Governance and Practices of Operational Risk Management in Banks

Banking Research Series 2025

Keynote Paper of Research Workshop of BIBM

Issue No. 01

Dr. Shah Md. Ahsan Habib
Md. Nehal Ahmed
Dr. Md. Mahabbat Hossain
Rexona Yesmin
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. 01

Governance and Practices of Operational Risk Management in Banks

Research Team

Dr. Shah Md. Ahsan Habib
Professor (Selection Grade), BIBM

Md. Nehal Ahmed
Professor (Selection Grade) and Director (DSBM), BIBM

Dr. Md. Mahabbat Hossain
Associate Professor, BIBM

Rexona Yesmin
Assistant Professor, BIBM

Md. Emon Arefin
Lecturer, BIBM

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

Governance and Practices of Operational Risk Management in Banks

Editorial Advisor : **Md. Akhtaruzzaman, *Ph.D.***
Director General, BIBM

Editor : **Md. Alamgir *CIPA, CSAA***
Associate Professor and Director (Training), BIBM

Research Team : **Dr. Shah Md. Ahsan Habib**
Professor (Selection Grade), BIBM
: **Md. Nehal Ahmed**
Professor (Selection Grade) and Director (DSBM), BIBM
: **Dr. Md. Mahabbat Hossain**
Associate Professor, BIBM
: **Rexona Yesmin**
Assistant Professor, BIBM
: **Md. Emon Arefin**
Lecturer, BIBM

Support Team : **Md. Al-Mamun Khan**
Senior Officer (PPR), BIBM
: **Md. Habibur Rahman**
Assistant Senior Officer (General), BIBM
: **Md. Jalilur Rahman**
Officer (General), BIBM
: **Sumona Moqutadar Happy**
Officer (General), BIBM
: **Md. Morshadur Rahman**
Officer (PPR), BIBM

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

Published : June 2025

Forewords

In an era marked by digital transformation, global uncertainties, and heightened regulatory expectations, the ability of banks to effectively manage operational risk has become a strategic necessity. Operational Risk Management (ORM) is no longer confined to back-office controls – it is central to safeguarding institutional integrity, customer trust, and systemic stability.

The Bangladesh Institute of Bank Management (BIBM) remains committed to supporting a resilient and forward-looking banking sector through evidence-based research, capacity-building, and policy engagement. As part of this ongoing commitment, the current review paper titled "Governance and Practices of Operational Risk Management in Banks" provides a timely and in-depth assessment of the evolving ORM landscape in Bangladesh.

This study integrates quantitative and qualitative approaches, drawing from structured surveys, Focus Group Discussions (FGDs), and Key Informant Interviews (KIIs) with senior risk professionals across the industry. The research explores institutional governance structures, implementation challenges, monitoring tools, and compliance frameworks relevant to operational risk. It also reflects on international standards, national regulatory directives, and sector-wide practices to identify both gaps and opportunities for improvement.

I would like to extend my sincere appreciation to the industry professionals who contributed valuable insights to this research. I also commend the research team for their dedication, analytical depth, and professional rigor. Their efforts have resulted in a comprehensive document that will serve as a valuable resource for practitioners, regulators, academics, and other stakeholders in the banking sector.

I am confident that the findings and recommendations of this paper will support banks in enhancing their ORM frameworks and fostering a more resilient, transparent, and accountable financial system in Bangladesh. Besides, the regulators may also find it as a ready for source for modifying the concerned policy framework.

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

Acknowledgment

The successful completion of this research study titled “Governance and Practices of Operational Risk Management in Banks” has been made possible through the invaluable contributions, support, and collaboration of numerous individuals and institutions. We would like to express our deepest gratitude to Dr. Md. Akhtaruzzaman, Director General of BIBM, for his unwavering guidance and strategic direction throughout the study.

We extend our sincere thanks to the Director (Training), BIBM, for their consistent support in facilitating institutional cooperation, logistical arrangements, and stakeholder engagement that significantly contributed to the timely execution of this research and dissemination the findings.

We are especially grateful to the wider banking community of Bangladesh, particularly the Managing Directors/CEOs and Heads/Deputy Heads of Risk Management Units, for their active participation and willingness to share data, insights, and operational experiences. Their engagement has deeply enriched the findings and relevance of this study.

We would also like to acknowledge the support of our colleagues at BIBM—especially those from the Training, Administration, Accounts, and Publication Wings—for their efficient cooperation across various operational aspects of the review workshop.

Finally, we are thankful to all individuals who, directly or indirectly, contributed to this research. The diverse viewpoints and open collaboration from stakeholders have enabled us to produce a comprehensive and meaningful reflection of the operational risk landscape in Bangladesh’s banking sector.

Dr. Shah Md. Ahsan Habib
Md. Nehal Ahmed
Dr. Md. Mahabbat Hossain
Rexona Yesmin
Md. Emon Arefin

Table of Contents

1.0 Introductory Note	01
2. Concepts and Guiding Framework for Operational Risk Management -Literature Review	04
2.1 Key Risk Elements and Issues of Operational Risk in Banking	04
2.1.1 Understanding the Nature and Origins of Operational Risk in Banking	04
2.1.2 Interdependencies of Operational Risk with Major Risks in Banking	06
2.2 Guiding Framework for ORM in Banks	08
2.2.1 Basel Principles for ORM in Banks	08
2.2.2 Basel Requirement and Calculation of Capital Requirement for Operational Risk	09
2.2.3 Principles for Effective Aggregation and Reporting of Risk Data	10
2.2.4 Financial Stability Board (FSB) Contributions to Operational Risk Governance	10
2.2.5 ISO and COSO Standards Relevant to Operational Risk Management	11
2.2.6 Integration of Anti-Money Laundering (AML) Standards into ORM	12
2.2.7 Governance and Practices of Operational Risk Management in Islamic Banks	12
3. ORM Framework and Practices in Banks: Global Context	15
3.1 ORM: Banks' Approach	16
3.1.1 Operational Risk Identification	16
3.1.2 Operational Risk Assessment	17
3.1.3 Operational Risk Monitoring and Reporting	18
3.1.4 Operational Risk Mitigation and Control	20
3.1.5 Business Resilience and Continuity Planning	21
3.2 Operational Risk Management: Regulatory and Supervisory Approach	22
3.2.1 Supervisory Mechanisms: Inspections, Audits & Risk-Based Supervision	23
3.2.2 Regulatory Framework for ORM and National Regulation	24
3.2.3 Internal Governance and Risk Reporting	24
3.2.4 Enforcement Actions and Sanctions	26
3.2.5 Technology in Monitoring ORM	26
4. Governance and Practices of ORM in the Banking Industry of Bangladesh	27
4.1 Regulatory Landscape for ORM in Bangladesh	28
4.2 Operational Risk Management Practices in Banks in Bangladesh - Survey Findings	29
4.2.1 Industry Governance and Practices [Opinion Survey] - Outcomes of KIIs	29
4.2.2 ORM Practices of Banks with Standalone ORM Units/Wings-Survey Outcome	36
4.2.3 Governance and Practices of 'Operational Risk Management' - Findings of FGD	38
4.3: Challenges Associated with Operational Risk Management and Governance in Banks	41
4.3.1 Operational Risk Elements and the Associated Challenges	41
4.3.2 Challenges of Operational Risk Management in Banks - Survey/KII Opinions	46
5. Challenges and Suggestions - Issues for Discussions	48
References	51

List of Tables

Table 4.1: Governance Structure of Operational Risk Management in Banks	30
Table 4.2: Board and Senior Management Oversight on ORM Practices in Banks	30
Table 4.3: Implementation of Three Lines of Defence Model in Banks	30
Table 4.4: Primary Tools and Methods Used to Identify Operational Risks in Banks	31
Table 4.5: Banks ORM Aligned with Regulatory Frameworks	31
Table 4.6: Internal Loss Event/Incident Data Collected and Managed in Banks	32
Table 4.7: Conducting Scenario Analyses in Banks	32
Table 4.8: Challenges of Conducting Scenario Analyses in Banks	32
Table 4.9: Monitoring Operational Risk Across Department/Branches in Banks	33
Table 4.10: Key KRIs used in Banks	33
Table 4.11: Frequency of ORM Reporting to Senior Management/Board in Banks	34
Table 4.12: Managing Operational Risk of Outsourcing	34
Table 4.13: Management of Cybersecurity Risk	34
Table 4.14: Building ORM Culture and Awareness in Banks	35
Table 4.15: Assessment of Training Effectiveness	35

List of Box

Box 2.1: Key Characters of Operational Risks in Banks	05
Box 2.2: Three Pillars of Operational Risk Management	09
Box 2.3: Capital Requirement for Operational Risk Under Basel Framework	09
Box 3.1: Operational Risk Management Framework & Tools	15
Box 4.1: Management Monitoring System	36
Box 4.2: Early Warning Indicators	37
Box 4.3: Managing Operational Risks Associated with the Agent Banking	37
Box 4.4: Managing Risks Generated by the Outsourcing Providers	38
Box 4.5: Basic Features of Contingency Plans Related to Disaster Recovery and Business Continuity	38
Box 4.6: Key Points of the FGD Discussion	40
Box 4.7: Crisis of High NPL in Bangladesh	41
Box 4.8: Gross Manipulation in Some Shari'ah Based Banks	42
Box 4.9: Big Scams and Operational Risks in Banking in Bangladesh	42
Box 4.10: Illicit Outflows using Trade is a Huge Risk	43
Box 4.11: Cyber security Concern in Banks	44
Box 4.12: Agent Banking Deserve Greater Attention	44
Box 4.13: Cyber Disruption	45
Box 4.14: CRO vs CCRO	45
Box 4.15: Change Management and Operational Risk in Banking in Bangladesh	46
Box 4.16: Challenges of Event Based Operational Risk	46

List of Appendix

Appendix Table A1: Top Operational Risks in Banking	55
Appendix Table A2: Twelve Principles and Role of Supervisors by BCBS	55
Appendix Table A3: Operational Loss Event Types	58

Executive Summary

This report presents a comprehensive assessment of the governance and practices of Operational Risk Management (ORM) in Bangladesh's banking sector. It builds on emerging global standards and national regulatory expectations, drawing insights from structured questionnaire surveys, Key Informant Interviews (KIIs), and Focus Group Discussions (FGDs) involving risk professionals, and senior bank executives. The primary objective is to evaluate governance and practices of ORM in banks in the global and Bangladesh context.

Operational risk has become an increasingly significant concern for the banking industry due to internal process failures, human errors, system breakdowns, and external events—including rising cyber threats and compliance lapses. Regulatory frameworks, especially those aligned with the Basel Committee on Banking Supervision (BCBS), the Financial Stability Board (FSB), and international standards like ISO 31000 and COSO ERM, emphasize the need for robust governance structures and integrated risk management. In Bangladesh, while ORM is embedded within broader risk guidelines issued by Bangladesh Bank, the absence of a standalone ORM framework has resulted in fragmented practices across institutions.

Field-level evidence reveals that only a limited number of banks have dedicated ORM units or clearly defined risk governance frameworks. The Chief Risk Officer (CRO) is expected to oversee operational risks, but role confusion, limited segregation of duties, and overlapping responsibilities remain prevalent. The study found that many banks conflate the responsibilities of operations and risk oversight, violating the principle of independent risk monitoring. ORM functions often lack authority, adequate staffing, or standardized methodologies such as Key Risk Indicators (KRIs), Risk and Control Self-Assessments (RCSAs), and scenario analysis.

Despite some progress – such as inclusion of ORM within board-level oversight and adoption of loss event tracking – bank practices are still highly variable and largely reactive. Notably, most banks rely on basic indicator approaches for capital calculation under RBCA guidelines, with minimal use of advanced techniques. The study also found low levels of automation in ORM processes, limited real-time monitoring capabilities, and minimal integration of risk data across departments.

A significant institutional insight from this research is the absence of formal accountability for ORM in many banks. Survey results indicate that even where policies exist, there is inadequate internal ownership of ORM responsibilities. Furthermore, many operational risks, including Shari'ah non-compliance in Islamic banks, remain under-reported due to weak process controls and insufficient training.

This report recommends the formulation of a dedicated Operational Risk Management Guideline by Bangladesh Bank, supported by enforceable standards on governance structures, reporting lines, and minimum qualifications for ORM leadership. Additionally, banks should implement robust ORM frameworks aligned with

international principles, invest in automation and analytics tools, and institutionalize continuous capacity building for risk professionals.

In sum, operational risk is no longer a peripheral concern – it is central to the strategic and reputational integrity of the banking system. Strengthening ORM is imperative not only for regulatory compliance but also for sustaining public trust and long-term institutional stability in Bangladesh's financial sector.

Governance and Practices of Operational Risk Management in Banks

1. Introductory Note

The risk landscape within the banking sector has undergone significant transformation, compelling institutions to place greater emphasis on the governance and execution of operational risk management (ORM). This shift is driven by increasing vulnerabilities related to breakdowns in internal operations, system failures, human lapses, and external disruptions – elements broadly consistent with the Basel Committee's definition of operational risk. The liberalization of financial markets, cross-border expansion of services, introduction of intricate financial instruments, consolidation through mergers and acquisitions, and extensive reliance on third-party service providers have collectively heightened the operational risk exposure across the industry. Moreover, rapid technological integration – particularly the rise of digital banking and automation – has further intensified these risks (EY, 2025).

Awareness around operational risk escalated notably in the 1990s following high-profile incidents, such as the Barings Bank collapse that resulted in USD 1.4 billion in losses. Since then, the banking industry has faced growing and more visible operational failures. For example, FDIC (2024) reported that in 2004, twenty U.S. banks participating in a Loss Data Collection Exercise disclosed a cumulative USD 15 billion in operational losses – tripling the amount reported in 2002. A more recent study of 82 international banks recorded operational losses amounting to EUR 129 billion between 2018 and 2023, with EUR 15.2 billion incurred in 2023 alone (EY, 2025). Prior to the 2000s, particularly in developing and Asian markets, operational risk was often overlooked. However, the implementation of Basel II and the fallout from the global financial crisis compelled regulators to distinguish operational and human-related risks as critical components within risk governance frameworks (Hugh, 2023).

Failures of internal processes and controls including faulty policies and compliance lapses have generated the largest fines in banking. Wells Fargo's fake-account scandal led to a USD 3 billion settlement; HSBC's deficient anti-money-laundering controls forced bank to forfeit USD 1.256 billion and pay an additional USD 665 million in penalties; JPMorgan lost USD 380 million for consumer-protection failures; Barclays agreed to pay about GBP 290 million for LIBOR manipulation (Barkha, et. al, 2024). Bank of Tokyo-Mitsubishi UFJ sanctions case was also fundamentally a process control breach, and regulators worldwide imposed a cumulative USD 4 billion in fines on financial institutions for AML/compliance failures.[1] India's RBI imposed fines of Rs 97.8 lakh on ICICI Bank in 2025 for KYC and cybersecurity process lapses.[2]

[1] www.washingtonpost.com/business/economy/bank-of-tokyo-to-pay-250m-to-ny-in-money-laundering-case

[2] RBI imposes penalties on ICICI Bank: The Economic Times (economictimes.indiatimes.co)

People risk i.e. misconduct, human error, and fraud has also driven major banking losses. In 1995, Barings Bank collapsed after a single trader's unauthorized bets lost; in the 2000s, one bank employee at Societe Generale caused roughly over USD 7 billion in losses; UBS lost USD 2.3 billion in 2011 to unauthorized trading by a London-based employee; Deutsche Bank took a USD 7.3 billion charge in 2016 largely for past misconduct (Chernobai et.al, 2016). After 2008, Asian banks faced more whistle-blower exposures and forensic probes. For example, in Singapore, a former DBS relationship manager in 2023 admitted cheating four clients of USD 348,000 by selling fake investment products.[3]

Technology and infrastructure breakdowns have proliferated as banks digitize with ample examples that hardware or software glitches, third-party IT errors, and cyber-attacks can halt critical operations. In 2012, an ill-tested software upgrade knocked out payment systems for weeks, affecting 6.5 million customers and leading to a GBP 42 million penalty (raised to GBP 56M) for RBS/NatWest outage.[4] In Asia, Japan's Mizuho Bank suffered three nationwide system outages in under 20 years: in 2002 it delayed 2.5 million auto-debit transactions during a merger; in 2011 its system buckled under emergency relief transfers; and in 2018 nearly 2,956 out of 5,395 ATMs went offline after a data transfer glitch.[5] Similarly, in India HDFC Bank was penalized by the RBI for two major Internet banking outages (Nov 2018 and Dec 2019)[6]

It is evident today that natural disasters, terrorist acts, or sudden legal changes can trigger huge operational losses for banks. For instance, hurricanes and pandemics have stressed banks' continuity plans (Hurricane Sandy in 2012 and COVID-19 in 2020) forcing many institutions to rely on emergency workarounds. In 2024 the collapse of ATM operator AGS Transact stranded about 38,000 ATMs across India's banks.[7] In 2025, DBS Bank disclosed that ransomware on a printing vendor potentially exposed the data of 8,200 customers.[8] Bangladesh Bank's SWIFT heist is an example of external geopolitical and cyber threats.

Available data support the fact that banks' operational environments have become much riskier and over the last three decades, operational failures have become more visible, costly, and complex, demanding closer study and mitigation. Given the persistent record of large losses, scholars and practitioners stress the need for better

[3]https://www.finews.asia/finance/42812-dbs-pang-yuheng-wealth-planning-fixed-deposits-cheating-singapore

[4] FCA fines RBS, NatWest and Ulster Bank Ltd £42 million for IT failures | FCA

[5] https://asianbankingandfinance.net/banking-technology/news

[6]indianexpress.com/article/business/banking-and-finance/hdfc-bank-admits-net-banking-glitches-customers-face-problem-in-accessing-services-7251455/ (2021)

[7]https://economictimes.indiatimes.com/industry/banking/finance/banking/ags-transacts-troubles-hurt-many-banks-atm-operations/articleshow/118824349.cms?from=mdr

[8]www.dbs.com/newsroom/DBS_made_aware_of_ransomware_attack_at_printing_vendor_Toppans_systems_affecting_mainly_statements_related_to_DBS_Vickers_accounts

metrics and data (Barkha, et. al, 2024). Today, effective operational risk governance and management are central to ensuring banking system stability, especially in the wake of growing operational complexities, financial crime, digital transformation, cyber threats, and geopolitical uncertainties. Especially cyber-security risks, third-party risks, compliance risks, change management risks, and financial crime risks deserve utmost attention (Appendix Table A1) with a structured ORM Framework. Despite improvement, the banking industry of the developing countries remained behind in this connection. Bangladesh banking industry does not seem to be different in this context.

Broadly, the paper is to discuss governance and practices of ORM in banks in the global and Bangladesh context. Specifically, the objectives of the study are: ***one***, to discuss governance and best practices of ORM in the context of the global banking industry; ***two***, to analyze governance and ORM practices of banks in Bangladesh; and ***three***, to identify issues and challenges to draw lessons relevant to the efficient ORM governance and practices for the banking industry of Bangladesh.

This study utilized a combination of primary and secondary data sources. Primary data was collected through a structured questionnaire administered to assess the governance structures and implementation status of operational risk management (ORM) practices. Besides, the openion survey targeted 15 local banks (excluding foreign entities) that reported having a defined Enterprise Risk Management (ERM) policy and an independent ORM unit. To gain deeper qualitative insights, Key Informant Interviews (KIIs) were conducted with the Heads or Deputy Heads of the Risk Management Departments in these institutions. Additionally, a Focus Group Discussion (FGD) involving the same set of risk leaders was held to identify key implementation challenges and to gather actionable recommendations. Supplementary secondary data – including case examples – were sourced from academic literature, media reports, and other publicly available publications. The draft report was presented at a BIBM workshop attended by approximately 50 banking professionals. The final version incorporates the feedback and recommendations provided during the session.

The structure of the paper is divided into five major segments. Section one outlines the background, research objectives, and methodology. Section two explores conceptual foundations and regulatory frameworks relevant to operational risk management. Section three examines global ORM frameworks and international best practices. Section four reviews the state of ORM governance and implementation within the Bangladeshi banking sector. Finally, section five presents critical issues and proposes directions for enhancing operational risk governance in Bangladesh's banking industry.

2. Concepts and Guiding Framework for ORM

Unlike several other risks associated with banking operations e.g. credit risk or market risks, operational risks cannot be managed solely or independently and thus require differential approach. As the subset of Enterprise Risk Management (ERM), Operational Risk can be a root cause of other risks; and it is crucial to recognize that Operational Risk is scattered in all the functional areas of banking and might be responsible for the erosion of trust in the banking institutions. With the growing recognition of managing operational risks, several global standards and guidelines are developed by international regulatory bodies/agencies to ensure sound risk management practices, financial stability, and resilience across the banking sector.

2.1 Key Risk Elements and Issues of Operational Risk in Banking

2.1.1 Understanding the Nature and Origins of Operational Risk in Banking

Operational risk refers to the potential for loss arising from deficiencies or breakdowns in internal processes[9], human actions[10], technological systems[11], or unforeseen external events[12]. This interpretation, which also encompasses legal risks while excluding strategic[13] and reputational risks, was initially outlined by the Bank for International Settlements (BIS) in its foundational document *"Sound Practices for the Management and Supervision of Operational Risk"* published in 2003 (BCBS, 2003). The same formulation was reaffirmed in the Basel Committee's 2004 framework titled *"International Convergence of Capital Measurement and Capital Standards,"* widely recognized as the Basel II Framework (BCBS, 2004). Basel III (BCBS, 2011) retained the definition and scope of operational risk while strengthening risk governance and capital adequacy considering the risk scenarios during the global banking and financial crisis (2007-2008). Finalised Basel III/Basel-IV did not change the scope of operational risk however, introduced a fresh standardised capital calculation approach to replace internal models.

[9] Inadequate / inappropriate guidelines, policies & procedures; Erroneous data entry; Poor customer / legal documentation; Inadequate back up / contingency plan.

[10] Breach of internal guidelines, policies & procedures; Breach of delegated authority; Criminal acts (internal); Inadequate segregation of duties; Staff oversight, etc.

[11] Inadequate hardware / network / server maintenance, etc.

[12] Criminal acts; Vendor mis-performance; Man-made disaster; Natural disaster; and Political regulatory causes.

[13] Strategic Risk in banks refers to the potential for losses arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to changes in the financial, regulatory, or competitive environment. Basel Committee including Federal Reserve, and ECB expect banks to manage Strategic Risk as part of their Enterprise Risk Management.

While maintaining its original definition, the Bank for International Settlements (BIS) integrated the concept of operational risk into the wider framework of operational resilience through its 2021 update of the Principles for the Sound Management of Operational Risk. These revised principles underscore the importance of ensuring business continuity, particularly in response to disruptions such as cyber incidents and large-scale natural events, including pandemics.

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 (Box 2.1).

Box 2.1: Key Characters of Operational Risks in Banks

First, operational risk is often difficult to isolate from other key banking risks such as credit and market risks, as these categories frequently interact and overlap in real-world scenarios. Their interdependence makes risk boundaries less distinct in practical applications.

Second, operational risk is inherently wide-ranging. It stems from a variety of sources including human behavior, system failures, procedural flaws, and unforeseen external events. Given the diversity in institutional structures, geographic locations, and operational models, the scope of operational risk varies significantly across banks and sectors.

Third, it is inherently unpredictable and dynamic. Operational risk can emerge in any department and is closely tied to management practices, staff behavior, organizational professionalism, and institutional culture. As the banking industry continues to evolve, static risk models prove insufficient in capturing emerging threats.

Fourth, operational risks may originate from human actions or system-related failures, with the former being more prevalent. Such risks can be mitigated through enhanced staff training, capacity-building initiatives, and continuous upgrades or redesign of internal systems and infrastructure.

Source: *Based on Lu Jin, 2024.*

Classifying operational risks into fixed categories is inherently difficult, as their nature often varies between institutions based on structure, processes, and operational complexity. Nonetheless, Basel II and its subsequent frameworks have proposed seven general event types that serve as a foundation for identifying and managing operational risk. The first category, **internal fraud**, refers to acts committed by employees that are detrimental to the institution's interests, such as embezzlement or unauthorized activities. **External fraud** encompasses criminal actions by third parties, including theft, check forgery, and cyber intrusion. The third category, **employment practices and workplace safety**, addresses violations of labor

regulations or health standards, which can expose institutions to legal or reputational consequences. The fourth type, **clients, products, and business practices**, includes failures to meet professional obligations to clients due to misconduct or negligence. **Damage to physical assets**, the fifth category, involves loss events resulting from natural disasters or other destructive incidents. **Business disruption and system failures** refer to interruptions caused by breakdowns in IT systems, supply chain issues, or third-party service failures that impair operations. Lastly, **execution, delivery, and process management** involves risks linked to transactional errors, documentation flaws, or inefficiencies in day-to-day banking operations, such as incorrect data entry or misrouted instructions (BCBS, 2006).

2.1.2 Interdependencies of Operational Risk with Major Risks in Banking

While categorized separately for analysis and regulatory capital purposes, the major risk types in a bank are deeply interdependent and there are two-way interconnections. **Operational Risk is a driver of Credit Risk, whereas Credit Risk is a Trigger for Operational Risk:** Operational risk and credit risk are tightly linked. Failures in operational controls can cause credit losses, and extreme credit events can generate operational strains (e.g. legal risks, fraud) in banks. Operational failings may lead to large volumes of high-risk loans, which then default and magnify credit losses across the banking system. Conversely, deterioration in credit portfolios can stress (legal disputes, processing errors, etc.) a bank's operations and potentially induce operational risk events (Kelliher et.al., 2020).

Operational Failures Lead Market Losses, whereas Market Turbulence Uncovers Operational Risk: Some of the most notorious 'market risk' debacles in banking due to operational failures (collapse of Barings Bank in 1995). The causality also runs the other way. A sudden market crash or spike in interest rates can, for example, reveal that a bank's valuation or risk measurement processes were flawed (FDIC, 2006). It is also noteworthy that both market and operational risks can jointly arise from certain events (World Economic Forum).[14]

Operational Events Cause Liquidity Stress, whereas Other Risks Transmit into Liquidity via Operational Channels: A severe operational failure can quickly turn into a liquidity crisis for a bank. More commonly, operational risk events undermine the confidence of depositors and counterparties, which in turn affects liquidity. Liquidity risk can also be a downstream effect when credit or market risks materialize through operational channels (BCBS, 2008).

[14] https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity

Operational Failures Cause Reputational Damage, whereas Reputational Risk Amplify Other Risks: Operational risk is perhaps most tightly interwoven with reputational risk. Many operational failures have an immediate reputational impact, and conversely, reputational concerns often arise from operational or compliance shortcomings. Once a bank's reputation is hurt, other risks are magnified (Management Solution, 2021).

Operational and Compliance Risks are Closely Interrelated and Failures in One Category can Readily Propagate to the Other: Operational and compliance risks are deeply interrelated in banking. Many frameworks consider compliance risk as a subset or component of operational risk, given that compliance failures often manifest as operational loss events (FDIC, 2006). BCBS guidance notes a close relationship between these risks, with some banks integrating the compliance function within their operational risk management function (BCBS, 2005). A breakdown in internal controls (operational risk) can lead to compliance breaches like operational process failure might cause violations of anti-money laundering (AML) regulations. The International Monetary Fund observes that regulatory sanctions stemming from compliance failures can escalate into broader financial risks (IMF, 2023).

Operational Risk Management is Subset of Enterprise Risk Management and Closely Interconnected: ERM provides a holistic approach to identifying, assessing, and managing all types of risks while aligning risk management with the bank's strategic objectives. Through shared tools such as risk appetite statements, KRIs, scenario analysis, and risk control self-assessments, ORM supports the ERM function in measuring, aggregating, and reporting risk exposures. Moreover, insights from ORM such as operational loss trends and incident reports are essential for ERM's strategic decision-making and regulatory compliance. Risk appetite and strategic tragets have implications for ORM in banks (Unrealistic sales target contributed Well furgo scandal)[15]. Together, ERM and ORM contribute to enhance both resilience and value creation.

[15] https://corpgov.law.harvard.edu/2019/02/06/the-wells-fargo-cross-selling-scandal-2/

2.2 Guiding Framework for ORM in Banks

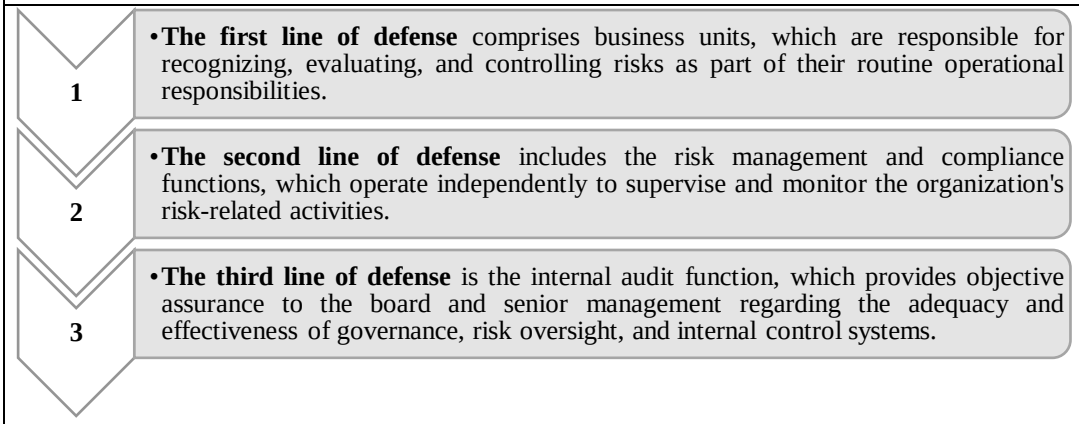
2.2.1 Basel Principles for ORM in Banks

The Basel Committee on Banking Supervision (BCBS) has played a central role in shaping global standards for ORM by guiding regulators and financial institutions in establishing structured governance mechanisms. In 2003, the BCBS introduced its foundational guidance titled "Sound Practices for the Management and Supervision of Operational Risk," outlining 11 core principles aimed at helping banks identify, assess, mitigate, and monitor operational risk exposures (BCBS, 2003). Over time, as the financial environment and institutional practices evolved, both regulators and banks gained deeper insights into the application of these frameworks. In response, the BCBS revised and refined the original set of principles in 2011, integrating considerations related to governance structures, risk management culture, and transparency through enhanced disclosure practices (BCBS, 2011).

Further developments came in March 2021, when the BCBS released updated guidance titled Revisions to the Principles for the Sound Management of Operational Risk (PSMOR). These updates emphasize the continued relevance of sound operational risk practices across institutions, regardless of their size or complexity. The revised framework comprises 12 principles (see Appendix Table A2), addressing areas such as governance, risk culture, information and communication technologies (ICT), business continuity planning, and disclosure. Importantly, the BCBS advises that these components should not be treated in isolation; rather, they should function as interconnected parts of an institution's broader operational risk and enterprise risk management frameworks—contributing to its overall operational resilience (BCBS, 2021).

The BCBS (2021) Principles clealry articulate 'three lines of defense' (Box 2.2), and the scope of the framework broadened to business resilience, pandemic response, and remote work. For business continuity management, the document emphasized risk culture, conduct, and operational resilience. The BCBS offers explicit guidance on emerging risks including cybersecurity, climate, pandemic, and innovation-related threats. As measures to handle third-party and outsourcing risks, it emphasized significant concentration risks and vendor governance. Supervisors are expected to evaluate the effectiveness, integration, and resilience of operational risk management (BCBS, 2021).

Box 2.2: Three Pillars of Operational Risk Management



Source: *BCBS (2021)*

2.2.2 Basel Requirement and Calculation of Capital Requirement for Operational Risk

Adequate capital is the key to risk abortion, and Basel frameworks are recognized guidelines for capital requirements as part of risk management in banks. Basel framework introduced several methods to estimate capital requirements for operational risks to be practiced by the global banking industry. Basel-II requires capital to be maintained by the banking institution for the first time. Basel suggested three methods: Basic Indicator Approach; Standardized Approach; and Advanced Measurement Approach (Box 2.3). The calculation and capital requirements for operational risks have evolved under the Basel III Framework, reflecting increased sensitivity to risk exposure and enhanced methodological sophistication.

Box 2.3: Capital Requirement for Operational Risk Under Basel Framework

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: Internal loss data; External data; Scenario analysis; Business environment and internal control factors, subject to supervisory approval.

Source: *Based on Basel III*

2.2.3 Principles for Effective Aggregation and Reporting of Risk Data

The BCBS introduced a dedicated framework – commonly referred to as BCBS 239 – to strengthen data governance, infrastructure, and reporting standards within financial institutions. This framework is particularly relevant to ORM, as it emphasizes the importance of data accuracy, timeliness, and responsiveness in enabling banks to manage emerging risks and adapt to evolving regulatory requirements.

To support proactive risk detection and response, institutions are encouraged to implement automated systems capable of continuously identifying potential issues and routing critical information to the appropriate personnel for swift action (Deloitte, 2018). A well-defined governance structure is essential, incorporating clearly assigned responsibilities and oversight mechanisms to ensure that data aggregation and reporting processes contribute effectively to the institution's overall risk management strategy, including ORM.

BCBS 239 outlines 14 core principles that guide banks in improving their ability to aggregate risk data and generate meaningful reports for informed decision-making. Among the foundational steps are: developing internal policies that clearly define what constitutes an operational risk event; specifying the data attributes required for each incident; and maintaining a robust internal loss database to support risk analysis. The committee recommends that banks accumulate at least ten years of historical data for ORM calculations, although a five-year baseline is permitted during transitional periods. Additionally, institutions must account for operational losses associated with discontinued business units and ensure collection of information on both loss recoveries and underlying causal factors (Deloitte, 2018).

2.2.4 Financial Stability Board (FSB) Contributions to Operational Risk Governance

The Financial Stability Board (FSB) plays an important role in supporting global financial stability through the development of standards and best practices. While the Basel Committee offers foundational guidance, FSB's work complements these efforts by focusing on resilience, governance structures, cybersecurity threats, and risks stemming from third-party relationships – all of which are integral to effective ORM.

In 2013, the FSB released its Guidelines for Effective Risk Appetite Frameworks, which emphasize the need for institutions to clearly articulate and enforce their risk appetite, including specific thresholds for operational risk exposure. These guidelines define the essential components of a risk appetite framework: the formal risk appetite

statement, the establishment of risk limits, and the delineation of responsibilities among senior leadership and the board of directors (FSB, 2013). The framework promotes alignment between strategic goals and operational risk tolerance, thus reinforcing strong governance.

In 2020, the FSB introduced the Effective Practices for Cyber Incident Response and Recovery, which sets out 49 actionable practices across seven domains: governance, preparation, analysis, mitigation, recovery, coordination and communication, and continuous improvement (FSB, 2020). This framework equips institutions to better manage disruptions caused by cyber threats, which represent a growing component of operational risk.

To address risks linked to outsourcing and third-party dependencies, the FSB in 2023 published a comprehensive toolkit aimed at enhancing oversight practices. This resource includes standardized definitions to foster uniform understanding across financial institutions, tools for identifying and evaluating critical external service providers, and supervisory mechanisms for assessing how institutions manage systemic dependencies. It is designed to promote consistent and transparent practices across jurisdictions in managing third-party risks (FSB, 2023).

2.2.5 ISO and COSO Standards Relevant to ORM

Operational Risk Management (ORM) functions as a critical component within the broader framework of Enterprise Risk Management (ERM). As such, globally recognized ERM standards are directly applicable to ORM practices. One such framework is ISO 31000, which outlines principles and a structured approach to managing organizational risks. Although not designed for certification, ISO 31000 serves as a universal guideline for establishing a risk-aware culture, defining governance responsibilities, and implementing a structured process for identifying, evaluating, and addressing risks throughout the organization[16].

Another relevant standard is ISO 22301, which pertains to Business Continuity Management Systems (BCMS). This international benchmark equips organizations with a comprehensive framework for preparing for and responding to operational disruptions. It emphasizes the continuity of essential functions during crises and supports effective change management and resilience-building strategies to ensure long-term operational stability.

The ERM Framework, developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), is also widely adopted in risk management and internal control assessments. COSO's model stresses the importance of embedding

[16] https://riskonnect.com/business-continuity-resilience/the-basics-of-iso-31000-risk-management/

risk considerations into an organization's culture, governance structures, and strategic planning processes. Notably, the framework highlights the intersection between operational and compliance risks – acknowledging that breakdowns in operational controls can lead to major compliance breaches, as evidenced in several high-profile banking failures. The COSO ERM framework, initially introduced in 2004 and later updated in 2017 and 2024, provides a principle-based structure to integrate risk management into overall strategic and performance objectives[17].

2.2.6 Integration of Anti-Money Laundering (AML) Standards into ORM

Anti-Money Laundering (AML) regulations serve as a critical safeguard to prevent the financial system from being exploited for illicit activities. Within the banking sector, deficiencies in AML implementation are widely recognized as a significant form of operational risk. Such vulnerabilities often stem from lapses in internal controls, governance, or compliance mechanisms – core elements within ORM structures.

The Financial Action Task Force (FATF) plays a leading role in formulating international benchmarks to counter money laundering, terrorist financing, and the financing of weapons proliferation. While FATF's primary focus is AML/CFT compliance, its recommendations inherently align with operational risk principles by emphasizing the need for strong internal governance, procedural integrity, technological safeguards, and resilience to external threats – all consistent with the Basel-defined categories of operational risk. FATF's 40 recommendations, most recently revised in 2023, require financial institutions to implement a Risk-Based Approach (RBA) to AML/CFT compliance. This approach closely mirrors ORM practices by mandating tailored risk assessments, continuous monitoring, and control mechanisms proportionate to the nature and complexity of risks faced by institutions.

2.2.7 Governance and Practices of ORM in Islamic Banks

Operational risk – defined by the Basel Committee as the risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events – is a critical component of the overall risk management framework in any financial institution, including Islamic banks. Similarly, the Islamic Financial Services Board (IFSB) defines operational risk as the risk of losses resulting from inadequate or failed internal processes, people, and systems, or from external events, including but not limited to legal risk, cyber risk, and Shari'ah non-compliance risk (IFSB, 2021). In Islamic banks, operational risk is further nuanced by the requirement to comply with Shari'ah principles, making its governance both a technical and faith-based

[17] https://www.coso.org/guidance-erm

responsibility. As per IFSB, operational risk excludes strategic and reputational risks. This section of the paper examines the distinct governance structures, compliance obligations, and operational practices adopted by Islamic banks to manage operational risk effectively.

Shari'ah-Integrated Risk Governance Framework

Islamic banks operate under a dual-layer governance system: conventional regulatory oversight and Shari'ah governance. In addition to the Board of Directors, Senior Management Team (SMT), Risk Management Committees, and Internal and External Audit functions, Islamic banks maintain an independent Shari'ah Supervisory Committee (SSC) and conduct both internal and external Shari'ah audits. These organs play a pivotal role in ensuring that all operations, contracts, and risk mitigation strategies conform to Islamic principles. This duality adds significant value to the governance system of Islamic Financial Institutions (IFIs).

The governance of operational risk is typically embedded within the broader Enterprise Risk Management (ERM) framework. Islamic banks must ensure that operational risk governance not only aligns with Basel guidelines but also incorporates the Maqasid as-Shari'ah (Objectives of Islamic Law), which emphasize justice, transparency, and ethical conduct.

Unique Operational Risk Factors in Islamic Banks

Islamic banks face certain operational risks not typically encountered by conventional banks. One of the most critical is Shari'ah non-compliance risk – defined as the risk arising from an IFI's failure to comply with Shari'ah rules and principles as determined by the Shari'ah Board of the IFI or the relevant body within the jurisdiction (IFSB, 2005). Any transaction or product that deviates from Shari'ah principles can result in reputational damage, financial loss, and regulatory penalties.
Islamic financial contracts (e.g., Mudarabah, Murabahah, Ijarah) often involve multi-step processes and detailed documentation, which increases the likelihood of human error and process failure. Moreover, a lack of global consensus on Shari'ah interpretations can lead to inconsistencies in product implementation and control mechanisms across jurisdictions. Additionally, a shortage of personnel with dual expertise in both banking and Shari'ah can contribute to operational inefficiencies.

ORM Practices in Islamic Banks

Islamic banks employ several strategies to manage operational risks, many of which are tailored to the needs of a faith-based financial system. Mitigating operational risk – particularly Shari'ah non-compliance – is crucial. If a transaction is found to be non-compliant, the entire revenue earned from that transaction must be excluded from the bank's earnings, even if detected years later. Therefore, the Internal Control System

(ICS) must be comprehensive, enabling the identification, assessment, monitoring, and mitigation of operational risks, with strong emphasis on process audits and ethical standards.

In addition to conventional audits, Islamic banks also conduct Shari'ah audits to assess compliance with Islamic principles. The Core Banking System (CBS) must be customized to accommodate Islamic finance transactions and automate compliance checks, reducing human error and ensuring process integrity. Regular training programs on ORM and Shari'ah compliance are necessary to foster a risk-aware culture within the institution. Moreover, systematic tracking of operational risk incidents and the maintenance of risk registers support the early detection and prevention of recurring issues.

Role of Regulators and Industry Standards

Standard-setting bodies such as the Islamic Financial Services Board (IFSB)[18] and the Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI)[19] issue guidelines on ORM and governance practices for IFIs. According to the IFSB, supervisory authorities should have a sound understanding of the diverse risks undertaken by IFIs and ensure that adequate risk management and reporting systems are in place (IFSB 2005). These authorities should also develop prudential guidelines for managing these risks. AAOIFI has issued several governance standards. In Bangladesh, the central bank has issued specific guidelines for both full-fledged Islamic banks and Islamic banking windows. These include instructions on reporting lines, Shari'ah board responsibilities, etc. However, Bangladesh Bank has not directly adopted IFSB or AAOIFI standards.

Effective ORM in Islamic banks requires an integrated approach that aligns global best practices with Shari'ah compliance mandates. Governance structures must support accountability, transparency, and robust audit systems. As the Islamic banking sector grows in scale and complexity, enhancements in automation, standardized procedures, and continuous capacity building will be essential for bolstering operational resilience and maintaining stakeholder trust. Ultimately, robust operational risk governance not only safeguards Islamic banks from losses but also ensures that the ethical and social objectives of Islamic finance are upheld. To promote sustainability and stakeholder confidence, the central bank may consider structuring prudential regulations in closer alignment with IFSB and AAOIFI standards.

[18] https://www.ifsb.org/wp-content/uploads/2023/10/ED-30_En.pdf

[19] AAOIFI Governance Standard No. 1 (GSIFI 1), titled 'Shariah Supervisory Board: Appointment, Composition and Report' (aaoifi.com/aaoifi-gs-1)

3. ORM Framework and Practices in Banks: Global Context

As operational risk has gained prominence, both global regulators and banks have strengthened their ORM frameworks. International standards – such as those from Basel – alongside national regulatory contexts, have significantly influenced these developments. Banks are now expected to proactively identify emerging risks, conduct cost–benefit analyses, minimize avoidable exposures, and delegate strategic risk planning to senior management (Segal, 2024). Although ORM tools and frameworks continue to evolve, several core practices have been widely accepted by the industry and endorsed by regulators. These can be grouped into five key stages of an ORM framework: Risk Identification, Risk Assessment, Monitoring & Reporting, Mitigation & Control, and Business Continuity & Resilience. Regulatory oversight plays a critical role in enforcing and supporting these components (Box 3.1).

Box 3.1: Operational Risk Management Framework & Tools	
I. Operational Risk Management: Banks' Approach	
Operational Risk Identification	Risk Control and Self-Assessment
	Collection and Analyses of Internal Operational Loss Data
	Review of External Loss Data and Industry Events
	Operational Risk Workshops for Business Process Mapping
Operational Risk Assessment	Scoring, Rating, and Analysing Operational Risks
	Determining Key Risk Indicators (KRIs) for Operational Risks
	Scenario Analysis or Stress Testing
	Models for Regulatory Capital and Additional Capital
Monitoring and Reporting of Operational Risks	Dashboards for Monitoring and Early Warning
	Governance for Operational Risk Reports
	Incident Management and Escalation
	Internal Audit and Independent Monitoring
	Disclosure and Reporting to Regulators
Operational Risk Mitigation and Control	Effective Internal Controls
	Policies, Procedures, and Culture
	Improvement or Redesigning Process
	Insurance and Risk Transfer
	Contingency Planning
	Training and Awareness Programs for Employees and Clients
Business Resiliency and Continuity	Business Continuity Planning
	Incident Response and Crisis Management
	Operational Resilience Frameworks
	Third-Party and Cyber Resilience
	Testing and Adaptation

II. Operational Risk Management: Regulatory Approach	
Supervisory Mechanisms: Inspections, Audits & Risk-Based Supervision	On-site Inspections and Audits
	Risk-Based Supervision
	Off-site Monitoring and Reporting
	Supervisory Review of Internal Audits
Regulatory Framework for Operational Risk Management and National Regulation	
Internal Governance and Risk Reporting	Periodic Operational Risk Management Reports
	Incident and Loss Reporting
	Internal Control and Audit Standards
Enforcement Actions and Sanctions	Supervisory Directives and Drawing Attention
	Formal Enforcement Actions and Penalties
	License or Management Action
Technology in Monitoring ORM	

3.1 ORM: Banks' Approach

3.1.1 Operational Risk Identification

Operational Risk Identification is the founding job that needs to be recognized across all products, processes and departments. For this purpose, the key practices and tools include:

Risk Control and Self-Assessment: As part of this tool, the responsible banker (process owners) documents, and estimate frequency. Business units of banks are expected to periodically identify and categorize these risks. A Risk Taxonomy is required to Categorise these risks.[20] For example, a retail banking division of a bank identifies fraud in account opening, assesses its likelihood and impact, and records current controls (dual verification, KYC checks, etc.) as part of its Risk Control and Self-Assessment (auditboard.com).[21]

Collection and Analyses of Internal Operational Loss Data: Banks are expected to maintain a database of the operational loss events like processing errors, and fraud incidents with details of causes and financial resources involved. Data analyses of this information are very helpful in identifying recurring and habitual issues. Basel III framework encourages gathering at least five years of loss data for risk management and capital modeling (BCBS, 2021). For example, by analysing loss data, a bank identified a pattern of ATM cash reconciliation errors and identified a need for strengthening cash-handling procedures.

[20] To ensure comprehensive coverage, identified risks are often categorized under the standard Basel taxonomy of operational risk events.

[21] https://auditboard.com/blog/operational-risk-management

Review of External Loss Data and Industry Events: Banks are expected to review external loss events, databases such as the ORX[22] consortium data, for identifying risks that a bank or banks is/are exposed to. External events and industry situations may offer banks the due lessons to act on those. For example, the collapse of Barings Bank in 1995 warned banks globally of the risk of inadequate trade monitoring and the importance of the segregation of responsibilities.[23]

Operational Risk Workshops for Business Process Mapping: Banks are expected to conduct periodic workshops and interviews with frontline staff and risk experts to identify potential risks.[24] The mapping processes should cover spotting points of failure and vulnerabilities and categorize them by types and business lines in their Risk Register that may cause business losses for banks. This is more about identifying emerging operational risks. For example, in a workshop a bank realizes that simply installing banking software might bring in Operational Risk if data reconciliation and other supportive steps are not ensured.

3.1.2 Operational Risk Assessment

The identified and categorized operational risks need to be assessed to understand their severity and prioritize these concerns also called measurement and analyses of the identified risks. This involves analyzing the likelihood of occurrence and potential impacts including financial loss, customer harm, regulatory fines, etc for each Operational Risk. The methodology or tools used for these purposes include:

Scoring, Rating, and Analysing Operational Risks: A Scoring System or Heat Map may be used by the banks for scoring and rating the Operational Risk to understand their severity and priority to act. Numbers may be used for scoring, or there are practices of using terms like 'Low', 'Medium' 'High' for frequencies and impacts of incidences. For example, a risk of data entry error in loan processing might be rated 'medium frequency &low impact', whereas a risk of a major payment system outage could be 'low frequency & high impact'. The assessed information may also be placed in a diagram or Heat Map with red, amber, and green zones to help management focus on top operational risk areas. Quantitative statistical analysis of loss data (internal and external) helps in assessing how severe certain risks can be, and the associated potential impact for the bank.

[22] ORX is built on a platform of sharing and working together; through ORX, our community shares insights, knowledge and data, developing best practice (https://orx.org/about-us).

[23] https://www.fia.org/marketvoice/articles/25-years-ago-barings-offers-hard-lesson-risk-control

[24] https://auditboard.com/blog/operational-risk-management

Determining Key Risk Indicators (KRIs) for Operational Risks: Banks are encouraged to use KRIs to quantitatively assess and monitor Operational Risk over time. Using KRIs are metrics that serve as early warning signals of increasing risk exposure. In the assessment stage, banks are expected to determine appropriate KRIs for major risks and set thresholds. For instance, a bank might track the number of failed login attempts as a KRI for cyber-intrusion risk. KRIs are linked to risk appetite, for example, if a threshold is breached (such as a spike in ATM outages beyond a set number), it signals heightened risk requiring attention (Segal, 2024).

Scenario Analysis or Stress Testing: Scenario analysis is a systematic process where banks imagine severe but plausible operational risk events and estimate their impact. This is particularly useful for low-frequency, high-impact risks that may not be in historical data. Scenario analysis is a valuable risk management tool and is linked to operational resilience planning. For example, a bank might assess a scenario of a major earthquake hitting its headquarters or a scenario of a cloud service provider outage lasting 5 days. Experts from business lines and risk management come together to evaluate how such scenarios would play out, estimate financial losses, and identify weaknesses (Dominic Wu, 2012).

Models for Regulatory Capital and Additional Capital: Capital holding by banks is the cushion for higher level of banking and other risks. In essence, banks with higher operational losses in the past will be required to hold more capital going forward.[25] Banks need to identify and determine models to ensure adequate capital to meet regulatory requirements and also to check the requirement of additional capital for higher or growing operational risks in banks.

3.1.3 Operational Risk Monitoring and Reporting

This is about continuous monitoring reporting arrangements for tracking risk indicators, auditing controls, and informing board and policymakers or regulators about the risk profile. The common tools used for the purpose include:

Dashboards for Monitoring and Early Warning: The KRIs with their thresholds or trigger levels need monitoring to draw signals of increasing risks, if any. These KRIs are often aggregated into operational risk dashboards or scorecards, which are reviewed by senior management and risk committees. A well-designed KRI framework and Dashboard act as an early warning system.[26] For instance, one Asian bank noticed its ATM uptime KRI dropping below 95% (target) to 90% in one region, indicating frequent outages. This prompted an investigation that discovered a power

[25]https://www.moodys.com/web/en/us/insights/regulatory-news/eba-proposes-operational-risk-standards-under-final-basel-iii-package.html

[26] https://auditboard.com/blog/operational-risk-management

supply issue at a local vendor – an issue that was fixed before it could cause more serious cash outages (Segal, 2024).

Governance for Operational Risk Reports: Banks are expected to have regular reporting routines. Business units report their risk and loss incidents on a monthly or quarterly basis to a central operational risk function (Institute of International Finance, 2015). Consolidated reports then go to the bank's Operational Risk Committee (often a sub-committee of the enterprise risk management committee) and ultimately to the Board's Risk Committee. These reports include summaries of top risks, KRI outliers, details of significant incidents that occurred, status of mitigation actions, and trending analysis (BCBS, 2021).

Incident Management and Escalation: Banks are expected to establish incident response procedures for different types of operational events like a fraud response team. When incidents happen, they are logged and classified. 'Near-misses', events that almost caused a loss, are also tracked as they are valuable risk signals. A culture of reporting even minor incidents or near misses without fear of blame is considered a mark of a mature risk culture. For significant incidents, internal escalation to senior management is required, and in many jurisdictions, external reporting to regulators is mandated (BCBS, 2021).

Internal Audit and Independent Monitoring: Audit findings often highlight control weaknesses that management must address. The audit can also validate that 'Risk Control and Self-Assessment' are accurate and that KRIs are reliable. While business lines and the risk management function monitor day-to-day controls (the first and second lines of defense), Internal Audit (third line) provides independent assurance through periodic audits. For example, an internal audit might test a sample of transactions in a trading operation to ensure that all trades are confirmed by the back-office; any exceptions would be reported as issues to be fixed, thus feeding back into risk mitigation (Institute of Internal Auditors, 2013).

Disclosure and Reporting to Regulators: Under Basel's Pillar 3 disclosure requirements, banks publicly disclose their ORM approach and certain data, such as the operational risk capital number, and sometimes a qualitative discussion of major loss events and improvements (BCBS, 2015). Beyond that, regulators often require immediate notification of major operational incidents. For example, adopted in 2022 in the US, regulators have a 36-hour notification rule for significant cybersecurity

incidents at banks. These reporting rules force banks to have robust monitoring to even know when a threshold is breached and an incident becomes reportable.[27]

3.1.4 Operational Risk Mitigation and Control

Mitigation and Control are about building a robust internal control environment, improving processes, and preparing risk minimization strategies. The techniques:

Effective Internal Controls: The primary way to mitigate operational risks is through effective internal controls. Controls can be preventive (aimed at stopping an error or fraud before it happens, e.g. segregation of duties, approval checks) or detective (aimed at finding issues quickly if they occur, e.g. KRI breaches. For each significant risk identified, banks ensure that appropriate controls are in place (COSO, 2013). For instance, to mitigate the risk of trade financing, a bank is expected to enforce segregation of duties between business and compliance. Controls should be regularly tested (as part of monitoring) and updated if found weak.

Policies, Procedures, and Culture: Operational Risk Mitigation involves having clear policies (e.g., an operational risk management policy, business continuity policy, information security policy) and detailed procedures for key operations (BCBS, 2021). Well-documented procedures act as controls by reducing reliance on individual knowledge and ensuring consistency. For example, a documented procedure for processing wire transfers that includes verification steps can prevent costly mistakes or fraud. A strong risk culture encourages employees to follow these procedures and not circumvent controls in the name of convenience or short-term profit (Financial Stability Board, 2014).

Improvement or Redesigning Process: Sometimes the best mitigation is to redesign a process to eliminate risks (BCBS, 2021). This could mean automating a manual process (to reduce human error), adding duplicate systems (to reduce single points of failure), or simplifying a complex procedure. Banks often undertake Operational Risk Assessments for new products or major process changes These assessments aim to build controls into the product/process before launch (COSO, 2013). For example, when a bank launched mobile banking, it likely built in mitigations like two-factor authentication and transaction limits to control fraud risk.

Insurance and Risk Transfer: For certain residual risks that cannot be fully controlled, banks use insurance as a risk mitigation tool. Banks commonly purchase cyber insurance, fidelity insurance, etc., to transfer some of the financial impacts of events like fraud, cyber-attacks, or physical damage. While insurance does not prevent

[27] *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Provider;* Final Rule, effective May 1, 2022: https://www.fdic.gov/news/press-releases/2021/pr21107.html

the event, it mitigates loss impact. Under Basel rules, certain insurance coverage could even be recognized to reduce operational risk capital (though with strict criteria). For example, a bank might insure against cash-in-transit robberies or ATM theft – if such an event happens, the insurance pay-out offsets the loss (BCBS, 2011).

Contingency Planning: Mitigation overlaps somewhat with business continuity in that having contingency plans (like backup systems, alternate staff for critical roles, etc.) can mitigate the impact of certain risks (BCBS, 2021a). For instance, the risk of a key data center outage is mitigated by having a secondary data center that can take over. Similarly, to mitigate the risk of losing key personnel (a people risk), banks implement succession planning and cross-training.

Training and Awareness Programs for Employees and Clients: Training and awareness are critical components of an effective operational risk management framework. By ensuring that staff at all levels understand risk policies, procedures, and the importance of control adherence, banks can significantly reduce the likelihood of human error, fraud, and process failures (BCBS, 2021). The training and awareness component may include, induction and refresher training on operational risk policies and controls; targeted training for high-risk roles; scenario-based learning to help staff recognize and react to operational threats; promoting a risk-aware culture where employees are encouraged to report issues and near misses, etc. (Institute of Operational Risk, 2010). While most operational risk management strategies focus on internal controls and staff training, banks are increasingly recognizing the importance of client awareness training as a frontline defense against certain types of operational risks-particularly those related to cybersecurity, fraud, and process errors.

3.1.5 Business Resilience and Continuity Planning

Business resilience and continuity measures are designed to enable banks to sustain essential functions and recover swiftly during operational disruptions, thereby limiting potential losses and operational setbacks.

Business Continuity Planning (BCP): Banks are expected to maintain detailed BCPs that outline how operations will be kept running in various disaster scenarios (pandemic, IT failure, building inaccessible, etc.). These plans identify critical business functions and resources needed to support them (systems, staff, data backups, alternate sites). BCPs are living documents that must be updated and tested regularly (ISO, 2019). In several instances, regulators require annual (or more frequent) BCP testing, for instance, a common test is a fire drill (BCBS, 2021a).

Incident Response and Crisis Management: Beyond pre-planned continuity steps, banks have crisis management teams and playbooks. These define how to manage the immediate aftermath of a major operational crisis. During the COVID-19 outbreak in 2020, several banks activated their crisis management teams to handle the sudden need for mass remote work and branch closures, and thus many were able to transition to remote operations with limited service disruption (Financial Stability Board, 2020).

Operational Resilience Frameworks: In recent years, the concept of operational resilience has emerged, expanding on traditional BCP, which is about Operational Resilience to build the ability to absorb shocks and continue providing services even in extreme scenarios. The Basel Committee's 2021 Principles for Operational Resilience and similar rules in the UK and EU formalize this (BCBS, 2021a; Bank of England, 2021). Key aspects include identifying a bank's important business services and setting impact tolerances, defining how much disruption can be tolerated (e.g., no more than 4 hours of outage for online banking). Banks must then ensure they can stay within these tolerances under severe but plausible scenarios.

Third-Party and Cyber Resilience: Business continuity now must address risks arising from third-party service providers and cyber threats. Regulators may require robust resilience testing by banks.[28] Banks perform due diligence on critical vendors' BCP capabilities, often requiring them to attest to recovery times and to participate in joint testing. Cyber resilience, a hot topic, involves capabilities like data backup isolation, network segmentation, and cyber range exercises. A resilient bank may have offline backups of critical data that cannot be corrupted by a cyber-attack and will rehearse recovering from a cyber incident scenario.

Testing and Adaptation: Banks are expected to conduct regular BCP drills and scenario simulations, and after each test or actual incident, lessons learned need to be documented and plans updated. In several instances, regulators expect banks to review incidents and incorporate those lessons (PwC, 2024).

3.2 Operational Risk Management: Regulatory and Supervisory Approach

For enforcing sound ORM, regulators employ a combination of supervisory mechanisms, regulatory frameworks, enforcement actions, and reporting requirements, increasingly augmented by technology. These tools are applied in both developed and developing countries, guided by international standards (like Basel guidelines) but tailored to the local contexts. Today, regulators are not expected to

[28] Regulations like DORA (Digital Operational Resilience Act 2022/2554) explicitly require robust ICT third-party risk management and resilience testing (https://www.digital-operational-resilience-act.com).

consider these only as compliance tools, but rather as strategic forces for sustainable banking operations.

3.2.1 Supervisory Mechanisms: Inspections, Audits & Risk-Based Supervision

On-site Inspections and Audits: These are traditional tools used by regulators and supervisors worldwide to evaluate a bank's internal controls and risk management mechanisms. Examiners conduct in-depth reviews of operational processes, often checking compliance with ORM policies, the resilience of IT systems, and the effectiveness of internal audits (BCBS, 2012). In developed markets (e.g. U.S., UK), large banks undergo regular safety-and-soundness examinations that include assessments of Operational Risk Management frameworks. In developing countries, supervisors have similarly adopted on-site examinations, sometimes with aid from international bodies to build capacity (IMF, 2019).

Risk-Based Supervision: Modern supervision emphasizes a risk-focused approach rather than one-size compliance. Under RBS, supervisory resources are allocated based on each bank's risk profile and systemic importance. This approach is embedded in the Basel Core Principles, which require supervisors to maintain a forward-looking assessment of banks' risks and use a proportionate range of techniques to monitor and address those risks Under RBS, higher-risk areas (like weak operational controls or rapid fintech adoption) receive closer scrutiny, and well-managed banks may face reduced inspection frequency (Melo et.al, 2024).

Off-site Monitoring and Reporting: Supervisors continuously monitor banks via required reports. The Basel Core Principles underscore that supervisors must collect and review regular prudential reports from banks, and verify them through on-site exams or external experts. In practice, banks must submit periodic risk reports, loss event reports, audit findings, etc., which regulators analyze for signs of operational risk issues (BCBS, 2024). For instance, India's RBI requires banks to report major frauds and operational loss events into centralized databases, enabling off-site analysis of trends.[29] Brazil's Central Bank (BACEN), mandates that banks maintain an internal operational risk loss database and include information on significant losses in management reports to the supervisor.[30] Such data-driven surveillance helps flag outliers or deteriorating Operational Risk Management practices between inspections. Regulators now require banks to monitor and report on third-party risks – if a critical service provider (cloud vendor, payment processor) has an outage or issue, the bank must capture and escalate that as it could indicate concentration risk (PwC, 2024).

[29] Reserve Bank of India (2021) Master Directions on Frauds-Classification and Reporting by commercial banks and select FIs: https://www.rbi.org.in

[30] https://www.bcb.gov.br/ingles/norms/brprudential/Resolution4557.pdf

Supervisory Review of Internal Audits: Several regulators treat a bank's internal audit and control functions as extensions of supervision (ECB, 2020). During inspections, they evaluate whether internal audit independently tests operational controls and if identified issues are promptly fixed. In some cases, supervisors can require external audits or independent reviews of specific operational risk areas (e.g. IT systems, fraud controls) if they lack confidence in the bank's own audit. This ensures an extra layer of assurance on Operational Risk Management in both advanced and emerging markets (BSBS, 2021a).

3.2.2 International Regulatory Framework and National-Level Regulation for ORM

The Basel Framework forms the global foundation for regulatory standards on ORM, which national regulators adapt into enforceable policies. Central banks and supervisory authorities implement Basel principles through local rules, guidelines, and supervisory expectations tailored to their jurisdictions.

In the European Union, Basel-aligned regulations are codified into law, requiring banks to maintain comprehensive governance and risk management systems that cover all significant risks, including operational ones. The UK's Prudential Regulation Authority (PRA) has supplemented traditional ORM with operational resilience mandates, compelling firms to identify critical business services, define impact tolerances, and ensure continuity under stress scenarios (Bank of England, 2021).

In the U.S., agencies such as the Federal Reserve, OCC, and FDIC embed ORM into supervisory frameworks, emphasizing governance, internal controls, and data integrity for systemically important institutions. Brazil, similarly, requires banks to adopt proportionate, integrated risk management systems that include operational risk components – such as incident databases, scenario planning, and structured governance mechanisms – aligned with Basel's definition.

Across jurisdictions, regulators require banks to formalize ORM frameworks, maintain policy documentation, implement risk identification and reporting systems, and establish robust business continuity planning – all subject to continuous supervisory oversight.

3.2.3 Internal Governance and Risk Reporting

Internal governance is the key to effective ORM in banks. Regulators generally require that a bank's Board of Directors and senior management take ultimate responsibility for managing operational risk. This is often formalized in guidelines. Banks must establish independent risk management functions (often led by a Chief

Risk Officer), as well as internal control units and compliance teams, to provide checks and balances. Risk reporting requirements are another crucial enforcement tool. Supervisors oblige banks to regularly report on their risk profile and exposures, ensuring transparency and enabling off-site monitoring. The reporting tools commonly include:

Periodic ORM Reports: Banks often must submit quarterly or annual operational risk assessments to the regulator, summarizing key risk indicators, loss events, and control issues. For example, in Brazil, management reports to the board (and available to the Central Bank) must include information on relevant operational losses.[31] These reports allow supervisors to verify that banks are actively managing op risk and to compare peer metrics (e.g. loss rates).

Incident and Loss Reporting: Many central banks require prompt notification of major operational risk incidents (such as significant frauds, cyber breaches, or system outages). For instance, RBI has long required banks to report all fraud cases above a threshold to the central bank's database, which feeds into supervisory assessments.[32] Such reporting enables regulators to ensure issues are being addressed and to possibly warn other banks of emerging threats. In Brazil's regulations, banks must 'timely collect relevant information to be included in the operational risk database; classify and aggregate material operational losses; and assess root causes' for each major loss– an implicit reporting and review expectation.[33]

Internal Control and Audit Standards: Regulators expect banks to maintain a sound internal control environment as part of ORM.[34] Supervisors sometimes offer standards for internal control and audit. Many regulators require banks to adhere to frameworks akin to COSO's internal control principles. Basel's Core Principles explicitly require that supervisors determine if banks have adequate internal control frameworks and independent internal audit covering all operations (Melo et. al., 2024). In practice, during inspections, supervisors are expected to evaluate if a bank's internal controls (e.g. dual controls, reconciliations, business continuity plans) are sound (Melo et. al., 2024a).

[31] Banco Central do Brazil (2017) Resolution No. 4,557-Risk Management Framework: https://www.bcb.gov.br

[32] Reserve Bank of India (2021) Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs. Retrieved from https://www.rbi.org.in

[33] Banco Central do Brazil (2017) Resolution No. 4,557- Risk Management Framework: https://www.bcb.gov.br

[34] https://www.fia.org/marketvoice/articles/25-years-ago-barings-offers-hard-lesson-risk-controls

3.2.4 Enforcement Actions and Sanctions

Central banks and regulators have an array of enforcement powers to ensure compliance with ORM standards. When supervisors identify serious deficiencies in a bank's operational risk management, they can act ranging from informal warnings to harsh penalties.

Supervisory Directives and Drawing Attention: For certain issues, banks are often given supervisory recommendations or requirements to fix problems by a deadline. For instance, after an inspection, a regulator might require a bank to strengthen its IT security controls or improve vendor risk management, tracking progress in subsequent visits.

Formal Enforcement Actions and Penalties: In more severe cases, regulators are expected to issue formal enforcement actions covering cease and desist orders, monetary penalties, restrictions on activities, or even license revocation in extreme cases. Developed countries have seen high-profile penalties for operational risk failures.[35] These examples of fines show that enforcement is not limited to fraud or compliance issues; pure operational lapses (IT failures, internal control breakdowns) also attract sanctions in developed markets. According to the World Bank's Bank Regulation and Supervision Survey (2020), many developing country supervisors now have legal authority to impose financial penalties, though practical enforcement varies based on resource constraints and the maturity of the supervisory regime.

License or Management Action: Banking supervisors can ultimately threaten a bank's license or management if risk deficiencies endanger safety and soundness. Basel Core Principle 11 affirms that supervisors should have a 'range of tools' and the ability to take timely corrective actions, up to revoking a banking license for serious unresolved risk management (IMF, 2021). In practice, such extreme measures are rare, but there have been cases in developing countries where banks with egregious operational failures (World Bank, 2020).

3.2.5 Technology in Monitoring ORM

Central banks and financial regulators are increasingly adopting RegTech (Regulatory Technology) and SupTech (Supervisory Technology) to strengthen the monitoring and enforcement of operational risk management. These technologies enable regulators to automate data collection, conduct advanced analytics, and gain real-time

[35] OCC imposed a USD400 million fine on Citibank for enterprise-wide risk management and data governance failures, and mandated extensive corrective actions with ongoing oversight. In the UK, regulators penalized TSB Bank GBP48.65 million in 2022 for operational risk management and governance failures that led to a major IT outage during a 2018 IT migration that disrupted services for millions of customers.

insights into risk exposures. According to the BIS, SupTech tools are now widely used across jurisdictions to support supervisory functions related to credit, market, liquidity, and operational risks (BIS-FSI, 2020). For example, the U.S. Federal Reserve has invested in big-data capabilities that integrate inputs from internal bank systems, loss event databases, and even public sources to monitor the operational risk profiles of large financial institutions continuously (Federal Reserve, 2021).

The Monetary Authority of Singapore (MAS) has pioneered the use of machine learning algorithms to analyze transactional data for early detection of fraud and money laundering risks (MAS, 2022). Similarly, in developing countries, the Reserve Bank of India's Central Repository of Information on Large Credits (CRILC) originally developed for credit risk monitoring has inspired centralized platforms for fraud and cyber incident reporting. In Nigeria, the Central Bank of Nigeria (CBN) has developed a web-based regulatory portal where banks submit structured risk returns, including operational risk data, which feeds into a supervisory scoring model (CBN, 2021).

While the adoption of SupTech improves regulatory efficiency, timeliness, and data-driven enforcement, it also introduces new supervisory challenges, such as data privacy risks, model governance, and systemic dependence on digital infrastructure. Nevertheless, the integration of advanced technology is seen as essential for regulators to cope with the increasing complexity of operational risk, particularly in the context of cybersecurity threats, digital banking, and fintech innovations.

4. Governance and Practices of ORM in the Banking Industry of Bangladesh

ORM in developing countries remains a critical yet often underdeveloped area of financial sector governance. Despite the global shift toward integrated risk-based frameworks, many developing economies continue to struggle with weak internal controls, limited automation, understaffed compliance units, and inadequate regulatory enforcement. In countries like Bangladesh, where financial inclusion is expanding rapidly through digital platforms and agent banking, the risk landscape is evolving faster than the institutional capacity to manage it. As operational failures ranging from system outages to AML control lapses pose systemic threats to financial stability, it becomes crucial to unearth the true status and nature of ORM in the country. A deeper understanding is essential not only to inform policy reforms and supervisory practices but also to strengthen institutional resilience in line with global standards.

4.1 Regulatory Landscape for ORM in Bangladesh

Bangladesh lacks a dedicated standalone guideline on Operational Risk Management (ORM); instead, relevant directives are embedded across various regulatory documents issued by Bangladesh Bank.

Risk Management Guidelines (2012, updated 2018)[36]

These guidelines introduced ORM as a distinct risk category, requiring banks to establish internal frameworks and assign responsibilities for risk identification, reporting, and mitigation. However, it lacks standardized formats for loss reporting or mitigation checklists.

Risk-Based Capital Adequacy (RBCA) Guidelines[37]

RBCA has helped raise awareness of ORM by defining operational risk and establishing a capital charge framework. Banks follow the Basic Indicator Approach, maintaining capital equal to 15% of average gross income over last three years.

Internal Control and Compliance (ICC) Guidelines[38]

ICC guidelines provide structural requirements and tools for managing operational risk through compliance, monitoring, and audit. Instruments like the Departmental Control Function Checklist (DCFCL)[39], Quarterly Operations Report (QOR)[40], and Loan Documentation Checklist (LDCL)[41] are emphasized, alongside risk-based internal audits.

Self-Assessment of Anti-Fraud Controls[42]

This tool includes 80 control-check questions and a reporting format for fraud incidents. Quarterly reports, signed by the ICC head and CEO, are submitted to the central bank to enhance fraud oversight.

[36] Bangladesh Bank has issued this guideline through DOS Circular No. 4 dated October 08, 2018.

[37] Bangladesh Bank has issued this guideline through BRPD Circular No. 18, dated December 21, 2014.

[38] Bangladesh Bank has issued this guideline through BRPD circular no.03 dated March 08, 2016.

[39] DCFCL is a comprehensive list of activities to be carried out daily, weekly, monthly and quarterly by the designated officers to ensure smooth functioning of the internal controls placed in different business lines.

[40] Quarterly operations report is used to report issues related to policies, procedures, controls, protection of valuables, premises management, operational losses etc.

[41] It is a comprehensive list of documents to be obtained or created before disbursement of loans to a borrower.

[42] This document has been issued by Bangladesh bank through DOS circular letter no 17 dated November 7, 2012

Guidance on Anti-Money Laundering (AML)[43]

Includes organizational structure for AML activities, KYC forms, and suspicious transaction formats. Each branch must appoint an AMLCO, who reports to the CAMLCO at the head office and ultimately to the CEO.

Guidelines on Trade-Based Money Laundering (TBML)[44]

Issued by BFIU to address process failures in trade finance, the guidelines offer measures for due diligence and institutional vigilance to mitigate TBML risks.

ICT Security Guidelines (v4.0)[45]

These guidelines address risks from IT failures by covering security management, operations, software acquisition, disaster recovery, and vendor oversight.

Training, Job Rotation, and Mandatory Leave

Guidelines under ICC stress training, rotation, and mandatory leave as part of compliance and fraud prevention. Specialized departments like risk or treasury are exempt from rotation requirements.

Other Relevant Directives

Additional policies—including credit, foreign exchange, and asset-liability risk guidelines, Mobile Financial Services regulations, and deposit insurance schemes—complement ORM efforts, particularly at the business-line level.

4.2 ORM Practices in Banks in Bangladesh: Survey Findings

Secondary data on Operational Risk Management practices in the context of the banking industry of Bangladesh are scanty. The study attempts to capture the status and the associated challenges of ORM in banks through a Questionnaire survey, KIIs, and an FGD to reflect governance and practices of ORM in Bangladesh.

4.2.1 Industry Governance and Practices [Opinion Survey]: Outcomes of KIIs

As a subset of ERM, ORM should be integrated with ERM, and banks are expected to have a standalone ORM unit. The KII (opinion survey) of the expert bankers (Head/Deputy Head of Risk Management) reflects that only 30% banks of in the country have standalone ORM units, and 24% have an integrated arrangement with ERM. Over one-fourth of the banks do not have a formal Operational Risk Management governance framework, as opined (Table 4.1).

[43] Bangladesh Bank has issued this guideline through BRPD circular no.17 dated September 16, 2012.

[44] Bangladesh Financial Intelligence Unit (BFIU) has issued this guideline on 2019.

[45] Bangladesh Bank has issued this guideline through BRPD Circular No. 10, dated June 19, 2023.

Table 4.1: Governance Structure of Operational Risk Management in Banks	
	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%]

Source: *KII*

Accordong to the survey data, only 30% of banks conduct a regular review at the Board Risk Committee level. This indicates a gap in strategic risk oversight, suggesting that operational risk may not be fully integrated into the highest governance frameworks in many banks. A significant portion of banks reported ORM oversight as not applicable, possibly reflecting lack of formal governance structures, or exclusion of ORM from senior-level review altogether (Table 4.2).

Table 4.2: Board and Senior Management Oversight on ORM Practices in Banks	
	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%]

Source: *KII*

Only 17% banks fully implemented Three Lines of Defense, indicates limited maturity in comprehensive risk governance. The data shows that a majority of banks have incomplete or informal adoption of the Three Lines of Defence model, signaling the need for formalization, to strengthen risk oversight (Table 4.3).

Table 4.3: Implementation of Three Lines of Defence Model in Banks	
	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%]

Source: *KII*

Survey data reveal Internal audit (60%) dominate as the primary tool, indicating a reactive and compliance-driven approach. Risk control by business units (27%) and KRIs (22%) are underused, suggesting weak proactive risk ownership and limited use of early warning indicators. Incident/loss event reviews (16%) are least used, pointing to insufficient access or absence of the recording of past events or data (Table 4.4). Banks rely heavily on audits over proactive tools, revealing a gap in forward-looking risk identification practices.

Table 4.4: Primary Tools and Methods Used to Identify Operational Risks in Banks	
	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%]

Source: *KII*

Table 4.5 shows, 50% align with local regulations, reflecting compliance-driven practices. While most banks show some form of alignment, full Basel compliance remains limited, and a third lag behind, highlighting the need for stronger regulatory integration.

Table 4.5: Banks ORM Aligned with Regulatory Frameworks	
	Industry Survey (Opinion)
Fully aligned with Basel	40% [10%-70%]
Aligned with Local Regulation	50% [15%-100%]
Limited Alignment	30.5% [5%-50%]
Not Aligned	2.5% [5%-50%]

Source: *KII*

The data reveals that robust loss data management is lacking, undermining effective risk analysis and regulatory compliance. Only 20% use a centralized and regularly updated system; and 30% rely on periodic departmental consolidation, showing fragmented data practices. Of the banks, 25% do not formally maintain data, highlighting significant weaknesses in loss data governance (Table 4.6).

Table 4.6: Internal Loss Event/Incident Data Collected and Managed in Banks	
	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%]

Source: *KII*

Scenario analysis remains inconsistently applied, with most banks lacking structured, enterprise-wide practices essential for anticipating operational risks. Only 23% conduct it across all business lines, indicating limited comprehensive risk preparedness. Of the banks, 18% do not conduct it at all, reflecting a critical gap in forward-looking risk management (Table 4.7).

Table 4.7: Conducting Scenario Analyses in Banks	
	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%]

Source: *KII*

The data (Table 4.8) reveals that methodological gaps, data limitations, and lack of expertise are major barriers to effective scenario analysis in banks. Lack of standardized methodology (39%) is the top challenge, indicating inconsistencies in approach across banks; and limited historical data (37%) highlights data gaps, making risk projection difficult, as opined.

Table 4.8: Challenges of Conducting Scenario Analyses in Banks	
	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%]

Source: *KII*

Operational risk monitoring (Table 4.9) remains largely audit-dependent, with insufficient adoption of proactive, standardized tools. Of the banks, 57% rely on internal audit/compliance, indicating a reactive oversight model; and only 28% use standardized dashboards and KRIs, showing limited real-time, data-driven monitoring, as opined.

Table 4.9: Monitoring Operational Risk Across Department/Branches in Banks	
	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%]

Source: *KII*

Banks prioritize a few key KRIs. Fraud incidents (40%) top the list, showing focus on financial crime detection. System/IT failures (27%) and staff turnover (30%) reflect attention to operational and human resource risks. Low use of loss even frequency (15%) and media reports (2%) signals limited holistic and reputational risk tracking (Table 4.10).

Table 4.10: Key KRIs used in Banks	
	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%
Note: Survey with Head of Risk Management of Selected Banks	

Source: *KII*

Table 4.11 reveals, quarterly reporting (42%) is most common. Monthly reporting by 35% banks shows a stronger risk awareness and monitoring culture in some banks. While most banks report operational risk regularly, only a minority follow high-frequency reporting, highlighting scope for improving timeliness and responsiveness in ORM oversight.

Table 4.11: Frequency of ORM Reporting to Senior Management/Board in Banks	
	Industry Survey (Opinion)
Monthly	35% [10%-90%]
Quarterly	42% [10%-80%]
Semi-annually	15.5% [10%-40%]
As & when required	7.5% [5%-20%]

Source: *KII*

Data reflects, outsourcing-related operational risks are poorly managed in many banks, with a clear need for structured vendor risk frameworks. Only 35% have vendor risk assessment and monitoring, indicating limited proactive oversight. Of the banks, 29.5% have no framework, and 23.5% address it inconsistently – highlighting significant gaps in outsourcing risk management (Table 4.12).

Table 4.12: Managing Operational Risk of Outsourcing	
	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%]

Source: *KII*

Data show that cybersecurity is largely treated as an IT issue, with minimal cross-functional coordination, posing risks to enterprise-wide resilience. According to the opinion survey, 70% rely on the IT team, showing a technical, isolated approach. Only 3% involve all key units, indicating weak integration across functions. Low involvement of ORM (15%) and Internal Audit (12%) suggests limited risk governance and independent oversight (Table 4.13).

Table 4.13: Management of Cybersecurity Risk	
	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%]

Source: *KII*

Table 4.14 shows, 60% use training and communication, showing a basic awareness effort. Only 20% conduct risk culture assessments, and 15% link incentives to risk, indicating limited depth in cultural integration. Banks need further efforts to build ORM culture.

Table 4.14: Building ORM Culture and Awareness in Banks	
	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%]

Source: *KII*

According to the opinion survey, 50% use post-training assessments/surveys, showing a basic evaluation approach. Only 20% link training to performance or KRIs, indicating limited impact measurement. And, 30% rely on informal or no assessment, reflecting weak training accountability.Training effectiveness is not systematically measured in many banks, limiting its role in strengthening operational risk capabilities (Table 4.15).

Table 4.15: Assessment of Training Effectiveness	
	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: *KII*

It is to be noted here that high range of variation in survey responses indicates limited reliability in drawing consistent conclusions from the data. It may reflect heterogeneous adoption levels of ORM practices across institutions or lack of available information. This inconsistency also suggests absence of industry-wide standardization. And probably banks are at different stages of maturity, making generalizations difficult.

4.2.2 ORM Practices of Banks with Standalone ORM Units/Wings: Survey Outcome

Only a few banks in Bangladesh report having formal Enterprise Risk Management (ERM) strategies and separate Operational Risk Management (ORM) units. Among these, some demonstrate practices that could serve as benchmarks for the industry. However, ORM governance across the sector remains fragmented, with a lack of standardized structures and procedures.

In sound governance frameworks, ORM falls under the broader oversight of the Chief Risk Officer (CRO), who reports to the Board Risk Committee and oversees all major risk categories. In larger institutions, operational risk oversight is often delegated to a Head of ORM, a senior role tasked with developing ORM frameworks, managing incident reports, compiling loss data, conducting Risk and Control Self-Assessments (RCSA), monitoring Key Risk Indicators (KRIs), and leading scenario analysis. This role typically sits within the second line of defense, ensuring that first-line business units comply with established ORM policies. In mid-sized banks, the Head of ERM may oversee ORM functions, while in smaller banks, a single Head of Risk may cover all risk categories due to limited capacity.

In Bangladesh, it is rare to find a dedicated Head of Operational Risk. Inappropriately, some banks assign this role to the Head of Operations, despite their position being part of the first line of defense, which compromises segregation of duties. Survey results reveal widespread ambiguity around ORM responsibilities, reporting structures, and role accountability—even in banks that have established ORM units.

Nevertheless, 90% of surveyed banks indicated that ORM is subject to board-level monitoring. Common practices include formulating ORM policies and risk appetite statements, obtaining management feedback, reporting through the CRO or Head of Operations to the Board Risk Committee, reviewing internal audit findings via the Board Audit and Risk Committee, and presenting KRIs at the board level. Key monitoring tools reported by banks are summarized in Box 4.1.

Box 4.1: Management Monitoring System
• Risk Committee raises risk issues in Management Committee, ERMC. ICCD and RMD share findings with respective heads. Operational Risk issues are discussed in ORM Committee and ERMC. • DCFCL, QOR, ICCD Audit Reports, BB Inspection Reports, Customer Complaints are also considered. • Monitored through ICCD, IT Division, and Operations Division

Source: *Survey Data*

Early warring system is a critical tool for operational risk management. Banks claim to have early waring systems covering a number of indicators (Box 4.2). Three-fourth of the selected banks demanded to have approved threshold for each early warning indicators (survey data).

Box 4.2: Early Warning Indicators
• Risk Appetite, Risk Threshold, Risk Register, Management Action Trigger, Self-Risk Assessment, Risk Mapping, KRIs, Historical Data Analysis. • Fraud Risk, HR Risk, IT Risk, Credit Process, Compliance Risk, Loss Monitoring, DCFCL, QOR • Risk Reports/Indicators: regulatory non-compliance, limit breach, system downtime, customer complaints, media reports. • System Failure, Fake Note in ATM, Excess Cash, Suspense Entries, Unknown Mail, Unusual transactions.

Source: *Survey Data*

A significant number of banks in the country are offering agent banking services. These agents could be a significant source of operational risks. Banks are using several tools to manage operational risks associated with these agents (Box 4.3). These tools commonly include:

Box 4.3: Managing Operational Risks Associated with the Agent Banking
• The Bank's Agent Banking Department and a monitoring team of ICCD checks that the process is duly followed by Agent Banking. • Through implementing Risk & Control Self-Assessment, Key Risk Indicator, and Control Assurances tools for managing operational risk of Agent Banking operations. • A detailed Agent Banking Policy as well as Agent Banking Operational Guidelines for streamlining the agent banking operations carried out by our Bank with a view to managing the operational risks. Moreover, controlling their operation through setting different limits ensures a control environment. • Fully automated system-driven operation, thumb-based operation is installed to minimize the risks. The voucher and SMS will be generated after depositing the money into the respective account only. • Operational risk is actively managed through a structured and multi-layered risk management framework. It includes agent due diligence and selection, arranging training programs, technology and system controls, transaction monitoring and alerts, audit & surprise inspections, insurance coverage, complaint and incident management.

Source: *Survey Data*

Most banks draw services from outsources companies. These include different IT related services including hardware, software, networking etc. Of the sampled bank, 90% draw services from one or more outsourcing companies. However, only 30% of these banks claimed to have for Business Process Outsourcing. Banks use several techniques to manage third party risk in banks in Bangladesh (Box 4.4).

Box 4.4: Managing Risks Generated by the Outsourcing Providers
• Third-party risk is managed through a competitive process, service level agreement, annual performance evaluation, and compensation policy. • In case of engaging Business Process Outsourcing (BPO) providers, the bank enters into Service Level Agreements (SLAs) with the providers whereby different risk factors are pointed out and mitigation measures are put in place. • To minimize the risks, the bank shall hire those vendors who are competent to comply with the business requirements. Besides, vendors are to submit a third-party audit or risk assessment report whenever required by the Bank.

Source: *Survey Data*

Of the banks, 50% claimed to have Business Continuity Planning (BCP) that are approved by the board, and are taken care of by a number of departments. Key features of the BCP included in Box 4.5.

Box 4.5: Basic Features of Contingency Plans Related to Disaster Recovery and Business Continuity
• A disaster recovery and business continuity contingency plan fundamentally include a detailed risk assessment to identify potential threats, clearly defined roles and responsibilities for the response team, specific procedures for data backup and recovery, alternative communication strategies, documented steps for restoring critical business functions, and regular testing and updating protocols to ensure effectiveness in the face of disruptive events. • The contingency plans include different components including Disaster Recovery Site (DRS) for ensuring a secure and geographically separate backup facility for IT systems and data; Business Continuity Plan (BCP) covers all critical business functions and services (e.g., payments, core banking, ATM operations, and continuity of Shariah-compliant services). Moreover, a dedicated crisis management team is responsible for managing incident response. Data backup and recovery are done at regular intervals. Training and awareness campaigns emphasize emergency procedures and safety protocols, and regulatory compliance complies with Bangladesh Bank's IT and BCP guidelines. The bank updates its contingency plan regularly based on what it learns from real incidents and practice drills.

Source: *Survey Data*

4.2.3 Governance and Practices of ORM: Summary Findings of FGD

The interviews revealed a foundational concern: most other risks - such as credit or market risk – are often triggered by or rooted in operational risk. Despite this, risk governance is underdeveloped, and risk regulation frequently overshadows governance, which experts argue should be prioritized. A key weakness is the absence of a structured and comprehensive approach to managing operational risk components, including People, Processes, Systems, and External Events. In many banks, these elements are addressed inadequately or inconsistently, exposing institutions to compounding vulnerabilities.

One of the most pressing concerns highlighted was the lack of leadership and risk culture within banks. Operational risk management (ORM) often lacks strategic placement, as risk management officials are rarely promoted to the Chief Risk Officer (CRO) position. Instead, individuals from the Credit Risk Management (CRM) division - whose focus is primarily credit-related - are commonly assigned this critical role, undermining ORM's scope. The RMD (Risk Management Division), which should serve as the central authority on operational risk, is frequently misunderstood or undervalued by boards and senior executives. This results in insufficient deployment of skilled manpower and poorly defined mandates across institutions.

While policies related to operational risk do exist in most banks, they often lack follow-through and structured enforcement. Risk appetite for operational risk is generally articulated as a single line in policy documents, without detailed parameters or strategic integration, leading to vague application and inefficient risk allocation. Business proposals, when reviewed by RMDs, sometimes utilize structured tools such as the Internal Credit Risk Rating System (ICRRS); however, this is not universally practiced. Only a few banks have implemented structured ORM frameworks, including key risk indicators (KRIs) and risk research desks, reflecting a lack of uniformity and commitment to proactive risk management.

The operational failure of the "three lines of defense" model was another critical theme. In many banks, the model is dysfunctional, with limited clarity between the responsibilities of business units (first line), risk management (second line), and internal audit (third line). However, some institutions have attempted to address this by appointing "risk champions" within business units to serve as a "1.5 line of defense", following International Finance Corporation (IFC) recommendations. Still, such practices remain exceptions, not norms.

A concerning trend noted by interviewees was the rise of innovative and complex irregularities, which require robust ORM systems to detect and deter. Although only a small fraction of banking staff are reportedly involved in unethical practices, the adverse impact of these few individuals has been disproportionately high. This underscores the need for improved screening, training, and placement by Human Resource (HR) departments, which currently fail to fulfill these responsibilities consistently. Additionally, conflict of interest issues were flagged, particularly where the roles of CRO and Head of CRM are combined, a practice strongly discouraged by some of the experts. They also recommended that rotation policies, while beneficial for operational/business staff, should not be applied to risk management personnel, to preserve domain expertise and continuity.

There is a general lack of awareness among bank leadership regarding the scope and function of the RMD. Many risk incidents are not reported to the CRO unless under special engagement, indicating selective and incomplete risk communication. Additionally, Pillar II, Point-10 of the Basel-III framework was cited as vague and undefined, creating room for inconsistent interpretations. Furthermore, credit

operations, while being a major source of income, also contribute significantly to op. risk, and therefore demand integrated management strategies.

To address these issues, informants proposed several forward-looking recommendations. Firstly, the Board of Directors (BoD) and Senior Management Team (SMT) must recognize ORM as a strategic priority, and establish a separate, dedicated ORM desk with clearly defined responsibilities. Secondly, Bangladesh Bank (BB) should strengthen its role by ensuring risk-based supervision explicitly includes operational risk, and by exerting regulatory pressure to improve ORM practices in the industry. It was also suggested that BB's inspection reports be analyzed systematically through a dedicated research desk and that industry-wide policies be formulated based on these findings. Furthermore, an effective whistleblowing mechanism should be instituted, and a comprehensive lost data register covering at least three years must be maintained to enable in-depth analysis and policy improvement.

Experts also called for bank-specific or group-specific frameworks under the Basel regime, rather than one-size-fits-all approaches. Immediate revision of BB's ORM guidelines was urged to reflect contemporary challenges. Additionally, the formation of a dedicated sub-committee on ORM within bank governance structures was proposed. Finally, it was emphasized that profit and dividend targets set by the BoD and SMT should be validated by the RMD to ensure alignment with risk capacity. A collaborative platform like BIBM and BB could be leveraged to design prudent and context-specific ORM strategies. The key points derived from the FGD is summarized in Box 4.6.

Box 4.6: Key Points of the FGD Discussion

- Operational risk is foundational, often triggering credit and market risks, yet receives inadequate strategic attention in banks.
- Risk governance is underdeveloped and overshadowed by regulation, which experts argue must be reversed to enhance proactive oversight.
- Banks lack a structured ORM approach, with inconsistent management of People, Processes, Systems, and External Events, increasing vulnerabilities.
- Leadership and risk culture are weak, with ORM often marginalized and CRO roles dominated by credit risk professionals, diluting operational focus.
- The RMD is frequently undervalued, leading to under-resourced mandates and unclear roles.
- Existing ORM policies lack enforcement and strategic integration, resulting in vague risk appetite definitions and inefficient resource allocation.
- The three lines of defense model is failing, with unclear role demarcation, though some banks have adopted '1.5 line' champions as a workaround.
- Complex internal irregularities are rising, demanding robust ORM systems, better HR screening, and avoidance of role conflicts (e.g., combining CRO and CRM).
- Risk communication is selective, and Basel III's guidance lacks clarity, weakening uniform application and awareness among bank leadership.
- Experts recommend dedicated ORM units, regulatory reforms, enhanced data management, and tailored frameworks to improve risk culture and system resilience.

Source: *FGD*

4.3 Challenges Associated with ORM and Governance in Banks

4.3.1 Operational Risk Elements and the Associated Challenges

Not different from most other developing economies, the banking industry of Bangladesh has several common Operational Risk elements associated with cyber security, financial fraud and operational complexities. Certain operational concerns of the banking industry, however, deserve special attention considering their severity and graveness (Box 4.7 to Box 4.11). Further, certain issues need to be discussed to draw attention of the policymakers and bank management for improving Operational Risk Management governance and practices in banks (Box 4.12 to Box 4.15).

Box 4.7: 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.[46]

[46] 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)

Box 4.8: 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, 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

Box 4.9: Big Scams and Operational Risks in Banking in Bangladesh

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)

Box 4.10: 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.[47] A recent government white paper estimates USD 234 billion siphoned out over 2009–23 i.e. 16 billion per year.[48] UN agencies and NGOs highlight that Bangladesh produced official estimates of illicit flows (drugs, human trafficking, etc.) only in 2023.[49] 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.[50] These estimates underscore a persistent upward trend in illicit outflows and Bangladesh's trade mis invoicing over the years.

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

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

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

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

Box 4.11: 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)

Box 4.12: 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 41,955 (BDT crore), and remittances 173,390 (BDT 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.[51]

[51] 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)

Box 4.13: 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.
Based on IT Security Department of ABC Bank

Box 4.14: 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

Box 4.15: Change Management and Operational Risk in Banking in Bangladesh

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)

4.3.2 Challenges of ORM in Banks: Survey/KII Opinions

Follwing the suggestion of the Basel Committee, Bangladesh Bank has categorized seven operational risk events. These are: (i) internal fraud (ii) external fraud (iii) employment practices and workplace safety (iv) clients products and business practices (v) damage to physical assets, (vi) business disruption and system failure (vii) execution, delivery and process management. Survey data shows that banks are facing a number of challenges while identifying and assessing these event based operational losses. The summary of the challenges are given in Box 4.16.

Box 4.16: Challenges of Event Based Operational Risk

Event-1: Internal Fraud

- Complexity of identifying and preventing the crimes, poor internal controls, insufficient monitoring tools are the major reasons of internal fraud. Regulatory compliance, particularly with Anti-Money Laundering (AML) and sanctions regulations, also poses a significant hurdle. Additionally, the growth of digital banking channels and the use of sophisticated technologies by fraudsters introduce new vulnerabilities.
- Difficulty in tracing sophisticated fraud schemes, dependency on employee integrity, failure to follow the process, lack of MIS, weak internal audit, ineffective monitoring & detection, misuse of the IT system, weak internal controls or segregation of duties are also the reason of internal fraud
- Lack of timely whistle blower reporting or fear of retaliation

Event-2: External Fraud

- Fraudsters leverage cutting-edge technologies like AI, machine learning, and sophisticated malware to conduct attacks such as phishing, vishing, ATM skimming and social engineering with increasing effectiveness. Given the neck-breaking pace of technological advancements, the Bank's IT department finds it challenging to keep pace on an ongoing basis. Lack of customer awareness is also a big challenge.
- Sometimes, cheque and signature fraud cannot be detected. In case of loan fraud, false title deeds/documents may be used.
- Bank faces several challenges when managing external fraud, including sophisticated fraud schemes, the growth of digital banking, balancing security with customer experience, and regulatory compliance. Specifically, the increase in digital banking channels has broadened the attack surface, making it more difficult to detect and prevent fraud. Additionally, balancing strong security measures with a positive customer experience is a delicate task, as overly strict measures can frustrate users and drive them away.
- High cost of fraud mitigation as fraud detection systems is expensive, reputational damage due to loss of customer trust, brand erosion etc. are also create challenges.

Event-3: Employment Practices and Workplace Safety

- Identifying and assessing potential hazards in workplace, maintaining health and safety standards, especially, in remote work environments, managing a safe, harassment-free workplace, stress, bullying, and work-life balance are the major challenges in this OR event
- Managing staff grievances, employee dissatisfaction, discrimination, weak hiring & background checking, high stress environment, compensation Policy also creates severe threat.

Event-4: Clients, Products, and Business Practices

- Insufficient knowledge on products and services by the employees, Compromise of customer confidential data, Navigating complex and changing regulatory requirements, Managing reputational damage from customer complaints or litigation are major problems.
- Unhealthy competition and yearly business target sometimes influence the bank's business practices which in the long run create risk.
- Difficulty in verifying client identities and ensuring compliance with anti-money laundering laws can expose firms to legal and financial risks.
- Highly structured or innovative products may be misunderstood internally or mis-sold, leading to regulatory scrutiny or client disputes.

Event-5: Damage to Physical Assets

- Risk of unexpected failure like political turmoil and natural disasters such as threat of floods, earthquake, etc.
- Physical damage to buildings, data centers, or ATMs can halt banking operations, affecting customer service, transaction processing and market confidence.
- Rebuilding damaged assets, replacing equipment, and relocating staff can be extremely costly and time-consuming. Damage causing service outages or data compromise can erode customer trust, particularly if the bank is seen as unprepared.

Event-6: Business Disruption and System Failure

- IT system & process failure, communication disruption, utility outage and system outages (e.g., failed ATM transactions, mobile banking downtime) directly affect customers trust.
- Complex IT infrastructure make difficulty in identifying single points of failure or predicting system impacts of localized issues. Inadequate disaster recovery planning or testing is also a big challenge.

- Limited control and visibility into third-party operations; third-party failure can directly cause business disruption.
- Disruptions can stem from a wide array of sources, ranging from natural disasters (like the frequent monsoons and potential cyclones here in Bangladesh) and pandemics to geopolitical instability, cyberattacks, and even simple human error. The unpredictability of these events makes planning and preparation incredibly complex.

Event-7: Execution, Delivery and Process Management

- Human errors and negligence, wrong data entry, reconciliation, or reporting inaccuracies, erroneous legal documentation, unauthorized access to customer A/C, vendor disputes, poor or incomplete automation initiatives, ineffective control over outsourced or offshore operations are the mentionable challenges.
- Manual operations, poorly managed transitions (e.g., software upgrades, new product launches) can disrupt processes and introduce risk.
- Consistent and high-quality delivery and process management across all branches, channels (digital and physical), and customer segments is difficult.

Source: Survey Data

5. Challenges and Suggestions for Improving ORM Practices

One: Regulatory Framework and Incentives

Operational risk management (ORM) issues are currently covered under general risk management guidelines. However, the absence of explicit and enforceable regulatory mandates is likely contributing to inconsistent ORM practices across banks. Presently, banks have limited incentives from the market or the regulator to invest in robust ORM frameworks. There is a need for alignment with Basel standards at the enforcement level. Given the severity of operational risks, the Central Bank may consider issuing dedicated and enforceable guidelines. Additionally, incentive-based frameworks, regular supervisory reviews, and linking ORM maturity to supervisory rating systems should be developed. For loan-related operational risks, regulators must ensure legal actions against wilful defaulters.

Two: Proportional and Tiered Regulatory Approach

Banks do not follow uniform ORM governance and practices, justifying differentiated regulatory treatment. A one-size-fits-all approach lacks proportionality, especially considering variations in bank size, complexity, and risk exposure. The Central Bank may consider a tiered regulatory framework for capital requirements related to operational risk, providing appropriate incentives. Further, differentiated supervisory expectations should be set for small, medium, and large banks. Explicit frameworks for internal control, audit, and data management should be implemented across the banking sector.

Three: Integration of ORM with ERM and Risk Appetite Framework

Risk management in many banks is fragmented, with operational risk not integrated into the Enterprise Risk Management (ERM) framework. A clearly defined risk appetite statement-including operational risk thresholds-must be developed and approved by the Board. Current ORM risk appetite statements are vague and lack strategic alignment. Banks' Boards and top management must exercise due diligence in setting profit and growth targets, as aggressive targets can heighten operational risk. A dedicated ORM unit within the RMD should be established, with clearly defined responsibilities and measurable Key Risk Indicators (KRIs).

Four: Internal and External Loss Data Management

Most banks lack proper systems for the collection, centralization, and utilization of internal loss data, and are not part of external loss data consortia. It is essential to develop a centralized national loss data portal, maintained by the Central Bank or banking associations. Banks should be mandated to maintain internal loss event logs in standardized formats and encouraged to participate in external data-sharing platforms to support scenario analysis and stress testing.

Five: Change Management Governance

Banks generally lack structured change management policies and procedures, increasing operational risks during system upgrades, restructuring, or regulatory changes. A structured change management governance framework-aligned with ISO standards-is critical. Every change initiative should include risk assessments, stakeholder analysis, contingency plans, and post-implementation reviews as part of ORM processes.

Six: Third-Party and Agent Banking Risks

With the rise of third-party services and agent banking, banks face growing oversight and control risks. In many cases, contractual and monitoring mechanisms are inadequate. Banks must adopt rigorous third-party risk management policies, including due diligence, continuous monitoring, and regular audits. Third-party and agent activities must be integrated within the ORM framework and internal control systems.

Seven: Cybersecurity as an ORM Component

Cybersecurity is often treated as separate from ORM, despite being a major operational risk. There is limited integration of IT and cyber incident data into ORM registers. Banks should classify cybersecurity threats under ORM, incorporate cyber incidents in loss data and scenario analyses, and promote joint reviews between IT and risk teams to ensure holistic mitigation.

Eight: TBML and Trade Finance Risks

Trade-Based Money Laundering (TBML) poses a critical operational risk in Bangladesh's banking sector. Many banks lack adequate screening tools, segregation of duties, and compliance mechanisms in trade finance. Banks must enforce AML screening, vessel tracking, and price verification tools within ORM processes. Clear segregation of duties between origination, processing, and verification must be implemented. Staff should receive specialized training on TBML and trade compliance.

Nine: Use of Forward-Looking Tools

Banks seldom use forward-looking tools like scenario analysis and stress testing for operational risks. This is further hampered by the lack of adequate internal and external data. Banks should institutionalize regular scenario analysis workshops involving senior management, align findings with the risk appetite, and build data-supported stress testing models.

Ten: Capacity Constraints in RMD and Audit Functions

Many banks suffer from inadequate staffing and skills within their RMDs and internal audit teams. There is a shortage of operational risk specialists with deep process understanding. Banks should allocate more resources to RMDs, establish career development tracks, and encourage cross-functional rotations to improve risk culture and operational insight.

Eleven: Awareness and Training Gaps

There is limited awareness of ORM concepts among frontline and support staff, and few ongoing training programs tailored to specific responsibilities. Governance, compliance, and risk issues need to be addressed through targeted capacity development programs. Stakeholders should implement customized ORM training for bank staff at all levels, including clients, to foster an informed risk culture.

References

Bank for International Settlements -Financial Stability Institute (BIS-FSI) (2020). The use of supervisory technology by prudential authorities. Retrieved from https://www.bis.org

Bank of England (2021). Operational Resilience: Impact Tolerances for Important Business Services. Policy Statement PS6/21: https://www.bankofengland.co.uk/prudential-regulation/publication/2021

Barkha Jadwani, Shilpa Parkhi and Pradip Kumar Mitra (2024). Operational Risk Management in Banks: A Bibliometric Analysis and Opportunities for Future Research, Special Issue on Financial Reporting, Managing Risk, and Banking, MDPI: https://www.mdpi.com

Basel Committee on Banking Supervision (2011). Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches, Bank for International Settlements. https://www.bis.org/publ/bcbs190.htm

Basel Committee on Banking Supervision (2012). Core Principles for Effective Banking Supervision, BIS: https://www.bis.org/publ/bcbs230.pdf

Basel Committee on Banking Supervision (2015). Pillar 3 Disclosure Requirements – Consolidated and Enhanced Framework. Bank for International Settlements. https://www.bis.org/bcbs/publ/d400.htm

Basel Committee on Banking Supervision (2021a). Principles for Operational Resilience, Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.htm

Basel Committee on Banking Supervision (2024). Core Principles for effective banking supervision, BIS: https://www.bis.org/bcbs/publ/d573.pdf

Basel Committee on Banking Supervision. (2001). Working Paper on the Regulatory Treatment of Operational Risk, Retrieved from https://www.bis.org/publ/bcbs_wp8.pdf

Basel Committee on Banking Supervision. (2005). Compliance and the compliance function in banks. Basel: Bank for International Settlements.

BCBS (2003). Sound Practices for the Management and Supervision of Operational Risk, February 2003, BIS: https://www.bis.org/fsi/fsisummaries/psmor.htm

BCBS (2004). Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards: A Revised Framework, June 2004, BIS: https://www.bis.org/publ/bcbs107.pdf

BCBS (2006). International Convergence of Capital Measurement and Capital Standards, BIS, 2006.

BCBS (2008). Principles for Sound Liquidity Risk Management and Supervision, BIS: https://www.bis.org/publ/bcbs144.pdf

BCBS (2010). Basel III: A global regulatory framework for more resilient banks and banking systems, December 2010 (revised June 2011), BIS: https://www.bis.org/publ/bcbs189.pdf

BCBS (2011). Principles for the Sound Management of Operational Risk, June 2011, BIS: https://www.bis.org/fsi/fsisummaries/psmor.htm

BCBS (2017). Basel III: Finalising Post-crisis Reforms, BIS: https://www.bis.org/bcbs/publ/d424.pdf

BCBS (2021). Revisions to the Principles for the Sound Management of Operational Risk, March 2021, BIS: https://www.bis.org/fsi/fsisummaries/psmor.htm

BIS (2020). Operational and cyber risks in the financial sector, BIS Working Papers No 840: https://www.bis.org/publ/work840.pdf

Central Bank of Nigeria (CBN) (2021). CBN Regulatory Returns Portal and Risk-Based Supervision Framework: https://www.cbn.gov.ng

Chernobai, A., Jorion, P., & Yu, F. (2011). The Determinants of Operational Risk in US Financial Institutions. Journal of Financial and Quantitative Analysis, 1, 1683-1725.

Chernobai, Anna, Ali Ozdagli, and Jianlin Wang (2016). Business Complexity and Risk Management: Evidence from Operational Risk Events in U.S. Bank Holding Companies, Federal Reserve Bank of Boston, Working Paper, USA.

Committee of Sponsoring Organizations of the Treadway Commission (2013). Internal Control – Integrated Framework. https://www.coso.org

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013). Enterprise Risk Management—Integrated Framework: https://www.coso.org

Deloite (2018). The future of operational risk in financial services: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-the-future-of-operational-risk-in-financial-services.pdf

Dominic Wu (2012). Applying the Best Practice of Operational Risk Management in Technology and Operations, Bank of New York: https://www.plus-concepts.com

European Central Bank (ECB) (2020). Guide to internal models- Credit risk, Frankfurt, ECB, Germany.

FDIC (2006). Operational Risk Management: An Evolving Discipline, Supervisory Insights, Summer:https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum06/sisummer06-article1.pdf

Federal Reserve (2021). Supervisory and Regulatory Report - Risk Monitoring Enhancements: https://www.federalreserve.gov

Financial Stability Board (2014). *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture:* https://www.fsb.org/2014/04/140407/

Financial Stability Board (2020). COVID-19 Pandemic: Financial Stability Implications and Policy Measures Taken: https://www.fsb.org/2020/07/covid-19-pandemic-financial-stability-implications-and-policy-measures-taken/

FSB (2013). Principles for An Effective Risk Appetite Framework, November 2013: https://www.fsb.org/uploads/r_131118.pdf

FSB (2020). Effective Practices for Cyber Incident Response and Recovery, October 2020: https://www.fsb.org/uploads/P191020-1.pdf

FSB (2023). Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities, December 2023: https://www.fsb.org/uploads/P041223-1.pdf

Hugh Dang, Merlina Manocaran, Scott Murff, and Olivia White (2023).Direct losses from operational-risk failures are mounting, and in today's volatile economic environment, consequent losses in share price are many times greater: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/response-and-resilience-in-operational-risk-events

Institute of Internal Auditors (2013). The Three Lines of Defense in Effective Risk Management and Control: https://na.theiia.org

Institute of International Finance (2015). Risk Governance: From Evolution to Revolution: https://www.iif.com

Institute of Operational Risk (2010). Operational Risk Sound Practice Guidance-Developing Key Risk Indicators: https://www.ior-institute.org/

International Monetary Fund (2019). Building Supervisory Capacity for Risk-Based Supervision in Emerging Markets: https://www.imf.org/en/Publications/WP/Issues/2019/10/11

International Monetary Fund (2021). Enhancing Bank Supervision: Practices and Tools for Supervisory Intervention: https://www.imf.org

International Monetary Fund. (2023). 2023 review of the Fund's anti-money laundering and combating the financing of terrorism (AML/CFT) strategy—Background papers. Washington, DC: IMF.

ISO (2019). *ISO 22301:2019- Security and Resilience: Business Continuity Management Systems – Requirements: International* Organization for Standardizatio*n: https://www.iso.org*

Kelliher, P. O. J. M. Acharyya, A. Couper, E. Maguire, P. Nicholas, N. Pang, C. Smerald, D. Stevenson, J. Sullivan and P. Teggin (2020). Operational Risk Dependencies, British Actuarial Journal (2020), Vol. 25, United Kingdom.

Lu, Jin (2024). Analysing the Operational Risk Management of China's Commercial Banks, Modern Economy, 2024, 15, 725-732, Scientific Publishing: https://www.scirp.org/journal/me

Management Solution (2021). Trust and Reputation: Proactive Management of Reputational Risk: https://www.managementsolutions.com

Melo, Fabiana, Katharine Seal, and Valeria Salomao (2024). Revised Basel Core Principles for Effective Banking Supervision, IMF, July 2024, IMF.

Melo, T., Dias, J., & Pereira, R. (2024a). Operational Risk Governance in Banking: Audit, Control, and Regulatory Practices, Journal of Financial Regulation and Compliance, 55–72.

Monetary Authority of Singapore (MAS) (2022). Harnessing SupTech and AI in Supervision: https://www.mas.gov.sg

PwC (2024). Guidance Note on Operational Risk Management and Operational Resilience, June 2024: www.pwc.in/assets/pdfs/guidance-note-on-operational-risk-management-and-operational-resilience.pdf

Reserve Bank of India (RBI) (2021). CRILC Reporting System and Fraud Monitoring Guidelines: https://www.rbi.org.in

Segal, Troy (2024). Operational Risk: Overview, Importance, and Examples, September: https://www.investopedia.com/terms/o/operational_risk.asp

World Bank (2020). Bank Regulation and Supervision Survey: https://www.worldbank.org

Appendix Tables

Appendix Table A1: Top Operational Risks in Banking		
Operational Risks	**2023**	**2024**
Cyber risk: information security	1	1
Cyber risk: IT Disruption	3	2
Third-party risk	4	3
Regulatory compliance	2	4
Change management	7	5
Resilience risk	5	6
Geopolitical risk Execution	8	7
Execution and Process Error	6	8
External frauds	11	9
Conduct Risk	10	10
Note: Based on the survey of 81 major financial institutions (EY, 2025).		

Appendix Table-A2: Twelve Principles and Role of Supervisors by BCBS

Principle 1 emphasises the role of the board in promoting a strong risk management culture in the bank: The board of directors should take the leading role in establishing a strong risk management culture, implemented by senior management. The board should establish and regularly review and approve core policies. Through these policies, the board and senior management should establish a corporate culture guided by strong risk management, set standards and incentives for professional and responsible behaviour, and ensure that staff receives appropriate risk management and ethics training.

Principle 2 provides general requirements for the ORMF: Banks should develop, implement and maintain an ORMF that is fully integrated into the bank's overall risk management processes by the first line of defence, adequately reviewed and challenged by the second line of defence and independently reviewed by the third line of defence. The ORMF adopted by an individual bank will depend on a range of factors, including the bank's nature, size, complexity and risk profile.

Principle 3 describes the board's main duties with respect to the ORMF: The board of directors should approve and periodically review the ORMF. The board should also ensure that senior management implements the policies, processes and systems of the ORMF effectively at all decision levels.

Principle 4 sets guidance regarding the bank's risk appetite and tolerance statement: The board of directors should approve and periodically review a risk appetite and tolerance statement that articulates the nature, types and levels of operational risk the bank is willing to assume. The risk appetite and tolerance statement for operational risk should be easy to communicate and understand. Moreover, it should include key background information and assumptions, be forward-looking and clearly articulate the motivations for taking on or avoiding certain risks. It should also establish indicators to enable monitoring of these risks.

Principle 5 describes senior management's duties relating to the effective implementation of the ORMF: Senior management should develop for approval by the board a clear, effective and robust governance structure, commensurate with the nature, size, complexity and risk profile of the bank's activities. Its role is also to translate the ORMF (approved by the board of directors) into specific policies, procedures and processes and ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and resources.

Principle 6 sets guidance for the identification and assessment of operational risk: Senior management should ensure the comprehensive identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood. Examples of tools used for identifying and assessing operational risk include event management, operational risk event data, self-assessments of both operational risks and controls, control monitoring and assurance frameworks, operational risk metrics, scenario analysis, benchmarking and comparative analysis.

Principle 7 deals with change management: Senior management should ensure that the bank has policies and procedures defining the process for identifying, managing, challenging, approving and monitoring change on the basis of agreed objective criteria. Change implementation should be monitored by specific oversight controls. Change management policies and procedures should be subject to independent and regular review and update and should clearly allocate roles and responsibilities in accordance with the three-lines-of-defence model.

Principle 8 sets guidance for operational risk monitoring and reporting: Senior management should implement a process to regularly monitor operational risk profiles and material operational exposures. Appropriate reporting mechanisms should be in place at the board of directors, senior management and business unit levels to support proactive management of operational risk. Operational risk reports should include: breaches of the bank's risk appetite and tolerance statement, as well as thresholds, limits or qualitative requirements; a discussion and assessment of key and emerging risks; details of recent significant internal operational risk events and losses (including root cause analysis); relevant external events or regulatory changes and any potential impact on the bank.

Principle 9 describes the control environment and risk mitigation: Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies. A sound internal control programme requires appropriate segregation of duties and consists of four components that are integral to the risk management process: risk assessment, control activities, information and communication, and monitoring activities. In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party, such as through insurance.

Principle 10 highlights the importance of ICT risk management for the operational risk profile of the bank: Effective ICT performance and security are paramount for a bank to conduct its business properly. Therefore, banks should implement a robust ICT risk management programme in alignment with their operational risk management frameworks. The board of directors should regularly oversee the effectiveness of the bank's ICT risk management. Senior management should routinely evaluate the design, implementation

and effectiveness of the bank's ICT risk management to ensure data and systems' confidentiality, integrity and availability.

Principle 11 establishes the relationship between ORMF and business continuity planning: Banks should prepare forward-looking business continuity plans (BCPs) with scenario analyses associated with relevant impact assessments and recovery procedures. Banks should periodically review their BCPs and policies to ensure that contingency strategies remain consistent with current operations, risks and threats. BCPs should be linked to bank ORMFs.

Principle 12 describes the role of disclosure: Banks should disclose their ORMFs in a manner that allows stakeholders to determine whether the banks identify, assess, monitor and control/mitigate operational risk effectively. Banks should disclose relevant operational risk exposure information to their stakeholders (including significant operational loss events), while not creating operational risk through this disclosure (eg description of unaddressed control vulnerabilities). A bank should have a formal disclosure policy that is subject to regular and independent review and approval by senior management and the board of directors.

Role of supervisors: The PSMOR require supervisors to regularly assess banks' ORMFs by evaluating their policies, processes and systems related to operational risk. Supervisory evaluations of operational risk should include all areas described in the PSMOR. In certain circumstances, supervisors may choose to use external auditors in these assessment processes. Supervisors should take steps to ensure that banks address deficiencies identified through the supervisory review of banks' ORMFs.

Source: *BIS (2021) Revisions to the Principles for the Sound Management of Operational Risk, BIS: https://www.bis.org/fsi/fsisummaries/psmor.htm*

Appendix Table-A3: Operational Loss Event Types		
Loss Event Type	**Definition**	**Examples**
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party.	Intentional misreporting of positions, employee theft, and insider trading on an employee's own account.
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.	Robbery, forgery, cheque kiting, and damage from computer hacking.
Employment practices and workplace safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/ discrimination events.	Workers compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, and general liability.
Clients, products and business practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorized products.
Damage to physical assets	Losses arising from loss or damage to physical assets from natural disaster or other events.	Terrorism, vandalism, earthquakes, fires and floods.
Business disruption and system failures	Losses arising from disruption of business or system failures.	Hardware and software failures, telecommunication problems, and utility outages.
Execution, delivery and process management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.	Data entry errors, collateral management failures, incomplete legal documentation, and unauthorized access given to client accounts, non-client counterparty mis-performance, and vendor disputes.

***Source**: International Convergence of Capital Measurement and Capital Standards, BCBS, 2006*

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