International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A STUDY OF E-BANKING OPERATIONAL RISK MANAGEMENT FRAMEWORKS IN INDIA

Harnish kumar Shah, Dr. Parveen Kukkar

DESIGNATION- RESAERCH SCHOLAR SUNRISE UNIVERSITY ALWAR
DESIGNATION- PROFESSOR SUNRISE UNIVERSITY ALWAR

ABSTRACT

This will be accomplished by evaluating the present status of operational risk management procedures in India pertaining to operations involving electronic banking. In addition to this, the research will investigate the regulatory framework that governs e-banking in India as well as the implications that this framework has for risk management. In addition to this, the study will give insight on emerging trends, best practices, and possible areas for development in the operational risk management methods of online banking. In conclusion, this abstract lays the groundwork for a more in-depth investigation into the essential aspects of operational risk in e-banking. It provides significant insights for policymakers, financial organizations, and academics who are interested in improving the resilience and security of electronic banking systems in India.

KEYWORDS: E-Banking, Operational Risk Management, India, financial organizations

INTRODUCTION

The idea of operational risk is central to the digital transformation; it is complex and goes beyond the traditional credit and market concerns that banks confront. Technology failures, cyberattacks, data breaches, human mistakes, and process inefficiencies are all examples of operational risk in the e-banking industry. When things go wrong with online banking, it can have a devastating effect on both the banks' bottom lines and their customers' faith in the whole digital banking system. In light of operational risk's importance in this setting, it is critical to develop a theoretical framework that handles the intricacies of operational risk management in India's online banking sector.

As a result of operational risk's long-standing importance to financial institutions' stability, international regulatory agencies have developed frameworks to aid in risk management. The

BCBS, an important player in the development of international banking standards, has established guidelines for operational risk management in its Basel II and Basel III frameworks. These rules are based on a three-pronged strategy that includes mandatory minimum capital, periodic supervisory reviews, and market discipline. Recognizing the need for a systematic and all-encompassing risk management strategy, the theoretical framework for managing operational risks in online banking in India is in accordance with the principles stated by the BCBS, within this worldwide framework.

The theoretical foundation of operational risk management in India's e-banking sector should take into account both worldwide frameworks and norms that are not specific to any one business. An enterprise-wide framework for risk management is emphasized by the ISO 31000 Risk Management Standard, which offers a comprehensive perspective on risk management. When developing risk management methods for the online banking industry, this industry-wide standard is a great resource. These guidelines are supplemented by the Enterprise Risk Management (ERM) framework, which is a complete model for managing risks inside an organization. It is developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

The theoretical framework for e-banking operational risk management is significantly influenced by the specific features of the Indian regulatory environment. As India's primary regulatory body, the Reserve Bank of India (RBI) has taken the initiative to strengthen banks' ability to withstand changing risk conditions by adopting rules and regulations. Not only does India's regulatory system reflect the possibilities and threats posed by the country's ever-changing financial landscape, it also conforms to international norms. Because of this, the theoretical framework has to take a close look at the rules and regulations, including the RBI's recommendations, to make sure that operational risk management is both legal and specific to the Indian banking industry.

Due to the technical nature of online banking in India, any theoretical framework for operational risk management must investigate the complex relationship between new technologies and existing methods of reducing risk. As a subcategory of operational risk, technology risk includes dangers including using old technologies, having weak cybersecurity, and the possibility of systems failing. Knowing how technology affects

operational risk management is critical in the Indian setting, due to the country's strong digitization drive. The use of data analytics, machine learning, and artificial intelligence is becoming more important for proactively managing operational risks and finding ways to reduce them.

The theoretical framework for operational risk management in e-banking in India is a practical reaction to the changing dynamics of the financial system, rather than just an academic exercise. Management of operational risks in India's e-banking landscape presents both opportunities and challenges. This theoretical foundation aims to shed light on these issues by investigating international frameworks, industry standards, regulatory imperatives, and technological imperatives. As the trip progresses, it is set to shed light on operational risk management, providing insights that are both academically valuable and practically necessary for protecting the reliability and security of online banking in India.

OPERATIONAL RISK MANAGEMENT FRAMEWORKS

In order to identify, analyze, and mitigate operational risks, financial institutions and organizations rely on operational risk management frameworks, which provide a systematic and complete approach. International standards, legal mandates, and best practices in the sector have all played a role in the gradual evolution of these frameworks, which aim to guide users through the complex terrain of operational issues. There are a number of important models within operational risk management frameworks, and they all aim to improve companies' resilience and sustainability in their own ways.

An essential component of risk governance is the operational risk management framework put out by the Basel Committee on Banking Supervision (BCBS), which has played a significant role in molding international banking rules. In its Basel II framework, which was subsequently improved in Basel III, the BCBS established operational risk as a separate kind of risk and laid out a three-pronged strategy. Financial institutions must maintain capital that is proportional to the operational risk they face, as outlined in the first pillar, which focuses on minimum capital requirements. Banks' internal procedures for managing operational risk are evaluated by regulators as part of the supervisory review pillar, the second pillar. Banks are compelled to provide information on their risk management strategies as part of the third pillar, market discipline, which promotes openness. Along with making it easier to put a

number on operational risk, this all-encompassing framework highlights how critical it is to manage risk in an integrated and complete manner.

A more holistic view of operational risk management is offered by the International Organization for Standardization (ISO) 31000 Risk Management Standard, which is relevant across a range of sectors. ISO 31000 states that risk is the "effect of uncertainty on objectives" and promotes a procedure for managing risks that includes identifying them, assessing them, treating them, monitoring them, and communicating about them. Even while this standard isn't banking-specific, it does provide ideas and recommendations that the financial industry may use. ISO 31000 encourages a risk-aware culture to spread throughout an organization by highlighting the need of incorporating risk management into decision-making and governance processes.

Organizations such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) have also made significant contributions to the field of risk management via their Enterprise Risk Management (ERM) framework. Although COSO ERM was initially designed to handle risks related to financial reporting, it has expanded its scope to include operational risk as well. Setting goals, identifying events, assessing risks, responding to risks, controlling activities, information and communication, and monitoring are the eight parts that make up the framework. The COSO ERM framework integrates these elements to help organizations better understand risk and to ensure that risk management is in line with their strategic goals.

The COSO ERM framework, when applied to operational risk, helps businesses set up enterprise-wide risk management systems. Organizational culture, ethics, and governance shape risk management approaches, as shown by the focus on the internal environment. With the use of event identification and risk assessment, companies may anticipate and evaluate possible threats, and the risk response component directs the creation of plans to lessen, eliminate, or shift those threats. Integrating risk management procedures into day-to-day operations is achieved via control activities, information and communication, and monitoring. Ongoing review and improvement of the risk management framework is made possible by monitoring.

Although the aforementioned three frameworks provide a good basis for operational risk management, tailoring their application to match the specific difficulties faced by different businesses and sectors is essential. New factors and models are relevant in the banking industry. One prominent example is the Advanced Measurement Approach (AMA), which was established by the Basel Committee to enable big, globally active banks to use their own models for determining regulatory capital for operational risk. When it comes to quantifying operational risk, the AMA takes a more sophisticated and institution-specific approach than conventional methods by using a mix of loss data from the past, hypothetical situations, and statistical modeling.

In addition, operational risk management may make use of the Capability Maturity Model Integration (CMMI), which is popular in the tech and software sectors. CMMI evaluates how well a company has progressed in many process domains, one of which is risk management. Organizations improve their risk management capabilities as they advance through maturity stages, shifting from reactive and ad hoc methods to proactive and streamlined processes.

The ever-changing nature of operational risk has prompted regulatory bodies to continuously update and broaden their recommendations. For instance, the Federal Reserve System of the United States provides supervisory instructions on operational risk management that include expected practices in the areas of governance, risk assessment, measurement, reporting, and scenario analysis. In Europe, the ICAAP (Internal Capital Adequacy Assessment Process) is governed by the European Banking Authority (EBA), which issues recommendations for evaluating operational risk.

The rapidly expanding area of cybersecurity risk management also intersects with operational risk management frameworks. Organizations include cybersecurity risk into their operational risk frameworks in response to the growing sophistication and prevalence of cyber threats. Despite its narrow emphasis on cybersecurity, the NIST Cybersecurity Framework is consistent with concepts from operational risk management more generally. Key components of operational risk management are reflected in its five primary tasks: identify, protect, detect, respond, and recover. These functions highlight the need of taking a proactive and adaptable approach to cybersecurity. As a focal point for the growth of operational risk management frameworks, the banking industry plays a crucial role in increasing the

resilience of companies across numerous sectors. Building a strong risk management infrastructure is a team effort that includes industry-specific models like AMA and CMMI in addition to industry-wide standards like the BCBS and ISO 31000. To adapt to new challenges and build a culture of resilience, firms must adopt a risk-aware mindset and engage closely with regulatory agencies. This will help them traverse the complicated world of operational risks.

COMPONENTS OF E-BANKING OPERATIONAL RISK

For financial organizations providing digital financial services, operational risk in e-banking is complex and includes many different factors, each of which may be both a threat and an opportunity. To create an all-encompassing operational risk management plan that takes into account the complexities of electronic banking, it is crucial to understand these components. Each of the three main types of operational risk in online banking—technological, human, and process—contributes significantly to the unique set of problems that banks face in the modern day.

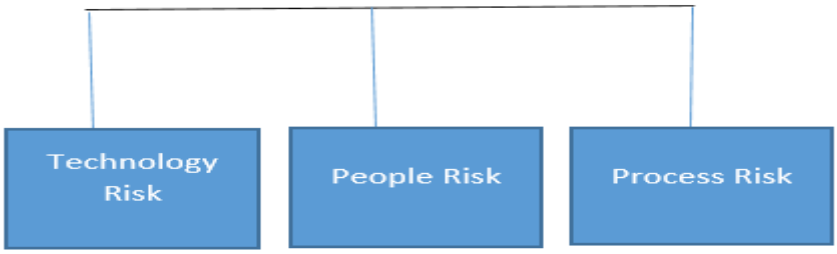

Figure 1 Operational Risk

Technology Risk:

Digital systems, software programs, and the interconnection of electronic platforms provide a variety of dangers that e-banking relies on for its foundation, technology. One of the most important issues is cybersecurity, which is a part of technological risk. The security of online banking operations is being increasingly threatened by the growing complexity of cyber threats, such as phishing attempts and ransomware. Cyber threats are always changing, so financial institutions need strong defenses, continual monitoring, and proactive steps to protect consumer data, financial transactions, and digital system integrity.

Technology risk is exacerbated by infrastructure weaknesses. System failures, outages, and interruptions are possible outcomes of the intricate network upon which electronic banking activities depend. Service outages, financial losses, and reputational harm may result from a single point of failure in the technology infrastructure. To lessen the blow of any technical failures, institutions should spend money on redundant and robust systems, test them often, and have disaster recovery plans in place.

In addition, there is a danger of obsolescence due to the quick rate of technical progress. To stay up with the times and satisfy customers, e-banking systems are always changing. Adopting cutting-edge tech like AI, blockchain, and open banking APIs comes with its fair share of dangers. These include compatibility issues, integration problems, and the possibility of unexpected obstacles. By balancing innovation with risk management, financial institutions may make sure that new technology adoption is in line with their risk appetite and regulatory needs.

People Risk:

The people involved, including workers, clients, and outside parties, are an important aspect of the operational risk of online banking. One of the fundamental concerns of the digital ecosystem is the possibility of employee mistakes or harmful insider operations. The best way to decrease the possibility of hazards caused by humans is to foster a cybersecurity-conscious culture inside the firm via training and awareness initiatives. Internal dangers may be lessened with the use of strong access restrictions, job separation, and monitoring systems.

The human factor poses hazards to customers in the form of account takeovers, identity theft, and social engineering attempts. Customers must be educated and made aware of the need of good cybersecurity hygiene in order to avoid falling prey to numerous frauds and scams. In addition, to strengthen the identification verification process and improve the general security posture of online banking platforms, banks should use biometric solutions, multi-factor authentication, and secure authentication procedures.

Using outside suppliers and service providers increases the potential for human error. When you rely on other parties to handle tasks like cloud hosting or processing payments, you open yourself up to potential dependency. In order to avoid interruptions in operations, data

breaches, or non-compliance with regulations, it is crucial to evaluate the security policies and resilience of third parties. Managing people risk in the e-banking ecosystem requires thorough due diligence, contractual agreements, and continuous monitoring.

Process Risk:

Everything from processing transactions to enrolling customers and delivering services is a part of the procedures that support e-banking operations. Deficits in these operational routines cause process risk in e-banking in the form of mistakes, inefficiencies, and vulnerabilities. Process risk includes the potential for fraud as one of its key components. The prevalence of fraudulent operations including account takeovers, phishing attacks, and payment fraud is increasing as financial transactions move to digital platforms. To effectively manage this process risk, it is crucial to implement systems for detecting and preventing fraud, monitoring transactions, and using algorithms to identify anomalies.

Among the many important aspects of process risk is compliance risk. The regulatory environment around online banking is ever-changing and is prone to frequent revisions. When it comes to consumer protection, data security, anti-money laundering (AML), and know your customer (KYC) rules, financial institutions have their hands full. Institutions risk legal and regulatory penalties and damage to their brand and trustworthiness when they fail to comply. As a result, in order to reduce process risk associated with compliance, it is essential to invest in compliance management systems, regularly check compliance, and remain updated on legislative changes.

Problems with data security, interoperability, and system integration arise with the introduction of new digital channels and technology. Data must flow freely across channels for e-banking platforms to operate properly, which in turn depends on the efficient integration of different systems. On the other hand, security holes, data discrepancies, and system failures are all possibilities due to integration's complexity. In order to manage the process risk that comes with integrating technology, it is vital to do thorough testing, conduct frequent audits, and adhere to industry standards for interoperability.

The effectiveness of operational procedures is also highly related to the quality of the customer experience. Dissatisfaction, customer attrition, and reputational harm may ensue

from any failure in the customer experience, whether it account opening, financial transfers, or dispute resolution. To improve the overall operational resilience of e-banking systems, financial institutions should focus on process optimization, invest in user-friendly interfaces, and deploy solutions that are customer-centric.

A multi-pronged strategy is necessary for the effective management of the many facets that make up e-banking operational risk. When it comes to running an online bank, there are three main types of risk: technology, people, and procedure. To overcome the ever-changing obstacles of online banking in the modern day, financial institutions should take the initiative to improve their cybersecurity, raise employee security knowledge, and streamline internal operations. In order to strengthen their defenses against operational risks and to cultivate a safe and resilient e-banking environment that inspires trust among stakeholders and clients, institutions must strike a balance between innovation and risk management.

RISK MANAGEMENT PRACTICES IN INDIA

In reality, knowledge theorists argue that risk management encompasses all four of these concepts—uncertainty, risk, equivocation, and mistake (Mohan, 2003). Lack of knowledge leads to uncertainty, which cannot be predicted even by random chance, and when information is gathered, this uncertainty turns into risk, where assessment of the result is conceivable. Risk management offers a means of limiting risk in an era of ever-increasing market information and awareness of potential outcomes. The inability to make a decision because of competing understandings is what leads to equivocality. Even though we have all the information we need, this still occurs. Because of this, financial institutions and others like them have developed control systems to cut down on mistakes, information systems to lessen the impact of uncertainty, incentive systems to handle agency issues in the risk-reward framework, and cultural systems to handle ambiguity.

When it came to risk management, Indian banks first relied on systems that evolved with the country's regulatory landscape and accounting norms. Banks are vulnerable to mark-to-market accounting due to the increasing rate of deregulation and the corresponding changes in consumer behavior (Mishra, 1997). Consequently, Indian banks have the task of creating a unified system for risk assessment and management that is both in line with business objectives and adaptable to changes in the market. Keeping an eye on the convergence of

national regulatory frameworks, changes in international accounting standards, and most crucially, changes in customers' business practices is crucial for banks in today's ever-changing market. Following specific risk management standards recommended by the RBI and BIS is, hence, urgently required.

ROLE OF RBI IN RISK MANAGEMENT IN BANKS

As of late, the Reserve Bank of India has begun gauging the health of Indian banks using the CAMELS rating system. These six parts make up the CAMELS Model: Capital Adequacy, Asset Quality, Management, Earnings, and the Model.

Quality, Liquidity and Sensitivity to Market risk

When evaluating a financial institution, the Basel Committee on Banking Supervision of the Bank for International Settlements (BIS) suggested the acronym CAMEL in 1988. This stands for capital adequacy, assets quality, management quality, earnings, and liquidity. Sensitivity to market risk (S), CAMEL's sixth component, was introduced in 1997. The majority of developing nations, however, are evaluating financial institutions' performance using CAMEL rather than CAMELS. Some nations' central banks, such as those in Nepal and Kenya, employ CAEL rather than CAMELS. It is usual practice to assess the stability of financial institutions using CAMEL's methodology.

Licenses, minimum capital requirements, pricing of services (including interest rates on deposits), reserves, and liquid asset requirements were the primary areas of statutory regulation of commercial banks in India by RBI until the early 1990s (Kannan, 2004). Under these conditions, solvency concerns were the primary emphasis of the oversight. To match its supervisory and regulatory standards with worldwide best practices, the RBI undertook a number of steps after the BIS prudential requirements evolved in 1988. Concurrently, it made sure that the prudential standards were gradually applied across various parts of the financial sector while taking into consideration the country's socio-economic conditions, business practices, payment systems, and mostly agricultural economy.

Lastly, in 1999, the Reserve Bank of India (RBI) acknowledged the need for proper risk management and issued guidelines to banks on asset liability management, credit management, market risk, and operational risk. Since 1994, the entire supervisory mechanism

has been realigned under the orders of a newly formed Board for Financial Supervision (BFS), which operates under the aegis of the RBI, to meet the demanding demands of a strong and stable financial system. With the exception of institutions involved in the capital markets and the insurance industry, the BFS's supervisory authority currently encompasses the entire financial system. Now, off-site monitoring that focuses on the risk profile of the monitored institution supplements the targeted evaluations by the Reserve Bank and the occasional on-site inspections. In 1999, a system was established to rate banks. For Indian banks, this system is called CAMELS, while for international banks, it is called CACS, which stands for Capital, Asset Quality, Compliance, and Systems & Control. Since then, the Reserve Bank of India (RBI) has implemented stricter capital adequacy standards and begun using a rating system based on CAMEL criteria—Capital adequacy, Asset quality, Management, Earnings, and Liquidity—to determine if Indian banks are financially stable. Financial institutions and non-banking financial enterprises are now within the regulatory and supervisory purview of the Reserve Bank. Because of these shifts, Risk-Based Supervision (RBS) is where the focus should be. Board for Financial Supervision (BFS) primarily deals with matters pertaining to both on-site and off-site bank supervision. Banks' on-site supervision system follows the 'CAMEL' model, which is updated annually. Core evaluations, including solvency, liquidity, operational soundness, and managerial prudence, are the emphasis, in line with the legislative duty. This is the foundation for bank ratings. In addition, the BFS must now supplement on-site supervision with off-site surveillance in order to capture 'early warning signals' that could help prevent another East Asian financial crisis, given the current trends towards financial integration, competition, and globalization. Capital sufficiency, asset quality, concentrated and huge credit, linked lending, profits, and risk exposures (including currency, liquidity, and interest rate concerns) make up the off-site monitoring system. Additionally, a secondary market indication of financial success for banks may be derived from fundamental and technical study of their stock. This means that each bank's risk profile will be based on RBS. Reducing the frequency of supervisory meetings and increasing the use of instruments targeted at structural meetings, extra off-site monitoring, frequent onsite inspections, etc., will result in more rigorous supervision of a high-risk sensitive bank. Doing this will help keep the Indian financial system from collapsing.

CONCLUSION

The need for this study on e-banking operational risk management in India arises from the transformative impact of technology on the financial sector. With the rapid adoption of e-banking services, financial institutions are confronted with a dynamic risk landscape that demands meticulous attention. The surge in cyber threats, technology failures, and evolving customer expectations necessitates a comprehensive analysis of operational risks specific to the Indian context. The regulatory framework governing e-banking in India is continuously evolving to strike a balance between innovation and security. Understanding and complying with these regulations is crucial for financial institutions to operate effectively and sustainably in the digital ecosystem. This study aims to provide insights into the intricacies of these regulations and their implications for operational risk management. As e-banking technologies continue to advance, it is imperative to evaluate their impact on operational risks. The study seeks to dissect the interplay between technology, human factors, and regulatory compliance, offering a nuanced understanding of how these elements converge in the e-banking domain. By addressing these critical aspects, the research aims to offer actionable recommendations for enhancing operational risk management practices, thereby fortifying the resilience and sustainability of e-banking services in India.

REFERENCES

1. Chapelle, Ariane; Crama, Yyes; Hubner, George & Peters, Jean Philippe (2005). Measuring and Managing Operational Risk in the Financial Sector: An Integrated Framework, February 27, 2005. Available at http://ssrn.com/abstract=675186

2. Chaturvedi, Ankita & Joshi, Sakshi. (2019). E-Business and Banking Industry: -An Analysis (A Study of ICICI Bank in Rajasthan). 10.13140/RG.2.2.29173.81122.

3. Chaudhry, Sahila & Singh, S. (2012). Impact of Reforms on Asset Quality in Indian Banking. *ZENITH: International Journal of Multidisciplinary Research*, 02(01), January, 13-31

4. Chaudhry, Sahila (2014). Risk of Careless Attitude of Service Providers in E-banking. *KAIM Journal of Management and Research*, 07 (02), November-April, 53-58

5. Chaudhry, Sahila (2015). Risk of Hacking in E-Banking: A Group-wise Study of Indian Banks. *Galaxy International Interdisciplinary Research Journal,* 3 (11), October, 61-71.

6. Chaudhry, Sahila (2015). Risk of Hacking in E-Banking: A Study of Nationalized Banks. *Galaxy International Interdisciplinary Research Journal,* 3 (9), September, 1623.

7. Coleman, Rodney. (2011). Operational Risk. 10.1002/9780470400531.eorms0591.

8. Curbelo, Aury M. & Cruz, Alferdo (2013). Faculty Attitudes toward Teaching Ethical Hacking to Computer and Information Systems to Undergraduate Students, paper presented at Eleventh Latin American and Caribbean for Engineering and Technology (LACCET 2013) "Innovation in Engineering, Technology and Education for Competitiveness and Prosperity", August 14-16, Cancun, Mexico

9. Daryakin, A.A. & Andriashina, S.G.. (2015). Problems of Evaluation and Management of Operational Risks in Banks. Procedia Economics and Finance. 24. 156-165. 10.1016/S2212-5671(15)00637-1.

10. Das, Rituparna. (2014). E-Banking in India: Risk Management in Payments and Settlement System. 10.4018/978-1-4666-4983-5.ch021.

11. Dmitri Sokolov (2007). E-banking: Risk Management Practices of the Estonian Banks. Published in Working Papers in Economics, School of Economics and Business Administration, Tallinn University of Technology (TUTWPE), pp. 21-37, accessed from http://deepthought.ttu.ee/majandus/tekstid/TUTW PE_07_ 156.pdf

12. Ebnother, Silvan; Vanini, Paolo; Mcneil, Alexander & Antolinez-Fehr, Pierrre (2003). Modeling Operational Risk. *Journal of Risk,* 5 (3), 1-16, December, available at SSRN: http://ssrn.com/abstract=293179

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org