements for a dedicated Internal Shariah Audit (ISA) function, ensuring independent, objective, and systematic evaluation of an institution's Shariah compliance processes. The standard defines the scope of Shariah audit, competency criteria for auditors, audit planning methodologies, reporting expectations, and requirements for follow-up and remediation. It positions ISA as an essential component of the Shariah governance system, functioning analogously to conventional internal audit but focused on verifying adherence to Shariah rulings across products, contracts, operations, and systems. GS 11 elevates the role of internal assurance in preventing Shariah non-compliance and strengthening institutional integrity.

AAOIFI GS 20: *SSB Functions and Operations* sets out the detailed framework governing the roles, responsibilities, and operational procedures of the Shari'ah Supervisory Board (SSB) within Islamic financial institutions. The standard defines the SSB's mandate, outlines its core functions in issuing Shari'ah decisions (fatwas), reviewing products and contracts, and overseeing Shari'ah compliance across all activities of the institution. It specifies requirements for SSB governance, independence, membership criteria, reporting lines, documentation standards, meeting procedures, confidentiality, and conflict-of-interest safeguards. GS-20 also describes the interaction between the SSB and internal Shari'ah control, Shari'ah audit, and management functions, and sets expectations for monitoring, rectification of Shari'ah breaches, and disclosure obligations.

AAOIFI GS 21: *SSB Review and Report* provides detailed guidance on the review responsibilities and reporting procedures of SSBs. It requires SSBs to conduct comprehensive Shariah reviews—distinct from audits—aimed at assessing the institution's conformity with Shariah principles across all activities, policies, and contracts. The standard stipulates the structure, content, and disclosure requirements of the annual Shariah report, including the SSB's opinion on compliance, identified breaches, and rectification measures. GS 21 strengthens market discipline by ensuring consistent, transparent, and credible Shariah reporting, thereby reinforcing public trust in Islamic financial institutions.

AAOIFI ASIFI 6: *External Shariah Audit* establishes the framework for external, independent Shariah assurance engagements conducted by qualified Shariah auditors. The standard defines the objectives, scope, ethical requirements, audit planning procedures, evidence-gathering techniques, materiality considerations, and reporting

obligations of an external Shariah audit. It ensures that an independent third party verifies the institution's compliance with Shariah principles, relevant AAOIFI standards, and the rulings of its SSB. ASIFI 6 enhances the credibility of Shariah assurance by aligning it with international assurance practices while preserving the unique requirements of Islamic finance.

3.2 Guiding Framework for ORM in Banks: Domestic

The domestic framework for operational risk management (ORM) in Bangladesh's Islamic banking sector has evolved through a series of deliberate regulatory, institutional, and policy actions undertaken since the early 1980s. The establishment of Islami Bank Bangladesh Limited in 1983 marked the formal beginning of Islamic banking operations, but this milestone was preceded by significant diplomatic and policy engagements—including Bangladesh's accession to the Islamic Development Bank in 1974 and successive international endorsements in 1978 and 1980—that laid the groundwork for a Shariah-based financial system. Building on these foundations, Bangladesh Bank progressively developed a regulatory architecture to support, supervise, and standardize Islamic banking practices, culminating in structured guidelines, preferential regulatory treatments, liquidity-support mechanisms, and oversight arrangements that together shaped the contemporary operational landscape of Islamic banks in the country. This historical progression anchors the domestic guiding framework for ORM and informs the operational guidelines that govern the sector today.

Bank Companies Act 1991

The Bank Companies Act, 1991 provides the fundamental legal foundation for the regulation and supervision of all banking activities in Bangladesh, including Islamic banking. Although the Act was originally framed for the conventional system, its prudential provisions—covering licensing, capital adequacy, liquidity requirements, risk management, corporate governance, inspection, and enforcement—apply equally to Islamic banks unless specifically exempted or supplemented by Bangladesh Bank. Over time, the Act has served as the principal statutory reference through which Bangladesh Bank exercises its authority to issue circulars, guidelines, and directives tailored for Shariah-based operations. In effect, the Act anchors regulatory legitimacy, empowers Bangladesh Bank to oversee both conventional and Islamic modes of banking, and enables the development of a coherent supervisory framework that accommodates the operational specificities of Islamic financial institutions while maintaining systemic discipline and financial stability.

Guidelines for Conducting Islamic Banking 2009

Bangladesh Bank issued the Guidelines for Conducting Islamic Banking on November 09, 2009 through BRPD Circular No. 15, invoking its authority under Section 45 of the Bank Companies Act, 1991. This circular marked the first comprehensive regulatory framework tailored specifically for the Islamic banking sector in Bangladesh. After Islamic banking had already become part of the mainstream financial system, the central bank recognized significant structural and operational differences between Shariah-based financing and interest-based banking. The 2009 Guidelines were therefore introduced to enhance transparency, accountability, governance, and Shariah compliance, ensuring that Islamic banks operated under a uniform and enforceable regulatory regime.

Section I of the Guidelines provides clear statutory definitions to distinguish Islamic banking activities from conventional operations. An "Islamic bank" is defined as a banking company—or a designated Islamic banking branch of a conventional bank—licensed by Bangladesh Bank that conducts all of its operations strictly in accordance with Islamic Shariah. Such an institution must avoid the receipt or payment of interest at every stage of its activities and must ensure that all products, transactions, and financial relationships adhere fully to Shariah principles. Similarly, "Islamic banking business" refers to banking activities whose objectives, processes, and operational practices are entirely grounded in Islamic Shariah. This definition requires that no component—whether in form, structure, or underlying substance—contains any element that contradicts Shariah rules. Together, these definitions create a clear regulatory boundary, ensuring that only genuinely Shariah-compliant institutions and activities fall within the scope of Islamic banking as recognized by Bangladesh Bank. A core requirement of the guidelines is the preparation of a detailed operational manual, mandated under Section II, which serves as the primary instrument for managing operational risk for a dual Islamic bank. This manual must clearly outline the segregation of Islamic funds from conventional funds, define internal processes and control mechanisms, and establish procedures to protect depositors' interests and uphold the contractual integrity of Shariah-compliant transactions. Consistent with these provisions, the guidelines require full segregation and prudential management of Islamic banking funds through dedicated accounting systems, separate record-keeping, and robust MIS frameworks to prevent commingling and ensure accurate profit allocation. In managing operational risks, banks are instructed to adopt a structured risk identification process that includes rigorous pre-sanction due diligence and continuous post-sanction monitoring of assets and clients. To complement these measures, banks must maintain strong internal controls, implement standardized

documentation, and ensure system-based oversight to reduce the likelihood of process failures.

The guidelines further provide a clear roadmap for converting a conventional bank into a full-fledged Islamic bank or establishing Islamic windows. This transformation requires the restructuring of interest-bearing assets, reconfiguration of liabilities, adjustment of operational processes, and alignment of all activities with Shariah principles. In line with operational risk mitigation expectations, banks must adopt strategies such as avoiding non-permissible activities, strengthening collateral and guarantees in accordance with Shariah, preventing losses through enhanced controls, and establishing duplication and contingency measures for critical functions. The guidelines also reinforce the Shariah compliance architecture by assigning the Board of Directors primary responsibility for ensuring that all operations, products, and contracts comply with Islamic jurisprudence. While the formation of an independent Shariah Supervisory Committee (SSC) is permitted—and encouraged—the Board retains ultimate accountability for any Shariah irregularity or non-compliance.
In addition to governance and compliance, the guidelines introduce structured reporting mechanisms covering Shariah compliance status, operational performance, and financial statements. The guidelines elaborate on the principles governing Islamic deposits, investment modes, CRR/SLR maintenance for Islamic banks, and frameworks for determining and distributing rates of return, thereby reducing displaced commercial risk and ensuring equitable treatment of investment account holders.

Internal Shariah Audit Guidelines

Bangladesh Bank issued Guidelines on Internal Control & Compliance in Banks 216 incorporating a dedicated section on internal Shariah Audit through BRPD Circular No. 03 dated March 08, 2016, which strengthened the internal control and Shariah governance structure of Islamic banks and Islamic banking windows in Bangladesh. While Islamic banking operates under the Bank Companies Act 1991 and the 2009 Islamic Banking Guidelines, Bangladesh Bank recognized the need for a dedicated mechanism to supervise Shariah compliance beyond conventional internal audit practices. The ICC Guidelines therefore formalized Shariah audit as a distinct function, responsible for assessing adherence to Shariah principles, validating contractual and documentation processes, and ensuring that all financing operations comply in form and substance with Islamic jurisprudence. The guidelines highlight that Shariah violations can lead to operational lapses, invalid contracts, reputational damage, legal consequences under BB regulations, and the generation of non-halal income.

To support risk-based supervision, the framework introduced a Shariah non-compliance risk rating system, classifying branches based on major and minor violations—such as disbursing cash in Bai-based modes, adjusting investments without asset transfers, bypassing documentary requirements, or obtaining backdated cash memos. Banks are required to develop a Shariah Index using this rating, which determines inspection frequency and priority. The Shariah audit process includes annual risk-based planning, surprise inspections of high-risk branches, and structured reporting of deficiencies to the SSC Secretariat, CEO, and Board. Quarterly summary reports must document audit findings and corrective measures. Overall, the ICC Guidelines 2016 enhance operational discipline, strengthen Shariah assurance, and reduce Shariah non-compliance and operational risks across Islamic banks in Bangladesh.

Guidelines on Risk Based Capital Adequacy 2014

Bangladesh Bank's Capital Adequacy Guidelines 2014, issued under the Basel III framework, strengthened the prudential capital regime for all scheduled banks, including Islamic banks. The 2014 framework introduced higher quality capital requirements, enhanced risk coverage, leverage constraints, and prudential buffers—all of which have direct implications for operational risk management (ORM). Under this guideline, banks must maintain a minimum Capital to Risk-Weighted Assets Ratio (CRAR) composed primarily of Common Equity Tier 1, alongside Additional Tier 1 and Tier 2 elements, after regulatory deductions. Importantly, the RBCA framework assigns explicit capital charges to operational risk, requiring banks to calculate capital under the Basic Indicator Approach (BIA) or the Standardized Approach (TSA). This embeds ORM within Pillar 1 capital computation and makes the strength of internal control, ICT governance, process integrity, Shariah compliance, and human resource capabilities critical determinants of capital adequacy.

Pillar 2 of the guideline—Supervisory Review Process (SRP)—further links operational risk to capital by requiring banks to assess risks not fully captured under Pillar 1, such as system failure risks, model risks, cyber and fraud risks, documentation weaknesses, and internal governance failures. Bangladesh Bank may impose additional capital requirements through the SREP dialogue if operational risk controls are inadequate. The framework also mandates stress testing, internal capital adequacy assessment (ICAAP), and enhanced disclosure under Pillar 3, promoting transparency of operational loss events, governance structures, and control functions.

Risk Management Guidelines 2018

Bangladesh Bank's Risk Management Guidelines 2018 provide the foundational supervisory benchmark for strengthening banks' internal control, governance, and risk oversight—core elements directly relevant to the operational risk management. The guidelines unify and update previous circulars to enforce a more structured, enterprise-wide risk culture, emphasizing board-approved risk appetite, strengthened roles for the Board Risk Management Committee (BRMC), Executive Risk Management Committee (ERMC), and the mandatory appointment of a Chief Risk Officer (CRO). For operational risk, the 2018 framework mandates comprehensive identification, assessment, mitigation, monitoring, and reporting processes, supported by updated organograms, clear segregation of duties, enhanced MIS, and scenario-based stress testing. Notably, it requires banks to institute robust internal controls, annual reviews of risk management effectiveness, and periodic reporting to Bangladesh Bank. For Islamic banks, these requirements reinforce the need for a system-based operational risk framework, improve the discipline around non-compliance risk, and ensure stronger governance, documentation, and audit mechanisms across all operational processes.

Other Circulars and Directives of Bangladesh Bank

Bangladesh Bank has progressively expanded the regulatory architecture for Islamic banking, particularly in the area of liquidity management and Shariah governance. The Bangladesh Government Islamic Investment Bond (BGIIB)—introduced in 2004 (amended in 2014 through DMD Circular No.05 dated 1st September, 2014)—was the first Shariah-compliant instrument designed to support Islamic banks in managing their liquidity in the absence of conventional interest-based tools. BRPD Circular Letter No. 42 (26 October 2022) replaced conventional refinance facilities with a Shariah-compliant prefinance structure. Similarly, BRPD Circular Letter No. 30 (8 July 2024) introduced prudential regulations for online banking services offered by conventional banks operating Islamic branches or windows to ensure that digital financial operations remain fully aligned with Shariah standards.

In the liquidity domain, BB has issued several specialized circulars. The regulatory framework also includes market-based liquidity arrangements. The Islamic Interbank Fund Market (IIFM), introduced through DOS Circular Letter No. 23 of 2011, provides a Shariah-compliant substitute for the conventional call money market using contracts such as Mudarabah, Wakalah, Murabahah, and Wadiah. BB issued DMD Circular 03 dated 05 December 2022 (subsequent amendment made through DMD Circular Letter No. 05 dated March 25, 2024) on introduction of Islamic Bank's Liquidity Facility (IBLF) to facilitate the short-term liquidity facility for scheduled Islami banks. BB issued DMD Circular 02 dated 05 February 2023 on introduction of

Mudaraba Liquidity Support (MLS) to facilitate the short-term liquidity facility for scheduled Islami banks. BB issued a letter (Ref. No. DMD/239/2024-149, dated 18 January 2024) on the issue of Special Liquidity Support (SLS) to facilitate the short-term liquidity facility for Islami banks. It also issued DMD Circular No. 05 (21 October 2020), which set out operational guidelines for the management of Bangladesh Government Investment Sukuk (BGIS), further strengthening the availability of Shariah-based liquidity instruments.

In the area of Shariah governance, IBRPD Circular No. 01 (28 September 2025) provides a comprehensive framework for the formation, appointment, removal, roles, and responsibilities of Shariah Supervisory Committee (SSC) members. This circular significantly strengthens Shariah oversight functions and ensures uniform governance standards across all banks offering Islamic banking services. Collectively, these regulatory instruments broaden the prudential, operational, and governance framework for Islamic banks in Bangladesh.

Chapter 4: ORM Practices in Banks of Bangladesh

4.1 ORM Practices in Banks in Bangladesh: Questionnaire Survey

A semi-structured questionnaire survey has been conducted and opinions have shared by the responding banks. The survey has been conducted comprising banking experts such as, the Head and the Deputy Head of the risk management department through FGD and KII to observe the status and challenges regarding the operational risk management in the Islamic banks in Bangladesh.

ORM Governance and Institutional Framework

The governance structure of operational risk management across the banking industry in Bangladesh remains inconsistent and weak. Only about one-third of banks maintain a standalone ORM unit, while many continue to integrate ORM within enterprise risk management or decentralize it across departments without proper coordination. Nearly one-fourth of banks still lack any formal ORM governance framework. Such structural deficiencies reflect the absence of a unified institutional approach, resulting in fragmented accountability and weak oversight.

Board and Senior Management Oversight

Board and senior management involvement in ORM is generally inadequate. Only around 30 percent of banks review ORM practices at the Board Risk Committee level, while others depend on irregular or internal departmental reporting. About one-fifth of the banks show no concern for ORM oversight at all, demonstrating a lack of strategic engagement at the leadership level. This limited attention from top management weakens the integration of risk management into corporate decision-making.

Implementation of the Three Lines of Defense

The adoption of the Three Lines of Defense model is largely informal. Only about 17 percent of banks have fully implemented the model across all business units, while most either apply it partially or without clear definitions. This indicates that the majority of institutions operate without clearly defined responsibilities for risk ownership, control, and assurance, which undermines accountability and control effectiveness.

Risk Identification and Control Tools

Risk identification in most banks relies heavily on internal audits and compliance oversight, representing a reactive rather than proactive risk management culture. Approximately 60 percent of banks depend on audit findings to identify operational risks, whereas tools such as Key Risk Indicators (KRIs), loss event databases, and

scenario analyses remain underutilized. This overreliance on audit and post-event assessments prevents early detection and mitigation of emerging operational risks.

Regulatory Compliance and Alignment

Compliance practices show uneven alignment with both domestic and international standards. About half of the banks align ORM practices with Bangladesh Bank regulations, while 40 percent follow Basel standards. However, nearly one-third of institutions exhibit limited or inconsistent compliance. The lack of uniformity in regulatory adherence demonstrates a weak regulatory culture and the need for stronger supervisory enforcement to ensure consistency across the sector.

Data Management and Scenario Analysis

Loss event and incident data management remains one of the weakest areas. Only 20 percent of banks maintain a centralized loss data system, while about 25 percent do not record such data at all. Scenario analysis, an essential element of forward-looking ORM, is also inadequately practiced—only about one-fourth of banks conduct it regularly across all business lines. The main barriers include lack of standardized methodology, limited historical data, and insufficient expertise.

Monitoring and Reporting Mechanisms

Operational risk monitoring remains largely dependent on internal audit and compliance functions, with 57 percent of banks using these as primary monitoring tools. Only 28 percent employ standardized dashboards or KRIs for real-time tracking of operational risk. Although ORM reporting is relatively consistent—mostly conducted on a monthly or quarterly basis—the lack of analytical depth and integration into decision-making weakens its effectiveness.

Outsourcing and Vendor Risk Management

Outsourcing-related operational risks are poorly addressed in most banks. Only around 35 percent conduct vendor risk assessments or maintain a formal vendor management policy, while nearly 30 percent have no framework at all. Given the growing dependency on third-party service providers, particularly in IT and payment systems, this gap poses a significant threat to operational resilience.

Cybersecurity and IT Risk

Cybersecurity risk is predominantly managed by IT departments, with minimal involvement of ORM or internal audit. Approximately 70 percent of banks depend solely on IT and information security teams, while only 3 percent ensure cross-functional coordination involving ORM, audit, and IT. This narrow approach isolates cybersecurity from the broader ORM framework and leaves banks vulnerable to systemic digital threats.

Risk Culture and Human Capital Development

The development of a strong risk culture remains in its early stages. Around 60 percent of banks conduct regular ORM training programs and communication campaigns, yet only 20 percent assess risk culture formally, and 15 percent link staff incentives to risk-related performance. While half of the banks conduct post-training assessments, there are no standard benchmarks to measure training effectiveness. This indicates that capacity building in ORM remains procedural rather than strategic.

Overall Insights and Implications

The findings indicate that operational risk management in Bangladesh's banking industry is still compliance-driven and fragmented. ORM practices lack integration, standardization, and forward-looking methodologies. Weak governance, limited use of analytical tools, insufficient data systems, and inadequate staff engagement hinder the maturity of ORM frameworks. As the industry becomes increasingly digital and interconnected, banks must adopt a holistic ORM approach that aligns with Basel III and IFSB-13 standards. Strengthening governance, formalizing data-driven monitoring, ensuring cross-functional coordination, and building a culture of proactive risk ownership are essential steps toward achieving a resilient and sustainable banking system.

4.2 Operational Risk in Banks of Bangladesh: Case Studies

Similar to many other developing countries, Bangladesh's banking sector faces a range of operational risk factors linked to human error, weak internal processes, cybersecurity threats, financial misconduct, and overall operational complexities. However, some operational vulnerabilities in the sector stand out due to their magnitude and seriousness. These critical areas warrant closer examination to alert policymakers and bank leadership about the urgent need to strengthen governance and enhance operational risk management practices. Drawing on the cases outlined in Appendix II, the key issues can be identified as follows.

Governance-Related Risks

- Weak board oversight and political influence undermine independence and accountability, as boards and sponsor-directors often misuse authority, approve unethical financing proposal, and divert funds for personal benefit. Strong corporate governance, fit-and-proper criteria, and board independence are essential for ORM integrity.
- Breakdown of Shariah governance in Islamic banks occurs when competent board and Shariah committee members are replaced by politically influenced individuals, leading to governance collapse. Integration of Shariah governance

within ORM is necessary to ensure Shariah-compliant decisions and independent oversight.

- CRO vs CCRO conflict arises because CROs in Bangladesh are frequently appointed from credit backgrounds and limit their roles to credit risk, neglecting comprehensive risk management. Banks must establish a dedicated, independent CRO responsible for all risk categories, including credit, market, operational, IT, and Shariah non-compliance risks.
- Fraudulent approvals and collusive governance are evident in large-scale scams, where executives, directors, and customers acted in collusion. Segregation of duties, internal control over approvals, and governance audits are essential safeguards.
- Lack of ethical culture and accountability is reflected in persistent irregularities and self-serving behavior across institutions. Building a strong risk culture, implementing a code of conduct, and enforcing a zero-tolerance policy for misconduct are crucial to maintaining operational integrity.

People-Related Risks

- Incompetence and lack of professionalism arise from appointing unqualified personnel and discontinuing training programs, reducing overall risk awareness. Strengthening talent management, capacity building, and professional certification (e.g., CIBFP, CSAA, CIPA) is essential for key risk functions.
- Internal collusion and fraud occur through document forgery, unauthorized withdrawals, and fake investment accounts, reflecting serious ethical lapses among staff. Behavioral risk assessments, whistleblowing mechanisms, and staff rotation policies are vital to detect and prevent such collusion.
- Lack of segregation of duties allows employees to exploit overlapping responsibilities, particularly during branch transfers and digital transitions. Enforcing job rotation, dual control, and hierarchical approval processes is necessary in all sensitive areas.
- Mismanagement in agent banking emerges from agent-level fraud, fund misuse, and customer deception, exposing weak human oversight. Strict background verification, digital monitoring, and structured training for agents are required to reduce these risks.
- Change management failures result from poor staff handling during technological or organizational transformations, leading to errors and fraud. Aligning change

management and human resource strategies with operational risk assessment and control mechanisms is essential for stability.

Process-Related Risks

- Process failure leading to high NPIs results from weak appraisal, monitoring, and recovery mechanisms that allowed credit defaults to escalate. Strengthening credit approval workflows, post-disbursement monitoring, and early warning systems is essential to reduce such risks.
- Bypassing core banking procedures occurs when approval hierarchies and internal controls are ignored, enabling corruption and financial misreporting. Strict adherence to standard operating procedures, process documentation, and audit trails is mandatory for transparency and accountability.
- Inadequate internal control and compliance expose banks to fraud through fake trade documents, shell companies, and fictitious letters of credit. Reinforcing internal audit functions, verifying trade finance activities, and automating compliance systems are crucial preventive measures.
- Deficient change and transition procedures during system upgrades or organizational shifts lead to fraud and data manipulation due to insufficient testing and segregation. Implementing change control protocols, approval gates, and post-change review processes is vital for process reliability.

System-Related Risks

- Cybersecurity vulnerabilities, as evidenced by the Bangladesh Bank cyber heist and ATM scams, expose weaknesses in system architecture and digital defense. Strengthening cyber resilience through multi-layered protection, real-time fraud detection, and dedicated incident response teams is crucial.
- Data integrity and manipulation at the head office level led to distorted financial reporting and loss of transparency in operations. Establishing robust data governance frameworks, access control mechanisms, and periodic data integrity audits are necessary to ensure reliability and accountability.
- Technological risks in MFS and e-money operations arise from fraudulent e-money creation and misuse of customer data within mobile financial platforms. Enforcing secure digital verification, system audits, and strong authentication controls across all fintech services is vital to prevent financial and reputational losses.
- Business continuity and disaster recovery deficiencies were evident during cyber disruptions, as many banks lacked predefined frameworks to sustain critical

operations. Developing comprehensive BCP and DR plans, real-time data replication, and alternative data centers is fundamental for operational resilience.

External Environment-Related Risks

- Trade-based money laundering (TBML) through large-scale trade mis-invoicing undermines the country's financial integrity and stability. Implementing AI-driven trade surveillance systems, integrating cross-border data, and enhancing due diligence are necessary to detect and prevent illicit flows.
- Regulatory gaps and inconsistent enforcement by supervisory bodies have enabled systemic irregularities and recurring financial scams. Strengthening supervisory enforcement, ensuring better coordination among regulators, and adopting risk-based inspection frameworks are essential to close these gaps.
- Political and external interference in credit approvals, board appointments, and management decisions compromise institutional independence and transparency. Safeguarding bank autonomy and insulating risk management functions from political influence are vital for sound governance.
- The evolving digital and market environment introduces emerging threats such as data breaches, third-party risks, and rapid technological changes. Continuous adoption of regulatory technology (RegTech) and supervisory technology (SupTech) is essential for proactive operational risk management.

Operational risk remains the most dominant source of distress in Bangladesh's banking sector, often appearing as credit-related issues but fundamentally rooted in governance lapses and internal process deficiencies. Islamic banks encounter a dual dimension of operational risk—traditional risks arising from systemic and procedural weaknesses, and Shariah-specific risks stemming from non-compliance and ethical violations. The reviewed cases collectively emphasize that governance reform, modernization of internal control systems, digital security enhancement, and the promotion of an ethical banking culture are vital to building institutional resilience. To ensure sustainable and compliant operations, banks must adopt holistic ORM frameworks aligned with international standards, while remaining consistent with core Shariah principles of *Mukhatarah*, *Al-Ghunm-bil-Ghurm*, and *Maqasid al-Shariah*.

Chapter 5: Findings and Data Analysis

5.1 Islamic Banking in Bangladesh

The four-year balance-sheet trend shows steady expansion of the bank's operations, with total assets rising from BDT 4,508 billion in 2021 to BDT 5,820 billion in 2024, driven mainly by consistent growth in general investments (Table 5.1). Liquidity components fluctuate, as cash in hand increases until 2023 before declining, and balances with Bangladesh Bank fall sharply—indicating tighter liquidity conditions and greater reliance on interbank placements, which rise notably in 2024. The investment portfolio shifts toward non-government securities, causing total investments in shares and securities to increase significantly in 2024. While fixed assets remain stable, a sharp rise in "other assets" signals higher receivables or pending adjustments, which may carry operational risk. On the liability side, deposits continue to dominate funding but grow slowly and shift toward higher-cost term deposits, while dependence on interbank borrowings increases markedly, pointing to liquidity pressure. Total equity declines in 2024 despite asset growth, weakening the capital buffer. Off-balance-sheet exposures increase moderately, reflecting continued trade-related activity. Overall, the data depict a bank expanding its financing portfolio while facing tightening liquidity, rising operational exposures, and increasing dependence on wholesale funding—elements directly relevant for assessing operational and liquidity-related risks in Islamic banking.

Table 5.1: Aggregated Balance Sheet of IBs (Amount in Billion BDT)

Particulars	2021	2022	2023	2024
Cash in Hand (including FC)	41.7	52.3	60.9	53.5
Balance with BB and SB (including FC)	385.2	257.2	257.6	234.8
Balance with other Banks and FIs	162.8	196.2	176.1	211.2
Placement with other Banks and FIs	18.3	8.0	8.3	7.0
Investments in Share and Securities				
Government	134.7	109.8	127.6	131.5
Others	171.6	170.3	177.3	291.4
Total Investments Share and Securities	**306.4**	**280.1**	**304.8**	**422.9**
General Investments	3282.2	3739.8	4026.2	4334.1
Bills Purchased and Discounted	132.4	208.7	249.7	113.6
Total Investments and Advances	**3414.7**	**3948.5**	**4275.9**	**4447.7**
Fixed Assets	55.7	56.3	53.7	53.2
Other Assets	122.4	171.1	251.9	388.8
Non-banking Assets	0.9	0.9	0.9	0.9
Total Assets	4508.0	4970.7	5390.2	5820.1
Liabilities				
Placement from other Banks/FIs/Agents	285.4	579.0	678.1	956.9
Current Deposit	411.0	412.3	471.2	427.8

Savings Deposit	766.9	802.5	773.6	751.2
Fixed/Term Deposit	2015.6	2002.4	2223.7	2319.9
Interbank Deposit	114.3	152.6	151.9	204.4
Other Deposit	352.5	397.5	361.4	354.4
Total Deposits	3660.4	3767.3	3981.7	4057.7
Bills Payable	31.3	37.5	48.7	41.0
Other Liabilities	326.2	361.8	443.3	553.2
Total Liabilities	4303.3	4745.5	5151.9	5608.9
Total Equity	204.7	225.1	238.3	211.2
Total Liabilities & Shareholder's Equity	4508.0	4970.7	5390.2	5820.1
Off-balance Sheet Items	774.9	807.2	775.8	848.2

Source: *Financial Stability Report 2024, Bangladesh Bank*

The aggregated income statement (Table 5.2) shows that Islamic banks experienced strong growth in profit income from 2021 to 2024, rising from BDT 248.6 billion to BDT 387.5 billion, but this gain was offset by a sharp increase in profit expenses—particularly in 2024—resulting in a decline in net profit income despite higher earnings. Non-profit and investment income fluctuated but strengthened again in 2024, contributing to a modest rise in total income. Operating expenses increased steadily each year, reflecting cost pressures associated with general overhead. Profit before provision remained positive but weakened in 2024 as funding costs and expenses escalated. The most notable shift is the surge in total provisions in 2024, which more than doubled compared to previous years, largely compressing profitability. Overall, while income generation improved over the period, the combined effect of higher profit expenses, rising operating costs, and substantial provisioning significantly eroded the bottom-line profitability of Islamic banks in 2024.

Table 5.2: Aggregated Income Statement of IBs (Amount in Billion BDT)

Particulars	**2021**	**2022**	**2023**	**2024**
Profit Income	248.6	266.3	324.6	387.5
Less: Profit Expenses	160.0	177.0	214.3	291.6
Net Profit Income	**88.6**	**89.3**	**110.2**	**96.0**
Non-Profit/Investment Income	35.6	54.7	49.0	66.3
Total Income	**124.1**	**144.0**	**159.2**	**162.3**
Operating Expenses	69.4	84.0	90.3	101.3
Profit before Provision	**54.7**	**63.6**	**69.0**	**61.0**
Total Provision	13.7	13.3	14.9	38.2
Profit before Taxes	**41.0**	**50.3**	**54.1**	**22.8**
Provision for Taxation	20.7	24.5	26.5	16.1
Profit after Taxation	20.3	25.8	27.6	6.7

Source: *Financial Stability Report 2024, Bangladesh Bank*

The performance comparison shows that Islamic banks outperformed the industry in profitability and efficiency from 2021 to 2023, with higher ROA, ROE, profit margins, and stronger profit income relative to total assets (see Table 5.3). However, in 2024 their performance deteriorated sharply: ROA and ROE declined steeply, capital adequacy turned negative, and classified investments rose dramatically, indicating severe stress in asset quality and capital buffers. It is widely recognized that the ongoing crisis in Bangladesh's banking sector is not a result of business model failure, but rather a fundamental breakdown in ORM.

Table 5.3: Comparative Performance of Banking Industry and IBs (%)

Indicators	2021		2022		2023		2024	
	All	IBs	All	IBs	All	IBs	All	IBs
ROA	0.2	0.5	0.6	0.5	0.6	0.5	0.43	0.12
ROE	4.4	9.9	10.7	11.5	11.1	11.6	8.70	3.18
Net Profit Margin	1.3	2.3	1.4	2	1.6	2.3	1.30	1.89
Interest (Profit) Income to Total Assets (TA)	4.3	5.5	4.4	5.4	4.9	6.0	5.58	6.66
Net Interest (Profit) Income to TA	1.1	2.0	1.2	1.8	1.4	2.0	1.12	1.65
Non-Interest (Profit) Income to TA	2.0	0.8	2.1	1.1	2.0	0.9	2.43	1.14
Advance (Investment) to Deposit Ratio	73.2	84.7	79	91.4	80.4	95.3	81.55	97.06
CRAR	11.1	12.8	11.8	12.7	11.6	12.7	3.08	-4.95
Classified Loans (Investment) to Advances	7.9	4.0	8.2	4.1	9.4	4.8	20.20	23.18
Classified Loans (Investment) to Capital	80.7	67.2	95	72.1	107.8	81.7	263.04	489.5

Source: *Financial Stability Report 2024, Bangladesh Bank*

The comparative figures presented in Table 5.4 show that both Islamic banks and conventional banks allocate the largest share of regulatory capital to credit risk. Market-risk capital is consistently the smallest component for Islamic banks, averaging just 2.20 percent. Islamic banks allocate around 8.07 percent of total capital to operational risk, a figure moderately lower than the 9.01 percent observed for conventional banks, although some Islamic banks—such as Shahjalal Islami Bank PLC—show significantly higher operational-risk proportions due to Shariah-sensitive processes and compliance complexities. It is well-known that both credit and market risks are mostly affected by the competency of associated people, internal procedures, comprehensiveness of IT infrastructure and external parties. Therefore, all risks could be managed properly if a bank can manage its operational risk prudently.

Table 5.4: Comparative Capital Requirements of IBs and CBs in 2023

S/n	Name of Bank	Capital Requirement for Credit Risk		Capital Requirement for Market Risk		Capital Requirement for Operational Risk		Total Capital Requirement of the Bank	
		(BDT Million)	%	(BDT Million)	%	(BDT Million)	%	(BDT Million)	%
A	**Purposively Selected 7 Full-Fledged Islamic Banks**								
1	Islami Bank Bangladesh PLC (IBB)	77,742.21	90.56	1,073.31	1.25	7,028.12	8.19	85,843.64	100
2	First Security Islami Bank PLC (FSIB)	30,543.30	89.45	802.80	2.35	2,799.40	8.20	34,145.50	100
3	Al-Arafah Bank PLC (AAIB)	28,352.59	90.60	523.53	1.67	2,418.70	7.73	31,294.83	100
4	Social Islami Bank (SIB)	27,814.92	90.92	605.13	1.98	2,172.25	7.10	30,592.30	100
5	Shahjalal Islami Bank PLC (SJIB)	19,274.77	85.05	641.65	2.83	2,746.26	12.12	22,662.68	100
6	Export Import Bank of Bangladesh PLC (EXIM)	3,391.65	89.23	194.02	5.10	215.53	5.67	3,801.20	100
7	Union Bank PLC (Union)	1,796.23	92.26	4.64	0.24	145.98	7.50	1,946.85	100
	Average	**26,987.95**	**89.72**	**549.30**	**2.20**	**2,503.75**	**8.07**	**30,041.00**	**100**
B	**Purposively Selected 7 Conventional Banks**								
1	IFIC Bank PLC (IFIC)	40,502.41	90.87	1,918.00	4.30	2,152.50	4.83	44,572.91	100
2	Eastern Bank PLC (EBL)	26,635.00	85.41	1,423.00	4.56	3,127.00	10.03	31,185.00	100
3	Mercentile Bank PLC (MBL)	25,698.40	87.86	696.10	2.38	2,854.60	9.76	29,249.10	100
4	Trust Bank PLC (Trust)	25,288.65	89.70	263.72	0.94	2,640.82	9.37	28,193.19	100
5	Bank Asia PLC (BA)	21,269.00	86.04	741.00	3.00	2,709.00	10.96	24,719.00	100
6	Dhaka Bank PLC (Dhaka)	20,761.50	89.20	455.90	1.96	2,057.60	8.84	23,275.00	100
7	NCC Bank PLC (NCC)	17,803.47	85.69	1,037.34	4.99	1,935.40	9.32	20,776.21	100
	Average	**25,422.63**	**87.82**	**933.58**	**3.16**	**2,496.70**	**9.01**	**28,852.92**	**100**

Source: *Annual Report of the Concerned Banks*

5.2 Summary of FGD and KII Outcomes

5.2.1 Perception About Salient Operational Risks of Islamic Banks

From the BASEL perspective, banking risks may be categories as Credit, Operational, Market, and Liquidity Risk. The figure presents a structured view of the major risk dimensions faced by Islamic banks, highlighting how operational risk interacts with other core risk categories and with Shariah-related considerations. It shows that Islamic banks are exposed to the standard financial risks found in any banking system—credit, operational, market, and liquidity risks—but with additional layers of complexity arising from their Shariah obligations. Under operational risk, the figure captures the main sources of vulnerability: people, processes, systems, and external events, which together explain the majority of day-to-day breakdowns observed in practice. The credit-risk components—such as covenants, financing amount, and profit or rent arrangements—reflect how lapses in documentation, contract execution, or collateral management can trigger operational failures, which lead to Shariah non-compliance risk. Market-risk factors include rate of return, exchange rate and commodity price movements, and equity market volatility. However, these factors illustrate the operational challenges Islamic banks face when managing Shariah-compliant assets and liabilities without relying on conventional hedging tools. Similarly, liquidity-risk elements may be explained from regulatory compliance, surplus or deficit liquidity position. These elements may lead to the Shariah non-compliance risk due to lack of instrument, proper mechanism and instruments.

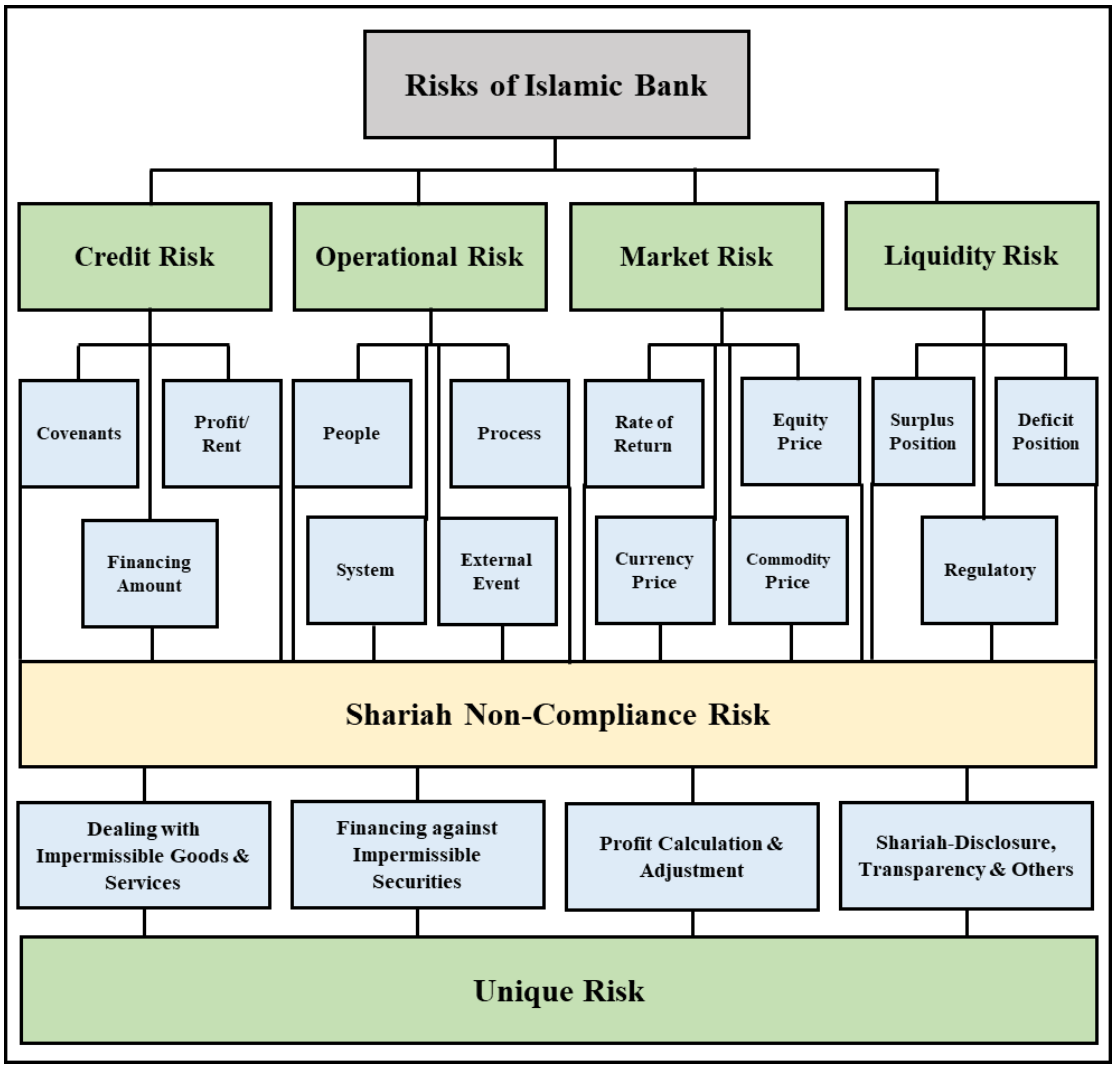
Therefore, the figure places Shariah non-compliance risk at the center, emphasizing that many operational failures in Islamic banks originate from deviations in product structuring, transaction execution, profit calculation, or dealings involving impermissible goods, services, or securities. These breaches not only create financial loss but also significant reputational and fiduciary consequences. The final layer, labeled “unique risk,” underscores that Islamic banks carry distinctive exposures not present in conventional institutions due to their additional requirements for compliance with Shariah principles.

Regulatory frameworks typically prohibit banks from dealing in certain goods and services, and Shariah requirements further narrow this permissible universe for Islamic banks. As a result, Islamic banks must ensure that all underlying assets used as security, or as the subject matter of financing, are fully Shariah-compliant in addition to being financially viable. This creates added complexity in calculating rate of profit/rent, service charges, or profit for the Mudarabah depositors where both Shariah principles and statutory requirements must be observed simultaneously. Moreover, Islamic banks must maintain clear, continuous communication with

contracting parties during contract execution, including when modifying covenants or adjusting terms. Such additional layers of contractual discipline and transparency, while not always necessary in conventional banking, are essential to safeguarding Shariah compliance and minimizing operational risk in Islamic finance.

Overall, the figure illustrates that operational risk in Islamic banks is multidimensional, heavily intertwined with Shariah governance, and deeply dependent on proper internal controls, accurate documentation, and disciplined adherence to permissible practices—making it a critical area for strengthening risk management frameworks.

Figure 5.1: Salient Operational Risk of Islamic Banks



Source: *Compilation by the Authors based on the FGD and KII*

The Box 5.1 highlights that many risk exposures in Islamic banks ultimately materialize through operational weaknesses, as errors in executing contracts, managing processes, or maintaining controls can easily convert ordinary credit, market, liquidity, or unique exposures into Shariah-related issues. In credit operations, issues arise when terms are not aligned with Shariah or documentation lacks proper structure. Market-related exposures become problematic when contracts are mishandled, rates are applied incorrectly, or impermissible instruments are used. Liquidity stress can also lead to non-compliant fund-raising or investment decisions if operational safeguards are weak. In addition, unique risks—such as dealing with impermissible assets, improper profit recognition, or inadequate disclosure—require strict procedural discipline. Therefore, the quality of people, processes, systems, and governance determines whether these risks remain contained or escalate into Shariah non-compliance, making robust operational control indispensable for Islamic banks.

Box 5.1: Relationship of Others Risks with Operational Risk of Islamic Banks

A. Credit Risk

a. Breach of Covenants: Lack of proper documentations and inclusion of impermissible covenants in credit document and contract may lead to Shariah non-compliance. For example, in case of HPSM, bank imposes customer to have an insurance at his own cost however, if the insurance does not cover the financing amount, client will be liable to settle the payment to the bank. In case of Murabahah, generally banks include compensation clause (in lieu of undertaking to donate) as a part of the agreement without segregating procrastinating debtor and forced measures.

b. Default in Payment of Financing or Investment Amount: As a part of credit risk mitigation, there is practice taking security through creation of charges. However, if the security is not Shariah permissible, it would be a Shariah non-compliance risk.

c. Default in Payment of Profit/Rent: As a part of credit risk mitigation, there is practice of rescheduling of debt. However, rescheduling of debt in case of Murabahah financing with additional charge is an explicit violation of Shariah. Furthermore, to mitigate risk, banks sometimes charge a mark-up in Murabahah considering the longer period and make a commitment to allow rebate for early settlement.

Check Point

i) Proper Shariah review of all contracts and associated documents by the SSC before execution of operations;

ii) Arrangement of proper training and knowledge development programs of the operational people and ensuring internal check by the business unit during execution of the contracts;

iii) Independent review and monitoring by the compliance and risk-management unit during the execution of the contract.

iv) Through Shariah audit by the competent internal and external Shariah auditors after the execution of the contracts.

v) Shariah review by the SSC after execution of the contracts mainly based on documents and audit reports.

B. Market Risk

a. Rate of Return: In case of interbank placement, generally provisional rate is declared under Mudarabah principle however, if this rate is not adjusted based on actual performance then it will be a Shariah non-compliance risk. In case of Mudarabah/Musharakah mode, if both the parities make an undertaking to give-up there claim above the provisional amount

distributed, this may also be a Shariah concern. Furthermore, excessive use of PER and gift may lead to Shariah non-compliance risk.

Generally, banks set a provision to change the rent in the subsequent period at its exclusive discretion without getting consent of the client or allowing him to liquidation of the contract.

b. Equity Price: As a part of portfolio, banks hold equity instruments as held for trading or held to maturity approach. However, holding of an equity instrument after becoming the instrument non-qualified subsequently because of dull market situation.
c. Currency Price: Banks need trade foreign currency. To prevent the currency price risk, conventional banks use some financial derivatives like forward, future, option however, these are not Shariah permissible. If any Islamic bank engages with these instruments, it would be considered Shariah non-compliance.
d. Commodity Price: To mitigate the commodity price risk, if there is a linkage between Istisna'a with parallel Istisna'a and Salam with parallel Salam contract. Furthermore, conduct the Murabahah contract before purchasing the commodity is also prohibited.

Check Point

i) Proper Shariah review of all contracts and associated documents by the SSC before execution of operations;
ii) Arrangement of proper training and knowledge development programs of the operational people and ensuring internal check by the business unit during execution of the contracts;
iii) Independent review and monitoring by the compliance and risk-management unit during the execution of the contract.
iv) Through Shariah audit by the competent internal and external Shariah auditors after the execution of the contracts.
v) Shariah review by the SSC after execution of the contracts mainly based on documents and audit reports.

C. Operational Risk

a. People: Hiding major information from the counter party during the contract may lead to Shariah non-compliance risk. Communicating with customers with unprofessional manner may be another source of operational risk.
b. Internal Process: As per the Shariah preview, ensuring the sequence is mandatory in some contract like Murabahah. For example, conclusion of Murabahah agreement before acquiring the underlying asset is a Shariah non-compliance.
c. System: Due to lack of compatible IT infrastructure, there is a high possibility of Shariah violation. For example, charging rent automatically before ensuring usability of the leased asset or booking mark-up after disbursement of fund without ensuring Murabahah contact.
d. External Event: Shariah non-compliance may be due to external parties like false purchase of goods by the agent, creating pressure as displaced commercial risk by the investment account-holders, non-cooperation to in ensuring Shariah-compliance process, accounting engineering by the Mudarabah/Musharakah client to hide the actual performance of the business.

Check point

i) Proper recruitment, staffing, training and development under the supervision of the SSC, SMT and BoD
ii) Vetting of all internal process-flow by the SSC and continuous internal review by the auditors.
iii) Acquiring Shariah compatible Core Banking Solution by the IFI and duly vetted by the SSC.
iv) Proper screening and selection of the customers, and arranging customer awareness programs.

D. Liquidity Risk

a. Regulatory: Like conventional banks, IBs need to maintain liquidity to comply with regulatory requirements. However, it is essential to ensure Shariah compliance in meeting the regulatory requirements. For example, due to shortage of BGIS or BGIIB, no IB can invest funds for meeting SLR requirement to the conventional T-bill or T-bond. Besides, any

short-fall in the CRR, the bank will be charged Penal Interest (Bank Rate plus 5%) by the central bank.

b. Surplus Position: When an IB is in surplus liquidity position, it needs to invest the fund in the Shariah-compliant instruments like, capital market exposure, interbank placement etc. However, there is a possibility of Shariah non-compliance risk due to impermissible instrument for process fault.
c. Deficit Position: To meet up the regulatory liquidity or business requirement, an IB need to collect funds from peer banks or from the central bank, as a lender of last resort. However, this fund collection should not violate the Shariah principles.

Check Point

i) Shariah review of all intended instruments and associated documents by the SSC;
ii) Independent review and monitoring by the compliance and risk-management unit during the execution.
iii) Through Shariah audit by the competent internal and external Shariah auditors after the execution.

E. Unique Risk Factors

a. Dealing with Impermissible Goods and Services: There are some goods and services, which are permissible in trading from conventional banking point of view however, Shariah may not allow all of these like tobacco, alcohol, port, etc.
b. Financing Against Impermissible Securities: Accepting securities of impermissible assets as collateral are not permitted for Islamic financial institutions.
c. Profit Calculation, Recognition and Distribution: In case of Murabahah, profit should not be calculated based on indirect cost. At this time of execution of Instisna'a and Salam contract, profit should not be recognized. In case of HPSM, profit calculation and recognition during the construction period should be compliant with Shariah. Furthermore, profit calculation for the Mudarabah depositors should follow some Shariah principles.
d. Disclosure and Transparency and Others: Besides avoiding Riba, there are some requirements to make a contract Shariah compliant like free from Gharar, Mysir, Combination of Contract, etc.

Check point

i) Ensuring at effective and proper governance structure in place with accountability.
ii) Ensuring proper and sufficient training and development programs for the Islamic finance professionals.
iii) Ensuring an independent Shariah review and audit mechanism.
iv) Adoption of international best practices and proper implementation customized regulatory framework.

Therefore, Shariah non-compliance risk is the salient operational risk of Islamic banking operations all over the globe.

Source: *Compilation by the Authors based on the FGD and KII*

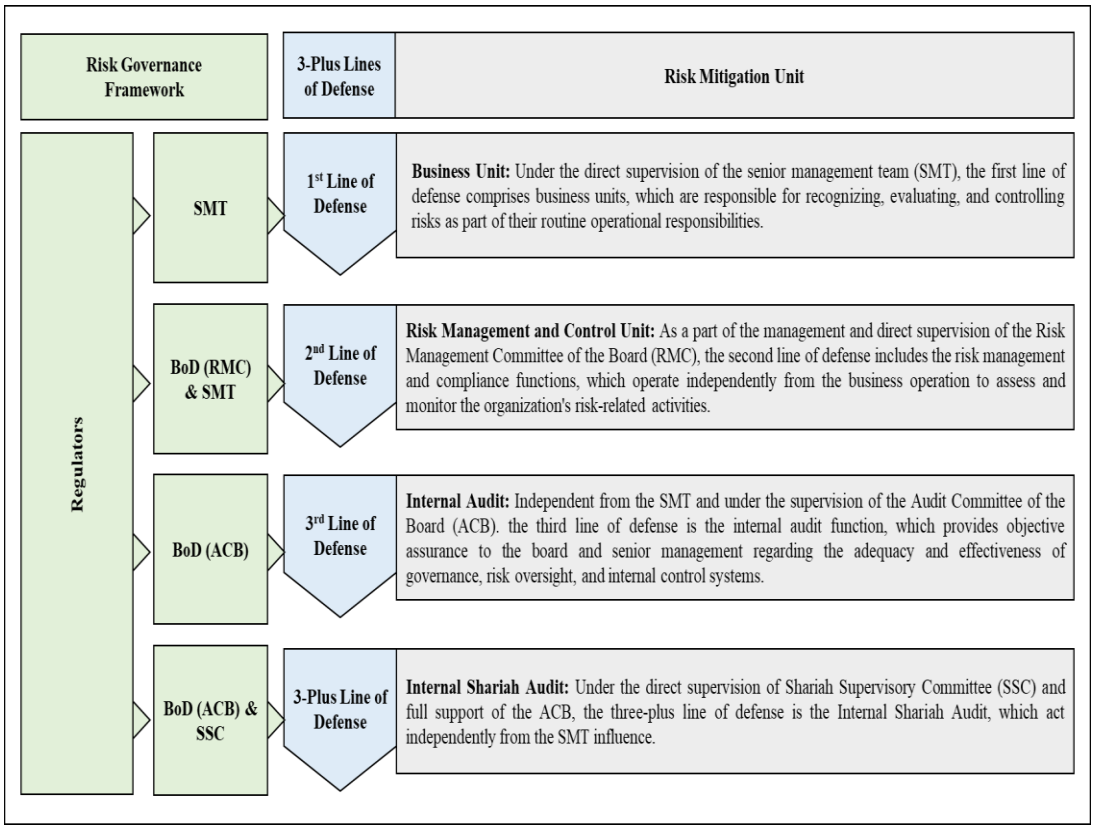
5.2.2 Operational Risk Governance Framework of Islamic Banks

The Figure 5.2 outlines how operational risk is governed in Islamic banks through a structured "3-plus lines of defense" model that incorporates both conventional risk controls and Shariah governance requirements. The first line of defense consists of business units operating under the supervision of senior management, responsible for identifying and managing risks during day-to-day activities. It is crucial to note that the operational executives must consider Shariah issues alongside business norms. The second line comprises the risk management and compliance functions, which work independently from business operations and report to the Board Risk Management Committee; their role is to oversee, guide, and monitor the bank's

overall risk profile including Shariah non-compliance risk. The third line of defense is the internal audit function, which reports directly to the Audit Committee of the Board and provides assurance on the effectiveness of internal controls, governance processes, and risk-oversight mechanisms. Internal audit should not exclude Shariah issues during the review process.

Islamic banks add an additional layer—the "plus" line of defense—through the Internal Shariah Audit, which operates independently under the direct supervision of the Shariah Supervisory Committee and with the adequate support of the Audit Committee of the Board. This function ensures that all activities, processes, and transactions adhere to Shariah rules and principles. Together, these layers create an integrated governance structure in which operational risk is controlled, monitored, and validated through multiple checkpoints, with Shariah compliance embedded as a core component of the overall risk-management framework. Regulatory grip should have over each and every stage for effective functioning. Failing this oversight role, create a mashup as observed during last few years.

Figure 5.2: Operational Risk Governance Framework of Islamic Banks



Source: *Compilation by the Authors based on the FGD and KII*

5.2.3 Control Points for Operational Risk Management of Islamic Banks

Effective management of operational risk in Islamic banks requires a coordinated focus on four core control areas: processes, people, systems, and external stakeholders.

Internal Processes

All product structures, process flows, and operational manuals must be vetted by the Shariah Supervisory Committee (SSC) before implementation and periodically reviewed to reflect evolving business practices and international standards. A robust Internal Shariah Audit (ISA) system is critical to provide independent assurance on the Shariah compliance of operations. Post-execution Shariah review by the SSC—based on audit reports, documentation reviews, and interaction with officials—ensures consistent oversight and timely correction of procedural deviations.

People

Islamic banks continue to face a shortage of qualified Islamic banking and finance (IBF) professionals relative to the size and growth of the industry. Strengthening human-capital capacity requires a multi-tiered approach: the central bank may encourage universities to offer IBF-focused academic programs; professional bodies such as Institute of Bankers, Bangladesh (IBB) may introduce specialized Islamic banking diplomas; and BIBM may expand structured training, certification, and advanced diploma programs. Recruitment policies should prioritize candidates with strong academic backgrounds and foundational IBF knowledge, supported by integrity screening, including psychological assessments where appropriate. After recruitment, structured induction programs and continuous professional development—including competency assessments—are essential for ensuring operational discipline and Shariah-sensitive decision-making.

Systems

Core banking system must be purpose-built or suitably customized to accommodate the contractual features and operational requirements of Islamic financial products. Developers should engage qualified Shariah experts during system design to ensure proper integration of Shariah requirements. Automated Shariah control checkpoints—such as blocking non-permissible transactions or preventing contract-sequence violations—are essential safeguards. Before implementation, the entire system must be reviewed and vetted by the SSC of the bank. During operations, ISA should conduct continuous Shariah-focused systems audits, and the SSC should periodically review end-to-end system processes to ensure ongoing compliance.

External Events and Stakeholder Behavior

Operational lapses often arise from customer-related factors, including insufficient understanding of Shariah requirements. Enhancing public awareness through state-level financial literacy initiatives—especially in academic curricula—would support better compliance. Industry-wide awareness programs, coordinated through collective Islamic banking forums, can expand outreach cost-effectively. Individual banks should also maintain regular customer engagement, both during business interactions and through dedicated programs, strengthening client understanding and reducing behavior-driven Shariah risks.

Box 5.2: Summary of Control Points for Operational Risk Management of Islamic Banks

A. People

- **Availability:** It is opined that there is dearth of competent IBF professionals considering existing IBF market size and its potential growth.
  - BB may take initiatives to motivate the concerned authorities to introduce Islamic banking and finance related degree and courses.
  - Institute of Bankers, Bangladesh (IBB) may take initiatives to introduce specialized Islamic banking diploma.
  - BIBM may introduce different programs on Islamic banking and finance in different levels. For example, regular training programs, certification programs for specialized areas and advanced level diploma/post graduate diploma.
- **Recruitment:** A candidate having academic excellency along with Islamic banking and finance knowledge should get priority in selecting the bankers. The selection criteria should be designed accordingly.
- **Honesty:** Banking is a very sensitive profession where an official may be deviated easily during dealing with finance. Therefore, banks may consider to introduce psychological test for assessing the moralities ethical standard. Reward and punishment system through proper key performance indicators.
- **Development Program:** After joining of new officials, a comprehensive training may be imparted before assigning the desk in the banking operations. Besides, continuous development program targeting different levels of executes and department, competency test may be introduced.

B. Internal Process

- **Shariah Vetting**: All of the product program guidelines and banking process flow should be properly vetted by the Shariah Supervisory Committee (SSC) before implementation. More on the that, all of these documents must be reviewed at a certain interval to accommodate changing business environment, updated knowledge, international standards and best practices.
- **Shariah Audit:** As a third eye of different stakeholders, internal Shariah audit (ISA) plays an important role by providing assurance service about Shariah compliance. Therefore, an effective and efficient ISA mechanism need to have in place.
- **Shariah Review:** After execution of the operations, the SSC will review through two ways – evaluating the report of ISA and separate review directly based on documents and interaction the bank-officials.

C. System

- **Compatible System:** It is expected that an Islamic banking software should be specially designed considering the salient features and activities. If it is not properly developed, there is risk of Shariah non-compliance. The system developer should engage competent Shariah scholars during the development process of the core banking solution.

- **Shariah Control Check Points:** To minimize the Shariah non-compliance risk, core banking system should incorporate some check points, which may automatically prevent the non-compliant transactions.
- **Shariah Vetting:** Before introducing a core banking solution, it should be thoroughly reviewed and vetted by the SSC. Without ensuring this, regulator may not allow to launch banking operations.
- **Shariah Audit:** As an independent organ, internal Shariah audit (ISA) should review end-to-end the core banking system from the Shariah lens during operations. Any deviation or deem to be non-compliant should bring to the notice of the SSC and other governance organ. It should be a continuous process in an Islamic financial institution.
- **Shariah Review:** At a certain interval, the SSC may be engaged to review the end-to-end process executed through core banking system.

D. External Event

- **State-Level Awareness Program:** It is generally opined that Shariah compliance is not possible without proper cooperation from the customers. Because of poor understanding and business priority, Islamic banking customers do not act accordingly in some cases. Therefore, it is important to improve financial literacy and especially Islamic modalities. It would be holistic, if state-level initiatives are taken like inclusion of Islamic banking and finance related courses in the relevant academic curricular.
- **Collective Program by Islamic Banking Industry:** In the second layer, Islamic banking sector may conduct national-wide awareness program through their collective forum. It will be affordable to increase coverage with a minimum cost.
- **Initiatives of Individual Banks:** Individual banks should also take some initiatives to share views with their customers. These may be materialized in two approaches - interaction during banking operations; and through separate customized program. This type of initiatives may also act as a market tools to reach the potential customers.

Source: *Compilation by the Authors based on the FGD and KII*

5.2.4 Internal Shariah Audit (ISA) and Shariah Supervisory Committee (SSC)

Effectiveness of Internal Shariah Audit (ISA)

The effectiveness of ISA depends on the breadth, depth, and independence of its oversight functions. *First*, audit coverage must move beyond selective sampling to population-based reviews, ensuring that all transactions and processes are examined from a Shariah perspective. *Second*, ISA should adopt a system-based approach capable of real-time detection, rectification, and prevention of Shariah breaches. *Third*, the structure of the ISA unit should mirror the Internal Control and Compliance Department (ICCD), incorporating:

- **On-site audits** conducted by competent *Muraqibs* with full operational independence;
- **Off-site surveillance**, supported by documentation reviews and ICT-enabled monitoring; and
- **Continuous follow-up and reporting** to ensure timely correction and escalation of issues.

Forth, auditor competency is central to ISA effectiveness; *Muraqibs* must possess sound Shariah knowledge, banking expertise, and audit skills. *Fifth*, however, concerns remain regarding the actual independence of ISA. Despite theoretical

independence, ISA sometimes face pressure, including reassignment or termination, which discourages objective reporting. *Sixth*, over time, this may lead to self-censorship, reducing the effectiveness of the Shariah audit function and increasing the risk of undetected non-compliance.

Activeness of the Shariah Supervisory Committee (SSC)

The SSC's activeness is a critical determinant of Shariah governance quality. An SSC should not be re-active only rather it may play pro-active role to create Shariah-compliant environment. An effective SSC requires proper composition, ensuring that members possess the necessary Shariah expertise alongside Islamic finance and banking knowledge. A well-defined Terms of Reference (ToR) is essential to outline responsibilities, authority, and reporting lines. Continuous professional development (CPD) should be provided to SSC members to keep them updated with evolving standards, regulatory requirements, and best practices. Furthermore, SSC representation in meetings of the Board of Directors and its committees is important to keep members informed about operational realities and to prevent Shariah issues at the policy level.

Strong institutional support, particularly from the Board of Directors and its Audit Committee, is indispensable to enable both ISA and SSC to perform their roles independently and effectively.

5.2.5 Regulatory Framework Addressing Operational Risk of Islamic Banks

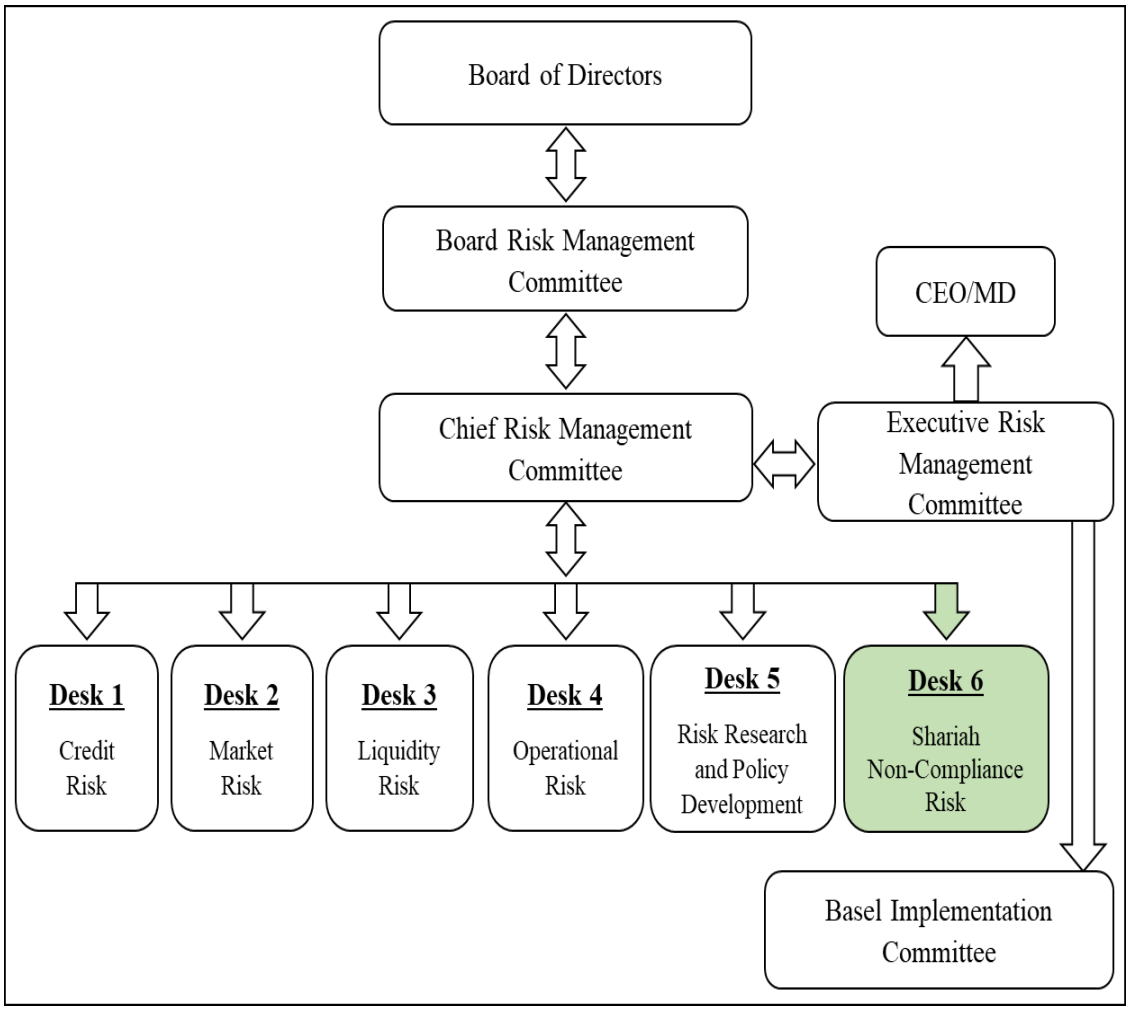
The regulatory environment governing operational risk in Islamic banks comprises global standards and domestic requirements, with Shariah non-compliance risk (SNCR) forming a distinct and critical component. Under the IFSB framework, Islamic banks are required to recognize SNCR within their capital adequacy calculations, reflecting the severe financial, legal, and reputational consequences arising from Shariah breaches. In contrast, the Basel framework omits Shariah-related exposures, which creates a structural gap for Islamic banks operating under Basel-driven capital standards. Consequently, Bangladesh Bank will need to progressively align market practices with IFSB requirements in addition to Basel norms to ensure an accurate representation of risk in Islamic financial institutions.

Bangladesh Bank may further strengthen supervisory oversight by extending the CAMELS rating to CAMELSS (additional 'S' for Shariah compliance), integrating Shariah governance into the rating system for Islamic banks. The Internal Control and Compliance Guideline (2016) already includes a dedicated chapter on internal Shariah audit, yet the current "Shariah Non-Compliance Risk Rating" template remains outdated. It requires comprehensive revision to capture risks arising from new business models, digitized delivery channels, technology-enabled operations, and

evolving sources of SNCR. Robust Shariah-aligned policies and procedures across all functions therefore remain fundamental.

In accordance with the "Risk Management Guidelines for Banks" (DOS Circular No. 04, October 08, 2018), banks must maintain an optimal risk management organogram consisting of five core desks: Credit Risk, Market Risk, Liquidity Risk, Operational Risk, and Risk Research & Policy Development. For Islamic banks and finance companies, an additional Shariah Non-Compliance Risk Desk is indispensable, as depicted in Figure 5.3, to ensure focused monitoring, reporting, and mitigation of SNCR across business lines. Furthermore, all guidelines, circulars, and directives applicable to both conventional and Islamic banking should undergo Shariah review before issuance to avoid inadvertent inconsistencies or non-compliant instructions.

Figure 5.3: Optimal Risk Management Organogram



Source: *Compilation by the Authors based on the FGD and KII*

5.2.6 Other Issues of Operational Risk of Islamic Banks

Operational risk in IBs extends beyond standard process failures and includes several institution-specific vulnerabilities arising from Shariah governance, these dimensions require careful attention to prevent SNCR and ensure operational integrity across all business lines.

Product Design and Shariah Validation

All products of an IB, whether deposit, financing, international trade, treasury, or offshore banking, must undergo comprehensive Shariah review prior to approval and rollout. This review should validate the contractual structure, underlying covenants, sequence of transactions, documentation design, customer obligations, and exit mechanisms. Any oversight at the design stage may embed structural flaws that later cause violations during execution.

Product Implementation Risks

Even when a product is designed correctly, improper implementation at the branch or operational level can trigger SNCR. Inadequate staff training, weak supervision, and inconsistent compliance checks may result in deviations from approved processes. Operational personnel must therefore possess relevant knowledge, product-specific Shariah conditions, and documentation protocols, supported by continuous supervision and periodic on-site reviews.

System Implementation and Automation Gaps

A well-designed and correctly executed product may still become non-compliant if the core banking system fails to reflect its Shariah features accurately. Errors in system configuration, automated charge generation, or workflow sequencing often necessitate manual overrides to restore compliance. Common examples include automated fixed rebates in early settlement of Murabahah receivable or automatic imposition of compensation charges on defaulting clients—both of which may violate Shariah requirements if not aligned with approved policies. System audits, user acceptance testing, and Shariah-compliant parameter settings must therefore be mandatory before deployment.

Board Composition and Accountability for SNCR

The Board of Directors must include members with adequate banking and Islamic finance exposure to provide informed oversight. The Board holds ultimate accountability for Shariah non-compliance and should ensure that policies, risk frameworks, and product strategies remain fully aligned with Shariah principles. Besides, different Shariah governance organs, e.g., ISA, SSC, may not work properly without adequate support of the Board. Failure at the Board level amplifies systemic risk and undermines stakeholder confidence.

Strengthening Oversight Committees

The Audit Committee of the Board (ACB) should engage regularly with the Internal Shariah Audit (ISA) function in the same manner it interacts with internal audit. Including members with Shariah banking background in the ACB enhances the quality of discussions, interpretation of findings, and follow-up actions. Similarly, the Board Risk Management Committee (BRMC) should include at least one member with demonstrated Islamic banking expertise, ensuring that SNCR receives proportionate attention within the bank's overall risk governance structure.

Shariah Competence of MD/CEO

The Managing Director/CEO must possess proven orientation in Islamic banking and finance before appointment. In addition, they should remain engaged in ongoing professional development programs to stay updated on evolving Shariah standards, regulatory guidelines, and international best practices. The tone from the top has a direct impact on compliance culture, it is not exception for SNCR management process.

Dedicated Shariah Inspection by Bangladesh Bank

Bangladesh Bank should institutionalize a dedicated function for Shariah inspection—similar to other risk-based inspection—under a specialized department. This will allow focused review of Shariah governance, product structures, system configurations, and branch-level implementation. Moreover, including at least one Shariah expert in each inspection team will significantly enhance the accuracy and relevance of supervisory assessments.

Inclusion of Shariah Expert in Internal Audit Team

Several banks already integrate IT specialists into internal audit teams to strengthen technology-related reviews alongside business audits. Following the same principle, every bank-level internal audit team should include a qualified Shariah expert to ensure that audit examinations adequately capture Shariah-related risks, validate product execution, and identify deviations from approved structures. Embedding Shariah expertise within internal audit functions enhances the robustness, accuracy, and credibility of the overall assurance process for Islamic banking operations.

Rationalizing Business Targets and Incentives

Unrealistic business targets may lead employees to deviate from Shariah requirements in product execution or documentation. Rationalizing targets and linking performance incentives to both growth and compliance indicators will mitigate the pressure-induced operational risks unique to Islamic financial institutions. Extent of Shariah violation disincentivizes an employee even achievement of all business targets. On the other hand, minimizing SNCR should incentivizes an employee.

Shariah-Compliant Investment Administration

The investment administration function must strictly adhere to Shariah requirements in documentation, asset verification, payment flows, collateral management, and post-disbursement monitoring. Weaknesses in execution may convert a Shariah-compliant financing structure into a non-compliant transaction, thereby exposing the bank to financial loss and reputational risk.

Enforcement of Job Rotation and Mandatory Leave

Proper implementation of job rotation and mandatory leave policies helps detect irregularities, prevent collusion, and strengthen internal controls. These measures are particularly important in Shariah-sensitive functions such as investment administration, trade operations, and treasury.

Chapter 6: Issues and Recommendations

Operational risk in Islamic banks reflects a combination of conventional operational vulnerabilities and Shariah-specific exposures arising from unique product structures, governance modalities, and compliance requirements. The findings of the survey, FGD, KII, case studies, and regulatory analysis collectively demonstrate that the majority of operational lapses originate from three root causes: (i) weak understanding and insufficient attention to ORM, (ii) inadequate Shariah governance and monitoring discipline, and (iii) systemic deficiencies across people, processes, systems, and oversight structures. Addressing these issues requires a comprehensive, institution-wide strengthening of governance, capability, regulatory alignment, and accountability mechanisms.

6.1 Understanding Level of and Attention to ORM

Most Islamic banks demonstrate limited institutional understanding of ORM. ORM remains compliance-driven rather than embedded into strategic decision-making. ORM units are often under-resourced, positioned too low in the hierarchy, or fragmented within risk or audit functions. Boards and senior management frequently provide inadequate oversight, resulting in reactive management rather than anticipatory risk control.

Recommendations

- Institutionalize ORM as a **strategic function**, requiring Board-level review of ORM reports and ensuring ORM independence under the CRO.
- Mandate an **institution-wide ORM framework** aligned with Basel III and IFSB-23.
- Enhance staff competency through **structured, mandatory ORM certification programs** for all officers involved in operations, trade finance, investment, treasury, and IT.
- Introduce **ORM dashboards**, Key Risk Indicators (KRIs), and loss-event databases to promote real-time awareness.

6.2 Shariah Non-Compliance Risk as Integral Part of Risk Management Process

Shariah non-compliance remains the most salient operational risk in Islamic banks. SNCR emerges from documentation errors, incorrect contract sequencing, weak supervision, system misconfiguration, and inadequate product knowledge. In most banks, SNCR is not fully integrated into ORM and remains compartmentalized within Shariah functions.

Recommendations

- Recognize SNCR as a **distinct but integral component of ORM**, with a dedicated desk under the CRO.

- Embed Shariah compliance checkpoints in **all stages of operations**—design, execution, system configuration, audit, and reporting.
- Mandate **SSC vetting of every product program guideline, SOP, process flow, and core banking system module** prior to implementation.

6.3 Proper Selection in Entry Level Officials and Development Subsequently

The shortage of qualified IBF professionals contributes significantly to operational failures. Recruitment processes often do not prioritize Islamic finance knowledge, ethical standards, or risk awareness. Training remains irregular, unspecialized, or insufficient against the growing complexity of Islamic products.

Recommendations

- Revise recruitment frameworks so that **candidates with strong academic profiles, IBF knowledge, and ethical screening** receive priority.
- Introduce **psychometric and integrity assessments** for entry-level recruits and sensitive operational roles.
- Institutionalize comprehensive **induction programs**, continuous CPD, competency tests, and structured learning pathways (CIBFP, CSAA, CIPA, etc.).
- Require banks to adopt **succession planning and rotation policies** for sensitive roles to reduce collusion and behavioral risks.

6.4 Introduction of External Shariah Review and Fiduciary Rating

Current assurance mechanisms rely solely on internal controls and the SSC, lacking external validation. Absence of external Shariah review reduces transparency, comparability, and stakeholder confidence. Similarly, fiduciary risks to investment account holders remain inadequately assessed.

Recommendations

- Introduce an **External Shariah Review Framework**, administered by an authorized independent agency.
- Mandate **annual Shariah assurance reports** audited by external Shariah reviewers.
- Develop a **Fiduciary Rating Framework** to assess how Islamic banks protect the interests of Mudarabah depositors or unrestricted investment account holders.
- Align the framework with AAOIFI-ASIFI 6, AAOIFI-GS 10, IFSB-1, IFSB-30, and international best practices.

6.5 Regulatory Initiatives and Updating Regulations

Regulatory frameworks remain partially aligned with IFSB and AAOIFI requirements and do not adequately reflect Shariah-governance needs in a digitized environment. There is no standalone Shariah inspection wing within Bangladesh Bank, and existing risk templates and guidelines are outdated.

Recommendations

- Establish a **Shariah Inspection Wing** at Bangladesh Bank staffed with qualified Shariah scholars and banking experts.
- Revise and modernize Shariah-related regulatory guidelines, particularly the SNCR rating system, internal Shariah audit chapter, and product governance requirements.
- A sperate guidelines on internal Shariah audit may be issued by BB in line with AAOIFI-GS 11. BB may consider to update the "Shariah Non-Compliance Risk Rating" template to reflect digital operations, new products, and emerging delivery channels.
- Require all circulars and guidelines applicable to Islamic banks to undergo **mandatory Shariah review** before issuance.

6.6 Shariah-Based KPI of Banks and Employees

Performance evaluation frameworks largely prioritize volume-driven growth, leading to excessive pressure, cutting procedural corners, and triggering SNCR. There is no standardized Shariah-based KPI mechanism across banks.

Recommendations

- Integrate Shariah-based KPIs into the **CAMELSS rating framework** (CAMELS + Shariah) for institutions.
- Establish regulatory penalties for banks that repeatedly violate Shariah rules or fail Shariah audits.
- For employees, develop **dual KPIs**: (i) business performance; (ii) Shariah compliance score, including adherence to processes, audit findings, and SNCR incidents.
- Introduce a **balanced scorecard** enforcing penalties for Shariah violations, process breaches, data manipulation, and unethical behavior. Apply negative scoring for **any Shariah breach**, irrespective of business achievements.
- Link promotions, incentives, and branch ratings to Shariah-compliance performance. Reward branches and officials demonstrating **zero SNCR, high audit scores, and exemplary compliance culture**.
- Implement a **whistleblower protection mechanism** to strengthen integrity.

6.7 Massive Shariah Awareness Programs

Customer behavior, lack of literacy in Islamic contracts, and weak understanding of Shariah guidelines contribute directly to operational lapses. Industry-wide awareness remains minimal.

Recommendations

- Introduce Islamic finance concepts into **national curricula** in universities and technical institutions.
- Conduct industry-wide awareness campaigns through **collective Islamic banking forums**, reducing cost and expanding coverage.
- Banks should run **ongoing customer sessions** during onboarding and product execution to mitigate behavioral risks.
- Develop digital content (videos, mobile alerts, FAQs) to communicate Shariah conditions in simple language.

6.8 Independency of ISA and Pro-activeness of SSC

Internal Shariah Audit (ISA) often lacks operational independence and institutional authority. SSC engagement remains uneven, sometimes reactive instead of proactive. In some banks, SSC and ISA face internal resistance and management influence.

Recommendations

- Ensure ISA's **functional independence**, reporting jointly to the SSC and the Audit Committee of the Board.
- Expand ISA coverage towards **population-based audits** and automated Shariah auditing using system logs.
- Ensure SSC involvement in **policy formulation, system vetting, product approval, and post-execution reviews**.
- Provide SSC members with **capacity-building and CPD programs** to keep them updated with evolving global standards.
- Require SSC participation in Board Risk Management Committee (BRMC) meetings to influence policy-level decisions.

Islamic banks in Bangladesh must shift from a compliance-driven, fragmented approach to an institution-wide, data-driven, Shariah-embedded operational risk framework. Addressing the identified issues requires strengthened governance structures, enhanced human capacity, modernized systems, updated regulations, and a culture of ethical and Shariah-conscious banking. Adoption of the recommended reforms will enable Islamic banks to improve operational resilience, protect depositors' interests, and uphold the Shariah integrity that defines their mandate.

References

Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI). (2019). *AAOIFI Governance Standard 11: Internal Shari'ah Audit*, Available at https://aaoifi.com/issued-standards-2/?lang=en.

Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI). (2021). *Auditing Standard for Islamic Financial Institutions No. 6: External Shariah Audit*, Available at https://aaoifi.com/issued-standards-5/?lang=en.

Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI). (2024). *AAOIFI Governance Standard 1: Shariah Governance Framework*, Available at https://aaoifi.com/issued-standards-2/?lang=en.

Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI). (2024). *AAOIFI Governance Standard 19: Shari'ah Supervisory Board_Appointment and Composition*, Available at https://aaoifi.com/issued-standards-2/?lang=en.

Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI). (2024). *AAOIFI Governance Standard 20: Shari'ah Supervisory Board_Functions and Operations*, Available at https://aaoifi.com/issued-standards-2/?lang=en.

Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI). (2024). *AAOIFI Governance Standard 21: SSB Review and Report*, Available at https://aaoifi.com/issued-standards-2/?lang=en.

Ahmed, H. (2009). Financial crisis: Risks and lessons for Islamic Finance. ISRA International Journal of Islamic Finance, 1(1), 7–32. https://doi.org/10.55188/ijif.v1i1.69

Al-Musheifri, Z. J. (2021). An investigation on Sharia governance in Islamic banking A case of Islamic banks in Oman. Advances in Social Sciences Research Journal, 8(7), 330–340. https://doi.org/10.14738/assrj.87.10483

Ayub, M. (2007). *Understanding Islamic Finance*. John Wiley & Sons. Basel Committee on Banking Supervision (BCBS). (2011). *Principles for the Sound Management of Operational Risk.* Bank for International Settlements.

Bank Negara Malaysia (BNM). (2019). *Shariah Governance Policy Document.*

Basel Committee on Banking Supervision (BCBS). (2011). *Principles for the Sound Management of Operational Risk*. Bank for International Settlements. https://www.bis.org/publ/bcbs195.pdf

Chapra, M. U. (2008). *The Global Financial Crisis: Can Islamic Finance Help?* Islamic Development Bank.

Cornwell, N., Bilson, C., Gepp, A., Stern, S., & Vanstone, B. J. (2023). Modernising operational risk management in financial institutions via data-driven causal factors analysis: A pre-registered study. Pacific-Basin Finance Journal, 79, 102011. https://doi.org/10.1016/j.pacfin.2023.102011

Dusuki, A. W., & Abozaid, A. (2007). *A Critical Appraisal of the Challenges of Realizing Maqasid Al-Shari'ah in Islamic Banking and Finance.* IIUM Journal of Economics and Management.

Federal Deposit Insurance Corporation (FDIC). (2023). *Operational Risk Management: An Evolving Discipline*. https://www.fdic.gov/bank-examinations/operational-risk-management-evolving-discipline

Ferreira, S., Nunes, A., & Pereira, J. (2019). A conceptual model of operational risk events in financial institutions. *International Journal of Finance and Economics*, 24(2), 321–334.

Grais, W., & Pellegrini, M. (2006). Corporate Governance in institutions offering Islamic Financial Services: Issues and options. In World Bank, Washington, DC eBooks. https://doi.org/10.1596/1813-9450-4052

Habib, S.M.A., Ahmed, M.N., Hossain, M.M., Yesmin, R., and Arefin, M.E. (2025). "Governance and Practices of Operational Risk Management in Banks", *Banking Research Series 2025*, Issue 01, pp. 1-58, workshop held on May 15, 2025 at BIBM, Dhaka.

Hasan, Z. (2011). *A Survey on Shariah Governance Practices in Malaysia, GCC Countries and the UK.* International Journal of Islamic and Middle Eastern Finance and Management.

Hassan, R. (2016). SHARIAH NON-COMPLIANCE RISK AND ITS EFFECTS ON ISLAMIC FINANCIAL INSTITUTIONS. Scientific Repository (Petra Christian University), 21(3). http://irep.iium.edu.my/56556/13/56556_Shariah%20non compliance%20risk_scopus.pdfArcher, S., & Karim, R. A. A. (2009). *Islamic finance: The regulatory challenge*. John Wiley & Sons.

Islamic Financial Services Board (IFSB). (2005). *Guiding Principles of Risk Management for Institutions Offering Islamic Financial Services (IFSB-1)*. Islamic Financial Services Board. https://www.ifsb.org/

Islamic Financial Services Board (IFSB). (2021). *Revised Capital Adequacy Standard for Institutions Offering Islamic Financial Services [Banking Segment], (IFSB-23)*. Islamic Financial Services Board. https://www.ifsb.org/

Islamic Financial Services Board (IFSB). (2023). *Revised Guiding Principles on Corporate Governance for Institutions Offering Islamic Financial Services (Banking Segment) (IFSB-30)*. Islamic Financial Services Board. https://www.ifsb.org/

Iqbal, Z., & Mirakhor, A. (2011). *An Introduction to Islamic Finance: Theory and Practice.* John Wiley & Sons.

Jadwani, B., Parkhi, S., & Mitra, P. K. (2024). Operational Risk Management in Banks: a bibliometric analysis and opportunities for Future research. Journal of Risk and Financial Management, 17(3), 95. https://doi.org/10.3390/jrfm17030095

Jayahama, R. (2005). *Basel II and operational risk* (Speech). Bank for International Settlements. https://www.bis.org/review/r051222g.pdf Bank for International Settlements

KPMG. (2022). *Operational risk in the new Basel framework*. https://assets.kpmg.com/content/dam/kpmg/ae/pdf/2022/04/operational-risk-in-the-new-basel-framework.pdf KPMG Assets

Makiyan, S. (2009). Risk management and challenges in Islamic Banks. https://www.semanticscholar.org/paper/Risk-Management-and-Challenges-in-Islamic-Banks-Makiyan/d05782b6d46d81aa1876585101c8671ab1149a87

Masood, O., & Javaria, K. (2018). *Risk management implementation and solutions for Islamic banking and finance*. Cambridge Scholars Publishing.

Pakhchanyan, S. (2016). Operational Risk Management in Financial Institutions: A Literature review. International Journal of Financial Studies, 4(4), 20. https://doi.org/10.3390/ijfs4040020

Reyazat, F. (2012). "Risk Management Framework in Islamic Banking: Basel II and III, Challenges and Implications in Islamic Banking", *Money and Economy*, Vol. 6, No. 2.

Shakhatreh, M. Z., Biancone, P. P., & Radwan, M. (2016). *Operational Risk Management Disclosure in Islamic Banks*. (Paper on operational risk in Islamic institutions)

Sundararajan, V., & Errico, L. (2002). *Islamic Financial Institutions and Products in the Global Financial System: Key Issues in Risk Management and Challenges Ahead.* IMF.

Appendix I: Industry Survey on Operational Risk Management in Banks

Governance Structure of Operational Risk Management in Banks	
Particulars	**Industry Survey (Opinion)**
Standalone ORM Unit function under RMD	30% [10%-40%]
Integrated with enterprise risk management	24% [5%-75%]
Decentralized across business units	35.5% [5%-50%]
No formal ORM governance framework	25.5% [5%-70%]
Board and Senior Management Oversight on ORM Practices in Banks	
Particulars	**Industry Survey (Opinion)**
Regular review at Board Risk Committee	30% [5%-70%]
Quarterly reporting to senior management only	33% [10%-50%]
Periodic updates	38.5% [10%-75%]
Not Applicable	20.5% [0%-70%]
Implementation of Three Lines of Defence Model in Banks	
Particulars	**Industry Survey (Opinion)**
Fully implemented and effective across all units	17% [5%-30%]
Partially implemented	31% [5%-80%]
Informally implemented without clear definition	34.5% [10%-65%]
Not implemented	17.5% [0%-80%]
Primary Tools and Methods Used to Identify Operational Risks in Banks	
Particulars	**Industry Survey (Opinion)**
Risk Control by the Business Unit	27% [10%-70%]
Internal audit findings	60% [15%-100%]
Incident/loss event reviews	16% [5%-50%]
Key risk indicators (KRIs)	22% [5%-50%]
Banks ORM Aligned with Regulatory Frameworks	
Particulars	**Industry Survey (Opinion)**
Fully aligned with Basel	40% [10%-70%]
Aligned with Domestic Regulation	50% [15%-100%]
Limited Alignment	30.5% [5%-50%]
Not Aligned	2.5% [5%-50%]
Internal Loss Event/Incident Data Collected and Managed in Banks	
Particulars	**Industry Survey (Opinion)**
Centralized database/system with regular updates	20% [10%-40%]
Departmental logs consolidated periodically	30% [5%-60%]
Manual tracking and adhoc updates	25% [10%-50%]
Loss data is not formally maintained	25% [10%-75%]
Conducting Scenario Analyses in Banks	
Particulars	**Industry Survey (Opinion)**
Yes, in all business lines	23% [5%-90%]
Yes, only in selected high-risk areas	22% [5%-50%]
Occasionally, as part of internal control	37% [10%-70%]
Not conducted	18% [0%-60%]
Challenges of Conducting Scenario Analyses in Banks	
Particulars	**Industry Survey (Opinion)**
Lack of expert input or engagement	28.5% [10%-70%]
Limited historical data	37% [20%-60%]
Lack of standardized methodology	39% [20%-70%]
Not prioritized due to resource constraints	22.5% [5%-80%]

Monitoring Operational Risk Across Department/Branches in Banks	
Particulars	**Industry Survey (Opinion)**
Standardized dashboards and KRIs	28% [10%-60%]
Internal audit and compliance oversight	57% [40%-80%]
Business units manage independently	17.5% [20%-50%]
No structured monitoring	15.5% [10%-50%]
Key KRIs used in Banks	
Particulars	**Industry Survey (Opinion)**
Number of fraud incidents	40% [5%-90%]
System downtime/IT failures	27% [10%-70%]
Staff turnover rate	30% [10%-60%]
Customer complaints	25% [10%-60%]
Unauthorized transactions	23% [10%-70%]
Loss event frequency	15% [5%-40%]
Negative media reports	2%
More criteria are considered	2%
Frequency of ORM Reporting to Senior Management/Board in Banks	
Particulars	**Industry Survey (Opinion)**
Monthly	35% [10%-90%]
Quarterly	42% [10%-80%]
Semi-annually	15.5% [10%-40%]
As & when required	7.5% [5%-20%]
Managing Operational Risk of Outsourcing	
Particulars	**Industry Survey (Opinion)**
Vendor risk assessment and monitoring in place	35% [10%-90%]
Included in ORM assessments occasionally	22% [5%-40%]
Not consistently addressed	23.5% [5%-70%]
No framework exists	29.5% [0%-50%]
Management of Cybersecurity Risk	
Particulars	**Industry Survey (Opinion)**
IT and Information Security Team	70% [20%-100%]
Operational Risk Management Unit	15% [5%-30%]
Internal Audit	12% [5%-25%]
All of the above	3% [0%-10%]
Building ORM Culture and Awareness in Banks	
Particulars	**Industry Survey (Opinion)**
Regular training and communication campaigns	60% [20%-100%]
Risk culture assessments	20% [10%-40%]
Staff incentives linked to risk performance	15% [5%-20%]
None of the above	5% [10%-40%]
Assessment of Training Effectiveness	
Particulars	**Industry Survey (Opinion)**
Post-training assessments and surveys	50% [10%-80%]
Monitoring performance/KRIs post-training	20% [0%-50%]
No formal assessment conducted	17.5% [0%-80%]
Feedback from supervisors only	12.5% [10%-50%]

Source: Habib et al. (2025)

Appendix II: Case Study Collected from BIBM Study

General Case of Operational Risk of Banks-1: Crisis of High NPL in Bangladesh

The banking sector is severely affected by an unparalleled crisis of NPLs, where wilful defaulters play a central role in the sectoral deterioration. Back in 2009, NPLs stood at Tk 224.82 billion. By September 2024, this figure rises steeply to Tk 2.84 trillion, excluding Tk 640 billion in written-off loans. The NPL ratio surged from 9.93% in September 2023 to 16.93% by September 2024. By December 2024, classified loans exceeded Tk 3.45 trillion (20.2% of total loans). As per the BB forecasts, NPLs may exceed 30% by June 2025 due to systemic weaknesses, regulatory gaps, and exploitative practices. As per the white paper released in December 2024, distressed assets (including NPLs, rescheduled, restructured, written-off, and litigated loans) crossed Tk 6.75 lakh crore by FY 2023-24. The consequences are severe due to a majority of large defaulters are politically connected business conglomerates. Top defaulters of the country are some business houses that have executed the crime in connivance with a section of bank executives and external powerful quarters. Additionally, sponsor-directors of banks often take loans anonymously through mutual agreements and don't repay them, then approve dividends benefiting themselves despite poor bank health. Basically, these are innovative irregularities to siphon off the money in the name of loan which matches with the definition of operational risk. These circumstances impede the stability of the entire financial system and demand urgent attention to governance reforms, stricter regulations, and cultural shifts in borrower accountability. This high NPL is the reflection of extremely high Operational Risk (not credit risk) in the banking industry of Bangladesh that reflects process failure, internal and external financial crime.[1]

General Case of Operational Risk of Banks-2: Gross Manipulation in Some Shari'ah Based Banks

ABC Shari'ah Bank PLC, once one of the most reliable customers and profitable Islamic banks in Bangladesh, encountered a sharp decline in performance due to a complete breakdown of operational risk management (ORM). Between 2017 and 2024, the bank's non-performing investment (NPI) ratio soared from 4 percent to over 40 percent. Once compliant with regulatory capital and liquidity requirements, the bank is now facing a capital deficit and severe liquidity crisis. This rapid deterioration is rooted in a fundamental failure of governance - where committed and competent board members were abruptly replaced by politically influenced and unethical appointees. Senior management was similarly overhauled, removing experienced leaders and installing individuals lacking expertise and accountability

In parallel, the bank's historically disciplined human resource practices collapsed. A bulk number of new recruits were appointed without proper screening, and staff development initiatives were discontinued. Critical operational processes, especially in credit and treasury, were bypassed or ignored, giving rise to unchecked exceptions and widespread corruption. Meanwhile, core banking systems were manipulated from the head office level-branch operations were restricted, data integrity was compromised, and frequent misreporting affected both internal communication and external disclosures. The situation worsened due to undue external interference in daily operations, which eroded institutional autonomy and encouraged unethical practices. Overall, this case highlights a gross failure across all key dimensions of ORM-governance, people, process, system,

[1] financialexpress.com.bd/ (Mar 03, 2025); (07 April, 2025) https://www.tbsnews.net/economy/banking/banks-npls-over-10-face-dividend-ban-2025-1091851 (17 March, 2025)

and external environment-serving as a cautionary example of how institutional breakdown can occur when operational risks are neither identified nor mitigated systematically.
Note: Based on Interview

General Case of Operational Risk of Banks-3: Big Scams and Operational Risks in Banking

The Hallmark Group committed one of the biggest financial scams in Bangladesh. The organization skimmed money of around 3600 crore taka over a number of years while presenting fraudulent company transactions using faked documents and letters of credit. Investigations disclosed that the bank's approval processes were highly corrupt, and several officials were engaged in the plan. (Source: The Daily Star)

The Bismillah Group scammed around 1200 crore taka using fake export documents. The group created shell companies to show fictitious international trade deals and to secure large loans. Bank officials were involved in approving these transactions without proper verification. A major vulnerability in Bangladesh's trade financing sector was unveiled through this scam. (Source: Prothom Alo)

Destiny Group operated one of Bangladesh's largest fictitious schemes. The company used a multi-level marketing policy to recruit new investors whose money was used to pay earlier participants. Later, it was found that none of the promised projects were operational, with funds being diverted to personal accounts. Around 4000 crore taka was siphoned off through this scam. (Source: Dhaka Tribune)

Mr. X was involved the systematic looting of ABC Leasing and several other financial institutions. He created a complex network of fake companies to get loans that were never repaid and approximately 3,634 crore taka was transferred from various banks, financial institutions and the capital market to Canada and India. (Source: The Business Standard)

The chairman and other directors of the ABC Bank approved loans to shell companies without proper collateral. Audits revealed serious irregularities in loan documentation and approval processes. The scandal forced Bangladesh Bank to intervene with a bailout package of around 4000 crore taka to save the bank from complete failure. (The Financial Express)

The XYZ Bank approved thousands of questionable loans without proper documentation. Investigators found that most borrower companies either didn't exist or were not operational. Despite clear evidence of a major scam, the politically exposed people involved were able to withdraw around BDT 4,500 crore. (Source: New Age)

The Crescent Group took large loans to develop state-owned jute mills, but instead diverted the funds for other purposes. Investigations revealed the mills never became operational despite receiving large financing. The group used complex financial maneuvers to hide the misappropriation of funds over several years and in this process, BDT 2,000 crore was siphoned off from the market. (Source: The Independent)

Evaly took advance payments for products it never delivered, using new customer deposits to pay earlier buyers. The scandal affected thousands of customers and merchants and around 1000 crore taka was scammed by Evaly. Later, It prompted new regulations for e-commerce businesses in the country. Source: Bangla Tribune)

General Case of Operational Risk of Banks-4: Illicit Outflows using Trade is a Huge Risk

Trade-Based Money Laundering (TBML) poses a significant risk to the financial integrity of Bangladesh, serving as a critical channel for illicit fund outflows through the manipulation of trade transactions. The true volume of illegal transfers is hard to measure, since much activity is hidden. Besides trade fraud, money is moved via underground banking, shell firms, and informal remittances. Bangladesh loses billions of dollars each year to illicit financial outflows (IFFs), undermining growth and governance. Transparency International Bangladesh (TIB) cites GFI data finding an average of USD 8.275 bn/year (2009–18) via export under-invoicing and import over-invoicing-about 17% of trade value.[2] A recent government white paper estimates USD 234 billion siphoned out over 2009–23 i.e. 16 billion per year.[3] UN agencies and NGOs highlight that Bangladesh produced official estimates of illicit flows (drugs, human trafficking, etc.) only in 2023.[4] Available figures point to large and growing flows: the Bangladesh Bank Governor reported a single Chattogram-based scheme that sent USD 20 bn abroad illegally.[5] These estimates underscore a persistent upward trend in illicit outflows and Bangladesh's trade mis invoicing over the years.

General Case of Operational Risk of Banks-5: Cyber security Concern in Banks

Bangladesh Bank Cyber Heist

In 2016, hackers attempted to steal nearly $1 billion from Bangladesh Bank's account at the Federal Reserve Bank of New York. While most transfers were blocked, approximately $81 million was successfully siphoned off. (Source: www.thedailystar.net)

Mobile Financial Services (MFS) Scam

MFS scammers imitate an MFS officials to extract sensitive information such as PINs and OTPs for unauthorized transactions. They collect customer information from MFS agent points and transfer the amount scammed to multiple accounts, which makes it difficult to identify. In another case, Bangladesh Bank detected fraud against MFS provider for creating Tk 645 crore in e-money without the necessary cash backing and filed a case in this regard. It is also blamed for unauthorized withdrawals of approximately Tk 1,711 crore from accounts maintained for government allowances. (Source: www.thedailystar.net)

ATM frauds

From 2016 to 2019, several ATM frauds were detected. Scammers frequently copied customer card information of various banks to withdraw approximately 10 million taka. Thieves stole 1.2 million taka from ATMs of a bank in two incidents and some of these scams were done by foreign groups. Additionally, customs officials found ATM cards illegally imported from Singapore, with 100,000 illegal cards linked to 4.1 million taka in unpaid taxes. Scammers also used POS machines at shops, hotels, and other businesses to steal over 50-60 million taka. Another scam involved a Turkish hacking group targeting a number of Bangladeshi banks. Foreign nationals withdraw 3 lakh taka from a bank's ATM booth (Source: www.thedailystar.net)

[2] https://www.ti-bangladesh.org/articles/commentary/6384

[3] thefinancialexpress.com.bd/special-issues/white-paper-on-state-of-the-bangladesh-economy

[4] https://unctad.org/news/first-ever-official-data-illicit-financial-flows-now-available

[5] https://www.thedailystar.net/business/news/bb-governor

General Case of Operational Risk of Banks-6: Agent Banking Deserve Greater Attention

Starting its operations in 2013 as a safe alternative delivery channel of banking services to the underserved population, agent banking expanded rapidly, particularly in rural areas. Till December 2024, the number of accounts grows to around 16 million, deposits BDT 41,955 (crore), and remittances BDT 173,390 (crore). The business is mainly performed by 16,021 agents of 31 banks through 21,248 outlets. Despite the rapid growth, some agents misappropriated deposits, misused funds, and engaged in unauthorized lending, leading to losses estimated in the hundreds of crores of BDT (For example, a major financial scandal has been alleged at the Akkelpur agent banking branch of a shari'ah based bank situated in Joypurhat in this year. The cashier was involved in withdrawing nearly BDT 3 crore from customer and institutional accounts, systematically using deceptive tactics. Another scandal had been alleged one year ago at Nimai kashari agent banking branch of the same bank in Narayangonj where the agent escaped with BDT 2 crore of customers' money. This kind of incidents lead to operational and reputational risks, which compel banks to follow conservative lending practices to mitigate risks and avoid systemic impact.[6]

General Case of Operational Risk of Banks-7: Cyber Disruption

In September 18, 2023 at 7:50 am, Dumni Network Operation Center (NOC) officials informed the Network Team that Internet DMZ Perimeter Firewall-01 had gone down in the network monitoring system (Nagios). Around 8:15 am, Mr. X from the network team arrived at SMDR and observed that the mentioned firewall was experiencing significant packet loss, causing a slowdown in the entire internet traffic. Mr. X then activated the standby secondary DMZ Perimeter Firewall-02. However, it also encountered high processing load (packet loss). The network team decided to shut down all public-facing services and gradually bring them back online around 9:00 pm. During this period, both DMZ Perimeter Firewalls generated substantial traffic and sent it to the Security Systems (SIEM, NBA).

In September 22, 2023 at around 2:25 pm, all internet-based services became inaccessible, and the Network Team identified that the CPU usage of the Internet DMZ Perimeter Firewall had exceeded 90%. During this period, the Authoritative Domain Name Service (DNS) server received 75 million connections between 2:25 pm and 3:45 pm. Concurrent connections/sessions at the Internet DMZ Perimeter Palo Alto Firewall (new) reached 1 million (10,00,000) at that time, whereas the Internet DMZ Perimeter Firewall (Cisco ASA 5525) could handle a maximum of 500,000 (0.5 million) sessions. As a result, the firewall's CPU utilization exceeded 90%, leading to the outage of all services.

Considering both situations, ITSD of ABC Bank reviewed the entire traffic on Security Information and Event Management (SIEM) and Network Behavior Analysis (NBA). After analyzing the NBA and SIEM traffic, ITSD observed that the regular NBA network traffic ranged from 70 million to 80 million. However, on September 22, 2023, during the incident, it reached almost 285 million. Furthermore, the regular SIEM flow was around 1 million, but during that time, the traffic exceeded 3 million. NBA collects network flow data for network connections, whereas SIEM only collects log data. Additionally, they observed DNS traffic initiated from different IPs and countries. Based on the traffic pattern and behavior, ITSD assumed that this was a Distributed Denial of Service (DDoS) attack. Source: Basd on FGD Discussion

[6] https://today.thefinancialexpress.com.bd (February 18, 2025, The Financial Express); The Business Standard Online; https://www.thedailystar.net/(Mar 3, 2025, The Daily Star); https://www.thedailystar.net/business (Jan 3, 2024, The Daily Star)

General Case of Operational Risk of Banks-8: CRO vs CCRO

Bangladesh Bank's 2018 Risk Management Guidelines mandate that all commercial banks establish a dedicated risk management division and appoint a Chief Risk Officer (CRO) at the rank of Deputy Managing Director to lead it. The CRO is expected to oversee the bank's entire risk landscape, ensuring robust risk practices and compliance with applicable regulations. This role involves identifying threats that may hinder the institution's strategic goals and fostering a risk-aware culture. According to the Basel Committee on Banking Supervision (BCBS), the CRO should serve as an independent senior executive, entrusted with the design and implementation of the institution's comprehensive risk management framework across all levels of the organization.

However, in the context of Bangladesh the scenario is somewhat different. As risk management is yet to get due importance in our banking system, the Head of RMD and the CRO is not the same person in most of the cases. It is also true that the CRO performs the role of Chief Credit Risk Officer (CCRO) as the CRO is appointed from the credit background. As such the CRO is primarily focused on managing credit risk instead of overall risk management. This is a serious cause of concern from the true risk management point of view.

Source: Basd on FGD Discussion

General Case of Operational Risk of Banks-9: Change Management and Operational Risk in Banking

When a bank undergoes a major transformation (e.g., digitalization), change management plays a critical role because poor handling of organizational or system changes can directly lead to operational risks, such as service disruptions, fraud, regulatory breaches, and data loss. In line with change management, talent management ensures the right people with the right skills are in place to support the change. Mismanagement of talents leads to errors, non-compliance, undetected fraud, reduced service quality, causing reputational damage and customer attrition. For example, in the year 2020, a bank employee serving as Chief Regional Officer at the Radhanagar branch in Magura of XYZ Bank, exploited systemic weaknesses by accessing official email accounts that shared a common default password. He sent a fraudulent Telegraphic Transfer (TT) order of BDT 5 lakh using these accounts.

In 2022, ABC Bank faced a massive loan scam where approximately Tk 20 billion was embezzled through loans to non-existent organizations. The fraudulent activities were facilitated by internal collusion and inadequate due diligence, leading to significant financial and reputational damage.

In 2023, seven bank officers, including a branch manager of PQR Bank, were implicated in the embezzlement of over BDT 3 crore. Their fraudulent activities included forging customer signatures, creating unauthorized loan accounts, and misappropriating funds through various channels.

The incidents indicate inadequate oversight during the transfer of personnel to critical positions, a lack of segregation of duties, allowing collusion among staff, and inadequate selection during internal transfers and promotions.

Source: https://www.tbsnews.net/, https://www.dailymessenger.net/ and, Kabir, Musnun & Hosen, Md. Mosharaf. (2024)

Source: *Habib et al. (2025)*

List of Abbreviations

AAIB : Al-Arafah Islami Bank PLC
AAOIFI : Accounting and Auditing Organization for Islamic Financial Institutions
ACB : Audit Committee of the Board
ASIFI : Islamic Finance Institution
AT1 : Additional Tier 1
ATM : Automated Teller Machine
BB : Bangladesh Bank
BCBS : Basel Committee on Banking Supervision
BCP : Business Continuity Plan
BDT : Bangladesh Taka
BGIS : Bangladesh Government Investment Sukuk
BIA : Basic Indicator Approach
BGIIB : Bangladesh Government Islamic Investment Bond
BIBM : Bangladesh Institute of Bank Management
BoD : Board of Directors
BRMC : Board Risk Management Committee
BRPD : Banking Regulation and Policy Department
CEO : Chief Executive Office
CET1 : Common Equity Tier 1
CIBFP : Certified Islamic Banking and Finance Professional
CIPA : Certified Islamic Professional Accountant
CPD : Continuous Professional Development
CRAR : Capital to Risk-Weighted Assets Ratio
CRO : Chief Risk Officer
CCRO : Chief Credit Risk Officer
CSAA : Certified Shari'ah Adviser and Auditor
DDoS : Distributed Denial of Service
DNS : Domain Name Service
DR : Disaster Recovery
ERM : Enterprise Risk Management
ERMC : Executive Risk Management Committee
ESG : Environmental, Social, and Governance
EXIM : Export Import Bank of Bangladesh PLC
FAQs : Frequently Asked Questions
FC : Foreign Currencies
FGD : Focus group Discussions
FDIC : Federal Deposit Insurance Corporation
FIs : Financial Institutions
FSIB : First Security Islami Bank PLC
GCC : Gulf Cooperation Council
GS : Governance Standards

HPSM : Hire Purchase under Shirkatul Melk
IAH : Investment Account Holders
IBs : Islamic Banks
IBB : Institute of Banker Bangladesh
IBB : Islami Bank Bangladesh PLC
IBF : Islamic Banking and Finance
IBLF : Islami Bank Liquidity Fund
IBRPD : Islamic Banking Regulations and Policy Department
ICAAP : Internal Capital Adequacy Assessment Process
ICCD : Internal Control and Compliance Divisions
ICT : Information and Communications Technology
IFIs : Islamic Financial Institutions
IFSB : Islamic Financial Services Board
IMF : International Monetary Fund
ISA : Internal Shariah Audit
IT : Information Technology
KIIs : Key Informant Interviews
KRIs : Key Risk Indicators
MFS : Mobile Financial Services
MIS : Management Information System
MLS : Mudaraba Liquidity Support
NBA : Network Behavior Analysis
NOC : Network Operation Center
NPI : Non-Performing Investments
NPLs : Non-Performing Loans
OECD : Organisation for Economic Co-operation and Development
ORM : Operational Risk Management
ORMF : Operational Risk Management Framework
OTPs : One Time Password
PLC : Public Limited Company
PSIAs : Profit-Sharing Investment Accounts
PSMOR : Principles for the Sound Management of Operational Risk
RegTech : Regulatory Technology
RMC : Risk Management Committee
RMD : Risk Management Division
ROA : Return on Assets
ROE : Return on Equity
SIB : Social Islami Bank PLC
SIEM : Security Information and Event Management
SJIB : Shahjalal Islami Bank PLC
SLS : Special Liquidity Support
SMT : Senior Management Team
SNCR : Shariah Non-Compliance Risk
SRP : Supervisory Review Process

SSB	: Shari'ah Supervisory Board
SSC	: Shari'ah Supervisory Committee
SupTech	: Supervisory Technology
TA	: Total Assets
TIB	: Transparency International Bangladesh
TBML	: Trade-Based Money Laundering
Tk	: Taka
ToR	: Terms of Reference
TSA	: The Standardized Approach
TT	: Telegraphic Transfer



Bangladesh Institute of Bank Management

Plot No.-4 MainRoad No.-1(South), Section No. - 2, Mirpur, Dhaka - 1216

Tel: 48032091-4; 48032097-8; 48032104; email: office@bibm.org.bd; Website: www.bibm.org.bd

Price: BDT 300.00
USD 8.00