

“RISK ANALYSIS OF E-BANKING OPERATIONS”

A Thesis

Submitted towards the Requirements for the Award of Degree of

**Doctor of Philosophy
In
COMMERCE**

Under the Department of Commerce

**By
ZEHRA FATIMA
(Enrolment No.: 220101146)**

Under the Supervision of

**Dr. Aiman Fatma
Faculty of Commerce**



2026

**P.K. UNIVERSITY
NH- 27, Vill. Thanra (P.O. Dinara)
Shivpuri, M.P. India - 473665
www.pkuniversity.edu.in**



P.K.UNIVERSITY
SHIVPURI (M.P.)

University Established Under section 2F of UGC ACT 1956 Vide MP Government Act No 17 of 2015

CERTIFICATE OF THE SUPERVISOR

This is to certify that the work entitled “**Risk Analysis Of E-Banking Operations**” is a piece of research work done by **Shri/Smt./Ku. Zehra Fatima** Under my Guidance and Supervision for the degree of Doctor of Philosophy of **Department of Commerce, P.K. University (M.P) India.**

I certify that the candidate has put an attendance of more than 240 day with me. To the best of my knowledge and belief the thesis:

I – Embodies the work of the candidate herself.

II – Has duly been completed.

III –Fulfil the requirement of the ordinance relating to the Ph.D. degree of the University.

Signature of the Supervisor

Date:

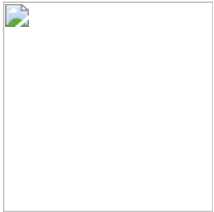


Result - September-2023

Course:	Ph.D. in Commerce	Semester:	First Semester
Enrollment No:	220101146	Institute Name:	Faculty of Commerce
Student Name:	ZEHRA FATIMA	Roll No:	227565421
Father's Name:	SYED HUSSAIN ALI	Session:	2022-23

S.No.	Subject Code	Subject Name	Credit	Grade	Grade Point	Credit Point
1	PHD101	RESEARCH METHODOLOGY	4	A	9	36
2	PHD102	COMMERCE	6	B	7	42
3	PHD103	RESEARCH AND PUBLICATION ETHICS	2	A	9	18
Total			12			96
SGPA:			96 / 12			8
CGPA:						8
Result:						Pass

* Grade in Repeat Examination





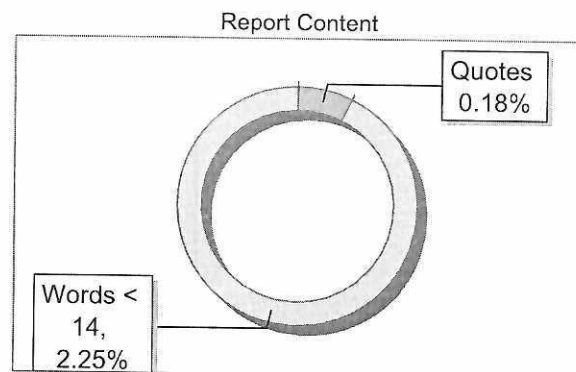
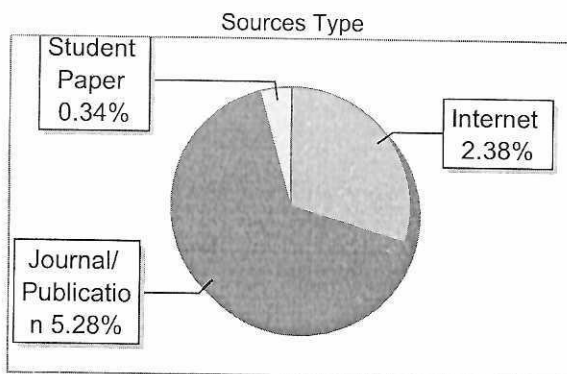
The Report is Generated by DrillBit Plagiarism Detection Software

Submission Information

Author Name	Zehra Fatima
Title	RISK ANALYSIS OF E-BANKING OPERATIONS
Paper/Submission ID	5405216
Submitted by	library.pku@gmail.com
Submission Date	2026-03-31 15:09:32
Total Pages, Total Words	146, 24354
Document type	Thesis Chapter

Result Information

Similarity 8 %



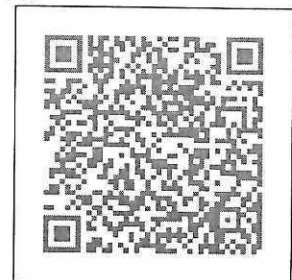
Exclude Information

Quotes	Not Excluded
References/Bibliography	Not Excluded
Source: Excluded < 14 Words	Not Excluded
Excluded Source	0 %
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

Unique QR Code used to View/Download/Share Pdf File



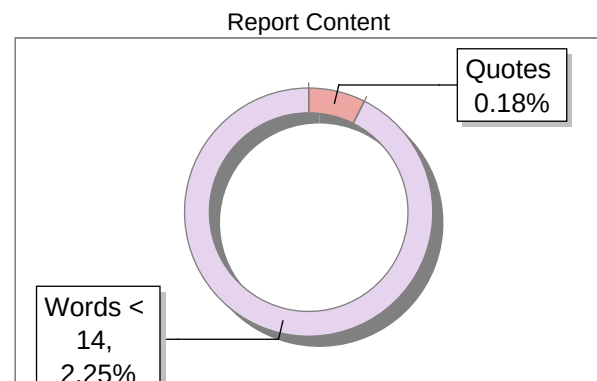
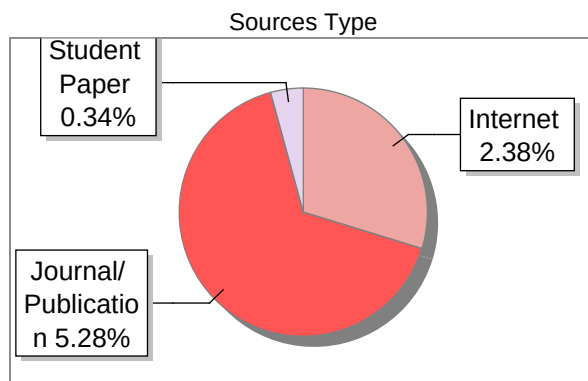
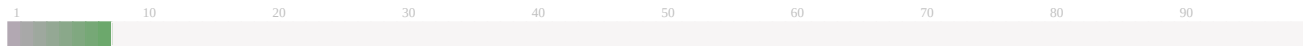
Shoban
LIBRARIAN
P.K. University
Shivpuri (M.P.)

Submission Information

Author Name	Zehra Fatima
Title	RISK ANALYSIS OF E-BANKING OPERATIONS
Paper/Submission ID	5405216
Submitted by	library.pku@gmail.com
Submission Date	2026-03-31 15:09:32
Total Pages, Total Words	146, 24354
Document type	Thesis Chapter

Result Information

Similarity **8 %**



Exclude Information

Quotes	Not Excluded
References/Bibliography	Not Excluded
Source: Excluded < 14 Words	Not Excluded
Excluded Source	0 %
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

A Unique QR Code use to View/Download/Share Pdf File





P.K.UNIVERSITY
SHIVPURI (M.P.)

University Established Under section 2F of UGC ACT 1956 Vide MP Government Act No 17 of 2015

DECLARATION BY THE CANDIDATE

I declare that the thesis entitled “**Risk Analysis Of E-Banking Operations**” is my own work conducted under the supervision of **Dr. Aiman Fatma** at **Department of Commerce, P.K. University (MP), India.**

Approved by Research Degree Committee. I have put more than 240 days of attendance with supervisor at the center.

I further declare that to the best of my knowledge the thesis does not contain my part of any work has been submitted for the award of any degree either in this University or in any other University, without proper citation.

Signature of the candidate

Date:

Place:



P.K.UNIVERSITY
SHIVPURI (M.P.)

University Established Under section 2F of UGC ACT 1956 Vide MP Government Act No 17 of 2015

FORWARDING LETTER OF THE HEAD OF
INSTITUTION

The Ph.D. thesis entitled “**Risk Analysis Of E-Banking Operations**” Submitted by **Shri/Smt./Ku. Zehra Fatima** is forwarded to the university in six copies. The candidate has paid the necessary fees and there are No Dues outstanding against her.

Name Seal

Date: Place:

(Signature of Head of Institution where the
Candidate was Registered for Ph.D degree)

Signature of the Supervisor

Date:

Address:

Place:

.....



P.K.UNIVERSITY
SHIVPURI (M.P.)

University Established Under section 2F of UGC ACT 1956 Vide MP Government Act No 17 of 2015

COPYRIGHT TRANSFER CERTIFICATE

Title of the Thesis: "Risk Analysis Of E-Banking Operations"

Candidates Name : Ms/Mr. Zehra Fatima

COPYRIGHT TRANSFER

The undersigned hereby assigns to the P.K. University, Shivpuri (MP) all the copyrights that exist in and for the above thesis submitted for the award of the Ph.D. degree.

Date:

Ms/Mr. **Zehra Fatima**

Signature

ACKNOWLEDGEMENT

The acknowledgement of a research endeavour is an opportunity to express appreciation for the joint efforts of those who have been sources of motivation and support and who have contributed invaluable knowledge toward achieving success in the pursuit of knowledge. With utmost humility and pride, I reflect upon the inspiring individuals who have propelled my work forward, and I am filled with immense pleasure, gratitude, and thanks for their unwavering dedication.

First and foremost, I would like to thank Almighty God for the perseverance, courage, and strength bestowed upon me to undertake and complete this project.

Furthermore, I extend my sincere thanks to the **Hon'ble Shri Jagdish Prasad Sharma, Chancellor, P.K. University, Shivpuri (M.P.)**, for providing the necessary infrastructure and facilities that were essential during my research work. My profound sense of gratitude, faith, and awe goes to **Hon'ble Prof. (Dr.) Yogesh Chandra Dubey, Vice Chancellor**, and **Hon'ble Prof. Mukesh Chourasiya, Pro Vice Chancellor**, P.K. University, Shivpuri (M.P.), for their generous and valuable support throughout my research.

I take this pleasant opportunity to express my deep sense of gratitude and reverence to **Hon'ble Dr. J.K.Mishra, Director (Administration), P.K. University, Shivpuri (M.P.)**, for his constant encouragement and for providing me with the required facilities that enabled me to complete my research work.

I extend my deepest appreciation to my esteemed **Dr. Aiman Fatma, Faculty of Commerce**, P.K. University, without whose support this work would not have come to fruition. Their exceptional guidance, unwavering support, kind cooperation, and provision of a conducive work environment have been invaluable beyond measure. I remain deeply indebted to them for instilling in me a relentless pursuit of excellence, a strong sense of honesty, and respect for the ethical principles that govern our profession.

I would also like to extend my sincere gratitude and deep appreciation to **Prof. Ashish Vishwakarma, Dean (Research); Dr. Aiman Fatma, Dean of Academics;** and **Prof. Jitender Kumar Malik, Registrar, P.K. University,** for inspiring and motivating me from the beginning of this work despite their busy schedules.

I owe a great deal of appreciation and gratitude to all the faculty members of the **Faculty of Commerce** and the non-teaching staff, without whose support it would have been difficult to shape my research work.

I also express my sincere gratitude to **Ms. Nisha Yadav, Librarian,** and **Mr. Anand Kumar, Assistant Librarian,** P.K. University, as well as the **IT Cell staff** for their assistance during the course of this research.

I have no words to express my gratitude to my family members and my better half for their love, support, and constant encouragement throughout the entire course of my research work.

Date

Zehra Fatima

Place

Enrolment No: 220101146

LIST OF ABBREVIATIONS

S.No	Abb.	Full Form
1	AMA	Advanced Measurement Approach
2	BCBS	Basel Committee on Banking Supervision
3	CMMI	Capability Maturity Model Integration
4	COSO	Committee of Sponsoring Organizations
5	ERM	Enterprise Risk Management
6	FSDC	Financial Sector Development Council
7	ISO	International Organization for Standardization
8	KYC	Know Your Customer
9	PIN	Personal Identification Number
10	RBI	Reserve Bank of India

LIST OF TABLES

S. No	Table. No.	Description	Page. No.
1	3.1	Gender of the respondents	70
2	3.2	Experience of the respondents	70
3	3.3	Qualification of the respondents	71
4	4.1	Factors Responsible for Risk of Repudiation of Customers' Transactions in Selected Banks of State Bank Group	74
5	4.2	Factors Responsible for Risk of Repudiation of Customers' Transactions in Selected Nationalized Banks	75
6	4.3	Factors Responsible for Risk of Repudiation of Customers' Transactions in Selected Private Sector Banks	77
7	4.4	Factors Responsible for Risk of Repudiation of Customers Transactions in Selected Groups of Banks	78
8	4.5	Impacts of Risk of Repudiation of Customers' Transactions in Selected Banks of State Bank Group	79
9	4.6	Impacts of Risk of Repudiation of Customers' Transactions in Selected Nationalized Banks	80
10	4.7	Impacts of Risk of Repudiation of Customers Transactions in Selected Private Sector Banks	81
11	4.8	Impacts of Risk of Repudiation of Customers' Transactions in Selected Groups of Banks	82
12	4.9	Measures for Overcoming the Risk of Repudiation of Customers Transactions in Selected Banks of State Bank Group	83
13	4.10	Measures for Overcoming the Risk of Repudiation of Customers' Transactions in Selected Nationalized Banks	85

14	4.11	Measures for Overcoming the Risk of Repudiation of Customers' Transactions in Selected Private Sector Banks	87
15	4.12	Measures for Overcoming the Risk of Repudiation of Customers' Transactions in Selected Groups of Banks	89
16	4.13	Factors Responsible for Risk of Outdated Staff and Lack of Management Expertise in Selected Banks of State Bank Group	91
17	4.14	Factors Responsible for Risk of Outdated Staff and Lack of Management Expertise in Selected Nationalized Banks	92
18	4.15	Factors Responsible for Risk of Outdated Staff and Lack of Management Expertise in Selected Private Sector Banks	94
19	4.16	Factors Responsible for Risk of Outdated Staff and Lack of Management Expertise in Selected Groups of Banks	95
20	4.17	Impacts of Outdated Staff and Lack of Management Expertise in Selected Banks of State Bank Group	96
21	4.18	Impacts of Risk of Outdated Staff and Lack of Management Expertise in Selected Nationalized Banks	97
22	4.19	Impacts of Outdated Staff and Lack of Management Expertise in Selected Private Sector Banks	98
23	4.20	Impacts of Risk of Outdated Staff and Lack of Management Expertise in Selected Groups of Banks	99
24	4.21	Measures for Overcoming the Risk of Outdated Staff and Lack of Management Expertise in Selected Banks of State Bank Group	100
25	4.22	Measures for Overcoming the Risk of Outdated Staff and Lack of Management Expertise in Selected Nationalized Banks	102

26	4.23	Measures for Overcoming the Risk of Outdated Staff and Lack of Management Expertise in Selected Private Sector Banks	104
27	4.24	Measures for Overcoming the Risk of Outdated Staff and Lack of Management Expertise in Selected Groups of Banks	105
28	4.25	Factors Responsible for Risk of Inadequate Customers' Security Practices in Selected Banks of State Bank Group	107
29	4.26	Factors Responsible for Risk of Inadequate Customers' Security Practices in Selected Nationalized Banks	108
30	4.27	Factors Responsible for Risk of Inadequate Customers' Security Practices in Selected Private Sector Banks	110
31	4.28	Factors Responsible for Risk of Inadequate Customers' Security Practices in Selected Groups of Banks	111
32	4.29	Impacts of Risk of Inadequate Customers' Security Practices in Selected Banks of State Bank Group	112
33	4.30	Impacts of Risk of Inadequate Customers' Security Practices in Selected Nationalized Banks	113
34	4.31	Impacts of Risk of Inadequate Customers' Security Practices in Selected Private Sector Banks	114
35	4.32	Impacts of Risk of Inadequate Customers' Security Practices in Selected Groups of Banks	115
36	4.33	Measures for Overcoming the Risk of Inadequate Customers' Security Practices in Selected Banks of State Bank Group	116
37	4.34	Measures for Overcoming the Risk of Inadequate Customers' Security Practices in Selected Nationalized Banks	118
38	4.35	Measures for Overcoming the Risk of Inadequate Customers' Security Practices Selected Private Sector Banks	121

39	4.36	Measures for Overcoming the Risk of Inadequate Customers' Security Practices in Selected Groups of Banks	123
40	4.37	Factors Responsible for Risk of Hacking in Selected Banks of State Bank Group	125
41	4.38	Factors Responsible for Risk of Hacking in Selected Nationalized Banks	126
42	4.39	Factors Responsible for Risk of Hacking in Selected Private Sector Banks	127
43	4.40	Factors Responsible for Risk of Hacking in Selected Groups of Banks	128
44	4.41	Impacts of Risk of Hacking in Selected Banks of State Bank Group	129
45	4.42	Impacts of Risk of Hacking in Selected Nationalized Banks	130
46	4.43	Impacts of Risk of Hacking in Selected Private Sector Banks	131
47	4.44	Impacts of Risk of Hacking in Selected Groups of Banks	132
48	4.45	Measures for Overcoming the Risk of Hacking in Selected Banks of State Bank Group	133
49	4.46	Measures for Overcoming the Risk of Hacking in Selected Nationalized Banks	135
50	4.47	Measures for Overcoming the Risk of Hacking in Selected Private Sector Banks	138
51	4.48	Measures for Overcoming the Risk of Hacking in Selected Groups of Banks	140
52	4.49	Coefficient of correlation among the types of operational risks faced by various e-banking platforms.	143
53	4.50	ANOVA Result of demographic factors on operational risks in e-banking scenario of the selected banks	144
54	4.51	ANOVA Result Comparing Respondents'	144

		Expression on Prevalence of Drug Relapse Based on Educational Attainment	
55	4.52	Operational risks in e-banking Influencing the overall functioning of the selected banks (Chi-Square Test)	145

TABLE OF CONTENTS

SL. NO.	TOPIC	PAGE NO.
CHAPTER– 1 : INTRODUCTION		1-42
1.1	Overview	1
1.2	Concept of E-Banking	6
1.3	Risks Related to Internet Banking	13
1.4	Approaches for Secured E-Banking Services	16
1.5	Operational Risk Management Frameworks in Banking Sector	19
1.6	Components of Operational Risks in E-Banking Scenario	22
1.7	Managing and Controlling Risks in E-Banking	26
1.8	Regulatory Landscape of E-Banking in India	32
1.9	Internet Risk Management Practices in India	35
1.10	Statement of Aim	36
1.11	Need and Scope of the Study	37
1.12	Objectives of the Study	38
1.13	Hypotheses of the Study	38
1.14	Variables	39
1.15	Operational Definition	39
1.16	Limitations of the Study	40
1.17	Delimitation of the Study	41
1.18	Plan of Work	41
CHAPTER– 2 : REVIEW OF LITERATURE		43-65
CHAPTER– 3 : RESEARCH METHODOLOGY		66-73
3.1	Introduction	66
3.2	Theoretical Framework	66

3.3	Research Design	69
3.4	Population of the Study	69
3.5	Sampling Technique	69
3.6	Sample of the Study	70
3.7	Sources of Data	71
3.8	Data Collection Procedure	71
3.9	Statistical Techniques Used	72
3.10	Reliability of Scale	72
CHAPTER– 4 : DATA ANALYSIS AND INTERPRETATION		74-145
4.1	Results of Human Resource Oriented Operational Risks	74
4.2	Results Related to Information Technology (IT) Oriented Operational Risks	106
4.3	Hypothesis Testing	143
CHAPTER– 5 : CONCLUSION, RECOMMENDATIONS AND FUTURE SCOPE		146-157
5.1	Conclusion	146
5.2	Findings of the Study	148
5.3	Suggestion of the Study	151
5.4	Recommendations of the Study	153
5.5	Future Scope of the Study	156
REFERENCES		158-164
Chapter 1		158
Chapter 2		160
BIBLIOGRAPHY		165-172
ANNEXURE		173-179
LIST OF PUBLICATIONS		

ABSTRACT

By making banking more accessible and convenient, e-banking has changed the face of the financial industry. Yet, technology has also brought about a range of operational concerns that might compromise the safety and effectiveness of banking operations. This research delves into the many operational risks linked to online banking, with a particular emphasis on how these risks affect the efficiency and effectiveness of financial institutions. The study finds and classifies several operational risks, such as HR-oriented and IT-oriented risks, by evaluating data from various e-banking platforms.

This study's population consists of financial institutions in India, namely those belonging to the State Bank Group, the Nationalized Banks, and the Private Industry Banks. The judgment sampling technique is used in this study. The 350 officials are selected at simple random sampling method from among the participating banks in Hyderabad, Telangana, with 35 representatives from each. In order to determine how these risks affect bank operations, the research uses several statistical methods, such as ANOVA and correlation analysis. There are noticeable differences in the kinds of dangers between platforms, and the results show how demographic characteristics affect the frequency and control of these risks. The research also looks at the relationship between operational risk reduction and the efficacy of risk mitigation strategies that have been put in place.

This research delves deeply into the operational hazards of online banking by methodically investigating different aspects of risk management at chosen financial institutions. Technical breakdowns, security breaches, and human mistake are some of the operational hazards that are common in online banking. The study goes on to list the causes of these dangers, such as weak internal controls, external threats, and vulnerable systems. The research sheds light on the difficulties financial institutions have in sustaining safe and effective online banking operations by investigating the effects of these operational risks on the efficiency and effectiveness of banks. An all-encompassing framework for risk management is provided by the inquiry, which goes beyond only identifying risks to define the criteria needed for successful monitoring, control, and detection. The report concludes with an analysis of the methods used to

reduce operational risks and practical suggestions for how risk management techniques and e-banking system resilience might be improved.

In light of the specific difficulties associated with online banking, the results highlight the importance of developing risk management plans tailored to this sector. In order to help financial institutions, traverse the digital banking environment, the study closes with suggestions for improving risk management techniques. These practices will increase the overall security and operational efficiency of e-banking systems.

CHAPTER -1

INTRODUCTION

1.1 OVERVIEW

The use of information technology has evolved into an instrument that is essential for modern businesses. The modern banking industry operates in an environment that is highly globalized, liberalized, privatized, and one that is competitive. Banks are required to make use of information technology in order to continue existing in current climate. Technology has brought about a new paradigm in business. The way in which it contributes to the enhancement of the services provided by the banking industry is becoming increasingly significant. The banking business in India has been witness to a remarkable amount of progress as a result of the extensive changes that are taking place in the field of information technology. A result of such a forward-thinking development is the emergence of electronic banking, as reported by the Asia Pacific Journal of Marketing. The majority of the problems that the banking industry is currently facing are seen to be able to be solved by modern technology. The credit-to-GDP ratio in India is one of the lowest among developing countries, which means that the country is still considered to be relatively unbanked even at the present time.

Thus, banks are confronted with the combined difficulty of increasing their market share while simultaneously experiencing rapid expansion. With the assistance of technology, the banking business is able to perform two tasks at once, so achieving a double win. As a result of the tremendous advancements that have been made in the sphere of technology, the globe has become a global village, and the banking business has undergone significant transformations as a result of these advancements. The brick-and-mortar manner of branch banking has been replaced by the click-and-order channel mode due to technological advancements. A significant amount of change has occurred in the way that banks operate over the course of the past twenty years. Bank operations have gotten significantly more technologically advanced in today's world. At the present time, electronic technology is playing a significant role in the world of business, particularly in the activities that are associated with banking. E-banking, often known as electronic banking, is the most recent delivery route where banking services can be obtained. The term "e-banking" is defined differently by different researchers. This is due to the fact that electronic banking encompasses a variety of

services that enable consumers of banks to make information requests and carry out the majority of retail banking services through the use of a computer, television, or mobile phone. In actuality, it has effectively "opened" twenty-four hours a day, seven days a week across the whole week. Without having to wait in line or on hold for telephone banking services, customers are able to complete their routine financial tasks without any inconvenience. Electronic banking provides customers with the ability to check the balances in their accounts, transfer funds between accounts, pay bills electronically, apply for loans, download information about their accounts onto their own computers, trade stocks or mutual funds, and view images of their checks and deposit slips. E-banking also allows customers to pay bills electronically.

The use of electronic banking is becoming increasingly widespread, and many financial institutions are employing it in order to lower the expenses associated with having workers physically serve customers, shorten the processing durations, increase the speed, improve the flexibility of business transactions, and provide better service overall. In addition, thanks to the rapid development of various other forms of electronic services, the majority of which are based on the Internet, there has been a surge in interest in online banking services. Online banking has played a significant role in the provision of an online transaction platform that supports a wide range of e-commerce applications, including online shopping, online auctions, and Internet stock. This is due to the rapid growth of Internet technology, which has enabled online banking to play a major role in the e-payment sector.

Financial institutions have been utilizing the Internet as one of its distribution channels due to the fact that Internet Banking services are advantageous to both the financial institutions and their consumers. As a result of its ability to assist banks in realizing cost savings, it has emerged as the most lucrative distribution channel for financial institutions. For the convenience of the consumers, it is possible to carry out their bank transactions or get in touch with their banks more quickly, whenever and wherever they choose. Electronic service is becoming a feasible option for contact between financial service providers and their consumers. Many organizations in the financial services sector have been quick to integrate Internet capabilities, and this trend is expected to continue. Clearly, in order to increase the number of customers who use internet banking, financial institutions need to make significant

enhancements that meet the concerns of customers. As a result of the proliferation of e-banking, also known as electronic banking, the dynamic structure of the global financial system has been altered. This has occurred as a result of a shift away from analog platforms and toward digital platforms for the delivery of traditional banking services. One of the countries with one of the world's most rapidly rising economies, India, has seen a significant rise in the number of people using online banking and financial services. However, this paradigm shift brings along additional challenges, including operational dangers, which were not previously present.

Within the realm of electronic banking, the operational risk spectrum, which encompasses internal processes, systems, human factors, and external events, has emerged as a significant focal point of attention. As the financial sector in India adjusts to the digital revolution, it is becoming increasingly vital to have a theoretical framework that is capable of effectively managing operational risks in electronically banking. The purpose of this introduction discourse is to investigate the technical fabric that constitutes this sector, as well as the fundamental concepts, international frameworks, regulatory aspects, and complexity of e-banking operational risk management in the context of India. The exponential growth of online banking is a clear indication of the revolutionary potential that technology possesses in India's financial sector. The dramatic rise of online banking in the country over the course of the past decade can be attributed to a number of factors, including the efforts of the government to encourage the development of a digital economy, the increasing sales of smartphones, and the broad availability of internet connection. Online banking, mobile banking applications, and other cutting-edge financial technologies are gradually displacing more traditional banking institutions that are located in brick-and-mortar locations. Not only has this shift altered the expectations of clients, but it has also prompted financial institutions to reevaluate their risk management strategies from the ground up.

A fundamental aspect of the digital transformation is the concept of operational risk, which is not only complicated but also extends beyond the conventional worries that banks have with credit and the market. The e-banking business is subject to a variety of operational risks, including but not limited to technological failures, cyberattacks, data breaches, human errors, and inefficiencies in the whole process. Whenever

something goes wrong with online banking, it has the potential to have a devastating impact not only on the bottom lines of the banks, but also on the faith that their consumers have in the entire digital banking system. In view of the significance of operational risk in this context, it is of the utmost necessity to build a theoretical framework that is capable of managing the complexities of operational risk management in the online banking sector of India. Due to the fact that operational risk has been of such long-standing significance to the stability of financial institutions, international regulatory authorities have devised frameworks to assist with risk management.

The Basel Committee on Banking Standards (BCBS), a significant participant in the process of developing international banking standards, has formulated guidelines for the management of operational risk within its Basel II and Basel III frameworks. These regulations are founded on a three-pronged strategy that consists of market discipline, periodic supervisory assessments, and required minimum capital requirements. The theoretical framework for managing operational risks in online banking in India is in accordance with the principles outlined by the BCBS, within this worldwide framework. This is in recognition of the fact that there is a need for a risk management strategy that is both systematic and comprehensive. When developing the theoretical underpinning for operational risk management in India's e-banking sector, it is important to take into consideration both global frameworks and norms that are not unique to any particular company.

A complete viewpoint on risk management is provided by the ISO 31000 Risk Management Standard, which places an emphasis on the establishment of a framework for risk management that is applicable throughout an entire organization. When it comes to the process of designing risk management strategies for the online banking business, this industry-wide standard is an excellent resource. In addition to these principles, the Enterprise Risk Management (ERM) framework, which is a comprehensive model for the management of hazards inside an organization, helps to augment these guidelines. Specifically, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) is the one responsible for its development. The special characteristics of the regulatory environment in India have a considerable impact on the theoretical framework that is used for the management of operational

risk in online banking organizations. In its capacity as India's principal regulatory agency, the Reserve Bank of India (RBI) has taken the initiative to increase the capacity of banks to withstand shifting risk conditions through the implementation of rules and regulations. The regulatory framework of India not only takes into account the opportunities and dangers that are brought about by the dynamic nature of the country's financial landscape, but it also adheres to the standards that are established internationally. Because of this, the theoretical framework needs to take a thorough look at the rules and regulations, including the recommendations made by the Reserve Bank of India (RBI), in order to guarantee that the practices of operational risk management are not only legal but also relevant to the banking industry in India.

Because of the technical nature of online banking in India, any theoretical framework for operational risk management needs to study the intricate interaction that exists between new technologies and the procedures that are already in place to reduce risk. Using outdated technologies, having inadequate cybersecurity, and the likelihood of systems malfunctioning are all examples of the types of risks that fall under the category of technological risk, which is a subclass of operational risk.

Because India is making such a strong push toward digitalization, it is essential to have a solid understanding of how technology influences operational risk management in the national context. When it comes to proactively managing operational risks and discovering ways to mitigate them, the utilization of data analytics, machine learning, and artificial intelligence is becoming an increasingly significant tool. There is more to the theoretical framework for operational risk management in e-banking in India than merely an intellectual exercise; rather, it is a practical reaction to the changing dynamics of the financial system. The management of operational risks in the e-banking landscape of India brings a number of opportunities as well as significant obstacles. Through the investigation of international frameworks, industry standards, regulatory imperatives, and technical imperatives, this theoretical foundation intends to shed light on the aforementioned challenges. It is anticipated that as the journey continues, it will throw light on operational risk management, delivering insights that are both academically valuable and practically necessary for the purpose of maintaining the dependability and security of online banking in India.

1.2 CONCEPT OF E-BANKING

The introduction of electronic banking, often known as e-banking, has brought about a significant shift in the relationship that exists between financial institutions and their clientele. The advent of the internet and the digitalization of financial services has brought about a transformation in the paradigms of traditional banking. This transformation has provided customers with an unprecedented access to a wide variety of services, convenience, and accessibility. E-banking encompasses a variety of services, including mobile banking, online banking, and digital wallets, in the context of the modern day. Users are able to manage their finances, gain access to their accounts, and conduct financial transactions with an easiness that has never been seen before thanks to these channels.

In the realm of electronic banking, one of the most important pillars is online banking, which is a platform that enables users to access their accounts and carry out a variety of financial activities through the use of the internet. Customers now have the option of banking online through banks' secure websites, which is a convenient service. This makes it possible for consumers to perform a variety of banking tasks from the convenience of their own homes, such as monitoring the balances of their accounts, transferring money, paying bills, and also more.

Banks have reshaped their interaction with their customers by becoming more active and dynamic as a result of the move from traditional brick-and-mortar banks to digital ones. This transition has also brought about a new age of convenience.

Another significant component of electronic banking is mobile banking, which makes use of the fact that people always have access to their cellphones in order to provide financial services while they are on the move. Mobile banking applications are developed and managed by financial institutions.

These applications enable customers to perform a variety of tasks, such as checking their account balances, making mobile payments, and even applying for loans at their convenience. Mobile banking has gained popularity in recent years, particularly in regions where there is a high concentration of smartphones. This is because mobile banking allows users to manage their accounts from any location and at any time.

The use of digital wallets as a means of conducting electronic transactions has become increasingly widespread in tandem with the rise of mobile banking and internet banking. E-wallets, which are also known as digital wallets, allow users to store their financial information in a secure manner and then use those wallets to pay for goods and services that are purchased online. The majority of these wallets come with a variety of additional features, including loyalty programs, discounts, and the capability to interact with other financial products. Payment procedures have been simplified as a result of the growth of digital wallets, which has enabled the widespread adoption of cashless transactions. This is in line with the greater global trend toward a cashless society.

E-banking has the potential to save customers and financial institutions time and effort, which is beneficial for both the clients and the institutions' bottom lines. Electronic cash transfers and online account management are two instances of automated operations that improve operational agility and save money by removing the need for human interaction. Both of these procedures are examples of automated operations. Banks are also able to contact a greater number of individuals through the use of electronic banking systems, which enables them to give financial services to locations that are either underserved or located at a great distance. Another advantage of digitizing banking services is that it enables financial institutions to respond rapidly to shifts in the market and the requirements of their customers. This is made possible through the utilization of real-time data analytics.

Despite this, the rapid growth of online banking has resulted in a number of negative consequences, the most prominent of which is the increased emphasis placed on the protection of online information. Because of the growing digitalization of financial activities, the banking industry is one of the most susceptible to cyberattacks. This is because it is easier for thieves to obtain sensitive data, which makes the banking business one of the most vulnerable industries. Both the customers of financial institutions and the organizations themselves are in grave danger when there is a breach in security, loss of data, or fraudulent behavior. In addition to the steady growth of online banking, it is essential to prioritize the implementation of robust cyber security measures, encryption techniques, and continuous monitoring in order to maintain the integrity of the international financial system.

In order to guarantee that financial institutions adhere to regulations that promote transparency, safety, and equity, regulatory frameworks are of utmost importance when it comes to considering the characteristics of electronic banking. Regulation authorities all over the world have set rules in order to guarantee the security of online banking, the personal information of customers, and the transactions that take place in the financial sector electronically. In India, for instance, the Reserve Bank of India (RBI) has published regulations that describe the safety measures that financial institutions are required to follow in order to protect the personal information of their customers and the electronic transactions that they conduct. The observance of these standards is not only the law, but it is also vital for the establishment and maintenance of confidence in the online banking system.

The use of electronic banking has a considerable impact on the socioeconomic system, as it extends beyond the sphere of individual transactions and has an impact on bigger economic patterns. It is possible for people living in rural or underserved areas to gain access to formal financial services through the use of electronic transactions. This has implications for financial inclusion because e-banking makes it possible to have a cashless economy. Through the reduction of the demand for actual currency, we may contribute to the development of a more transparent and accountable monetary system. This will be accomplished by reducing the prevalence of illegal activities like as money laundering, tax evasion, and black markets.

The progression of technology will have a significant impact on the future of digital financial services, particularly for the reason that online banking is continuing to advance. E-banking systems are increasingly utilizing data analytics, artificial intelligence (AI), and machine learning in order to enhance the user experience, personalize services to each individual, and identify suspicious behavior that may be an indication of fraudulent activity. For the purpose of providing an additional layer of protection against cybercriminals, biometric verification techniques such as fingerprint and facial recognition are being utilized.

Examples of ongoing innovations that are expected to have an impact on the future of online banking include block chain technology and cryptocurrencies. The decentralized and secure ledger technology that blockchain possesses has the potential to revolutionize the recording and verification of financial transactions in a number of

ways. Two of these ways include increased transparency and a lower chance of fraud. Even though they are still relatively new, cryptocurrencies present exciting opportunities for the development of digital finance. They pose a threat to the established fiat currencies that have been in use for a long time and may even redefine what it means to deal in money.

The financial industry has been revolutionized by e-banking, which has changed the way in which individuals and businesses engage with banks. E-banking has also leveled the playing field in terms of accessibility to banking services. The connection that banks have with their customers has been revolutionized as a result of the proliferation of e-banking technologies such as mobile banking, internet banking, and digital wallets. Additionally, banks have been able to streamline their operations as a result of these emerging technologies. It is imperative that we remain attentive and develop robust risk management strategies in order to address the issues that are associated with online banking, particularly in the realm of cyber security. Nevertheless, the benefits are readily apparent. The rapid development of technology has opened up a wide range of opportunities for the implementation of electronic banking in the future. Innovations that will have an effect on the financial industry are poised to impact this sector, which is prepared to undergo further transformation.

➤ **Definitions of E-banking and E-money**

Electronic banking is the provision of retail and small value banking goods and services through electronic channels. E-banking is also known as online banking. Some examples of such products and services are the acceptance of deposits, the supply of loans, the management of accounts, the provision of financial advice, the payment of bills electronically, and the provision of additional electronic payment products and services such as electronic money (which will be defined in a separate section below). Electronic banking is characterized by two key aspects: the type of the delivery channels via which activities are undertaken, and the mechanism by which clients can acquire access to those channels. The terms "closed" and "open" networks are frequently used to refer to distribution channels. The term "closed networks" refers to networks that restrict access to participants (consumers, merchants, financial institutions, and third-party service providers) who are bound by agreements on the terms of membership. There are no membership criteria for "open networks" in this

regard. Point-of-sale terminals, automated teller machines, telephones, personal computers, smart cards, and other devices are examples of the types of access devices that are currently in widespread use and can be used to offer clients with electronic banking goods and services.

The phrase "e-money" refers to "stored value" or prepaid payment systems that can be used to execute payments through point-of-sale terminals, direct transfers between two devices, or across open computer networks such as the Internet. Product categories that fall under the category of "stored value" include "hardware" or "card-based" mechanisms (also known as "electronic purses") and "software" or "network-based" mechanisms (also known as "digital cash"). There is a distinction between "single-purpose" and "multi-purpose" stored value cards. Single-purpose cards, such as telephone cards, are utilized for the purpose of purchasing a single category of goods or services, or products from a single vendor. On the other hand, multi-purpose cards can be utilized for a wide range of purchases from several suppliers. It is possible for banks to take part in electronic money schemes by acting as issuers; however, they may also perform multiple other functions. Among these are the distribution of electronic money that has been issued by other entities, the redemption of the proceeds from transactions using electronic money for merchants, the management of the processing, clearing, and settlement of electronic money transactions, and the maintenance of records of transactions.

➤ **Types of Internet Banking**

Understanding the various types of Internet Banking products will help examiners assess the risks involved. Currently, the following three basic kinds of Internet banking are being employed in the marketplace:

- **Informational:** This is the most fundamental level of banking for the internet. The bank typically maintains marketing information for the bank's products and services on a server that is separate from the rest of the network. Given that informational systems often do not have a path between the server and the bank's internal network, the risk is considered to be relatively minimal. Either the bank itself or a third party can be responsible for providing this level of Internet banking. The server or website may be susceptible to modification, despite the

fact that the risk to a bank is quite modest. It is therefore necessary to have appropriate safeguards in place in order to prevent unauthorized changes from being made to the server or website of the bank.

- **Communicative:** The customer and the bank's systems are able to engage with one another through the use of this particular kind of Internet banking services. It is possible that the engagement will consist solely of electronic mail, inquiries about accounts, and applications for loans, or updates to static files. In comparison to informational systems, the risk associated with this setup is significantly larger due to the possibility that these servers have a connection to the bank's internal networks. For the purpose of preventing, monitoring, and notifying management of any unauthorized attempt to access the bank's internal computer systems and networks, appropriate controls need to be put into place. In this setting, virus controls also become much more important than they were before.
- **Transactional:** Customers have the ability to carry out transactions once they reach this level of Internet banking. Due to the fact that there is generally a connection that connects the server to the internal network of the bank or the outsourcer, this design is the one that poses the greatest risk and requires the most stringent and comprehensive controls. Transactions involving customers can involve things like accessing accounts, paying bills, transferring payments, and other options.

➤ **Growth in Internet Banking**

In order to analyse their technology and evaluate their plans for electronic commerce and Internet banking, banks are being motivated to do so by a variety of criteria, including competitive cost, customer service, and demographic concerns. Numerous researchers anticipate a substantial increase in the number of clients who use products and services offered by online banks. National banks face the problem of ensuring that the cost savings resulting from the implementation of Internet banking technology are sufficient to more than compensate for the expenses and dangers that are connected with conducting business in cyberspace. The following are some of the reasons that have contributed to the significant rise in the use of internet banking over the course of the past few years.

- **Competition:** The most important factor that is driving the growing usage of Internet banking technology, according to studies, is the pressure from competitors. This factor ranks higher than the reduction of costs and the enhancement of revenue, which are in second and third place, respectively. Online banking is seen by financial institutions as a means of retaining their current clientele while also luring in new customers.
- **Cost Efficiencies:** Because of the Internet, national banks are able to provide banking services at transaction costs that are far lower than those of traditional branches. Depending on the delivery channel that is utilized, the actual expenses that are incurred to carry out a transaction will differ. There is an expectation that these expenses will continue to decrease. There is an abundance of compelling reasons for national banks to create the technologies that will enable them to provide banking products and services through the channels that are the most efficient in terms of cost. Nevertheless, national banks must use caution when making decisions regarding products. The creation and on-going costs connected with a new product or service should be factored into the decision-making process of management. These costs should include the costs of technology, marketing, maintenance, and customer support operations. The management will be able to practice due diligence, make judgments that are more informed, and evaluate the profitability of their business venture with the assistance of this.
- **Geographical Reach:** Internet banking makes it possible to have more meaningful interactions with customers by expanding geographical reach and reducing the cost of delivery methods. In point of fact, there are some financial institutions that conduct their business solely through the use of the Internet; these institutions do not have conventional banking offices and instead only communicate with their customers through the internet. Other financial institutions are turning to the Internet as an alternate delivery channel in order to communicate with their present clientele and engage with potential new clients.
- **Branding:** Developing relationships is a strategy priority for a number of national banks throughout the world. The technology and products of internet banking can give a mechanism for national banks to create and maintain an ongoing relationship with their consumers by providing quick access to a wide variety of

products and services. This can be accomplished by providing clients with a variety of banking options. Through the utilization of brand identity and the provision of a comprehensive range of financial services, banks have the objective of fostering client loyalty, facilitating cross-selling and enhancing repeat business for their customers.

- **Customer Demographics:** Customers of national banks are able to take use of a diverse range of banking alternatives thanks to the availability of internet banking. In order to complete their banking transactions, certain clients will resort to using traditional branches. Performing their banking transactions in this manner is, for many people, the most convenient option available to them. It is important to these clients that they have direct interaction with the company. Customers that are early adopters of new technology that are introduced to the market are another type of consumer. These customers were the first to acquire personal computers and the first to use them in the course of their banking operations. The customer base of financial institutions will continue to undergo demographic shifts. The difficulty that national banks face is in gaining an understanding of their customer base and locating the optimal combination of distribution channels in order to provide products and services to their various market segments in a manner that is profitable.

1.3 RISKS RELATED TO INTERNET BANKING

The use of internet banking presents national banks with additional issues in terms of risk management. When seen from the perspective of regulatory authorities, risk is the possibility that occurrences, whether anticipated or unanticipated, may have a negative effect on the earnings or capital of the bank. For the purpose of effectively managing a banking routine operation, it is necessary for the authority of the bank to have an understanding of and control over the risk culture of the bank. As a result, the first thing that we are going to do in our research is study the different kinds of dangers that are associated with internet banking. The following is a list of the numerous kinds of dangers that are connected to using the internet for banking.

Credit Risk: Credit risk is the risk that, in the event that an obligatory fails to meet the terms of any contract with the bank or otherwise fails to perform as agreed upon,

it poses a threat to the earnings or capital of the bank. Credit risk can be found in any activity in which the success of the activity is dependent on the performance of the counterparty, issuer, or borrower. If funds from a bank are extended, committed, invested, or otherwise exposed in any way through actual or implied contractual arrangements, this situation develops regardless of whether the funds are on or off the balance sheet of the bank.

Interest Rate Risk: The danger that is posed to earnings or capital as a result of fluctuations in interest rates is referred to as Internet rate risk. There is a difference between the timing of changes in interest rates and the timing of cash flows, which can lead to interest rate risk. Internet banking has the potential to attract deposits, loans, and other interactions from a larger pool of potential clients than traditional means of marketing that are now available. The necessity for managers to maintain proper asset and liability management systems, including the ability to react swiftly to changing market conditions, is reinforced by the fact that they have greater access to consumers who are primarily looking for the best rate or term.

Liquidity Risk: The danger to earnings or capital that arises from a bank's inability to satisfy its commitments when they come due without suffering losses that are unacceptable is referred to as liquidity risk. Financial institutions face this risk. A bank runs the risk of experiencing liquidity risk when it fails to notice or respond to changes in market conditions that have an impact on the bank's capacity to liquidate assets in a timely manner while minimizing the amount of value that is lost. The asset/liability and loan portfolio management systems that are recommended for use with internet banking products should be suitable for use with these products. When considering the volume and variety of actions that occur on internet accounts, it may be necessary to conduct a more thorough monitoring of liquidity as well as changes in deposits and loans.

Price Risk: There is a danger to earnings or capital that is referred to as price risk. This risk is caused by fluctuations in the value of a traded portfolio of financial instruments. In the interest rate, foreign exchange, equities, and commodities markets, the risk is caused by market making, dealing, and taking positions in those markets. As a consequence of operations related to Internet banking, financial institutions may be exposed to price risk if they establish or develop programs for the brokering of

deposits, the selling of loans, or the securitization of assets. The maintenance of appropriate management systems is necessary in order to monitor, measure, and manage price risk in the event that assets are traded through trade activity.

Foreign Exchange Risk: When a loan or portfolio of loans is dominated in a foreign currency or when it is funded by borrowings in another currency, there is a possibility of foreign exchange risk. In certain circumstances, financial institutions will enter into multi-currency loan agreements, which provide borrowers the opportunity to choose the currency that they would like to use throughout each rollover period. There is a possibility that political, social, or economic development could exacerbate the danger of foreign exchange. It is necessary to build appropriate mechanisms in the event that the bank engages in these operations.

Reputation Risk: The impact that bad public opinion has on a company's earnings and capital, both in the present and in the future, is referred to as reputation threat. The capacity of the organization to form new relationships or provide new services is impacted as a result of this. This risk may put the institution at risk of being sued, suffering financial loss, or seeing a decrease in the number of customers it serves. In the event that a bank fails to deliver on marketing claims or fails to offer services that are accurate and timely, the bank's image may suffer. In order to ensure that their business continuity plans are comprehensive, national banks must ensure that they include the internet banking business. Performing routine tests or implementing a business continuity plan, as well as developing communication strategies with the press and the general public, can assist the bank in ensuring that it is able to effectively and immediately respond to any negative reactions from customers or the media.

Transaction Risk: There is a current and prospective risk to earnings and capital that is referred to as transaction risk. This risk is caused by fraud, error, and the failure to offer products or services, maintain a competitive position, and handle information. Transaction risk is included in every product and service that is provided, and it includes product delivery, transaction processing, system development, computer systems, the complexity of products and services, and the environment in which internal controls are implemented. When it comes to Internet banking products, there is a greater potential for a high amount of transaction risk, particularly in the event

that these lines of business are not appropriately designed, implemented, and managed.

Compliance Risk: The danger of income or capital infractions of laws, rules, regulations, recommended practices, or ethical standards is referred to as compliance risk. Compliance risk could also be referred to as non-conformance risk. Compliance risk can also occur in circumstances in which the laws or norms that govern particular bank products or actions of the bank's customers may be unclear or have not been tested. The institution runs the danger of incurring fines, civil money penalties, the payment of damages, and the nullification of contracts if it does not comply with regulations.

Strategic Risk: The current and potential impact on earnings or capital that can be attributed to unfavourable business judgments, faulty implementation of decisions, or a lack of responsiveness to changes in the industry is referred to as strategic risk. The level of risk is determined by the degree to which an organization's strategic goals, the business strategies that have been devised to attain those goals, the resources that have been deployed against these goals and the quality of implementation are compatible with one another. It is necessary to have both tangible and intangible resources in order to successfully implement company strategy. Components such as communication channels, operating systems, distribution networks, and administrative talents and capabilities are included in this category. Changes in the economy, technical advancements, competitive pressures, regulatory policies, and other aspects of the environment must be taken into consideration while evaluating the internal features of the company.

1.4 APPROACHES FOR SECURED E-BANKING SERVICES

Increasing operational risks present issues for banks and its officials, who are tasked with providing a process that can quickly settle and resolve these risks? The deliberate and active risk control in all aspects, beginning with the training of the existing employees, the utilization of better technology sources for the purpose of storing and retrieving information, the implementation of appropriate backups in each block of transactions, and the utilization of advanced software and software service providers for the purpose of resolving technical defects and solutions to erroneous transaction

processing and failed transactions due to technical difficulty are some of the remedies that are included in the risk control system. These remedies help in actually reducing the operational risks that are faced by banks that are engaged in e-operations. With the staffing of experts in the bank who are skilled and experienced in enhancing risk mitigation measures for other associated risks, the compliance risks may be resolved more effectively. This would also result in a reduction in the legal and compliance risks. It is imperative that each and every bank establish a framework for risk management that will equip them with the ability to deal with the day-to-day operational and system risks that are associated with banking transactions. It is necessary for the banks to seek the assistance of experts in order to develop an effective risk management framework that will result in improved performance. It is imperative that the information security be strengthened in order to guarantee that the customers will not lose any personal information to non-affiliated third parties. In order to achieve results that are beneficial to both the bankers and the customers, the management of the outsourcing process needs to be organized. Through the appropriate deployment of practitioners and the encouragement of individuals to participate and share information with banks regarding the challenges and risks that they encounter in banking transactions that are carried out online, the legal and regulatory hurdles can be reduced. By taking the necessary precautions and changing passwords on a monthly or quarterly basis, it is possible to mitigate the security issues that manifest themselves as a result of hacking. Users are able to avoid falling into the traps set by software, including key board loggers, when they make use of virtual key boards. When customers use the systems or personal computers at internet cafes and other public locations, it is common for them to misuse their ids and passwords for online transactions. This is something that should be noticed. Therefore, it is recommended that customers of online banking utilise personal computers (PCs) that are not under the authority of other individuals. The customers will be able to close the technical loopholes if they properly monitor the programs that are placed on their computers, restart their personal computers before using the systems, and make use of virtual key boards. Furthermore, it is recommended that they do this before utilizing the systems. In order to ensure that customers are well-informed about the numerous concerns that are associated with e-banking transactions, it is strongly recommended that the professionals working in the banking industry should organize awareness programs and "know your banking" workshops for their customers. Further, the

Reserve Bank of India (RBI), in conjunction with the banks, ought to implement the following techniques in order to address the problem of attack risk in electronic banking.

a) KYC to KYA

RBI should implement two-eye techniques by allowing banks to implement Know Your Customer (KYC) procedures. These procedures primarily concentrate on identifying, assessing, and evaluating customers based on the documents that they provide in order to obtain financial services. Additional Know Your Accounts (KYA) procedures are going to be implemented for each and every account holder (also known as a consumer) who uses the services provided by banks. A lack of awareness is one of the most significant flaws that can lead to fraudulent activities. Each and every bank that is responsible for the customers should have sessions once every month or every quarter in order to educate customers on how to make secure use of banking services and to raise awareness about fraudulent activities that occur inside the banking network.

b) Strengthening record system

The maintenance of a multi-security record system is required of banks. The account summary of transfers is now being provided by the bank. This summary includes the bank account number of the receiver, the transaction unique number, as well as the date and time of the transfer. Banks are required to disclose further information regarding the IP address, mobile app, or cell number from which the transfer is performed. Additionally, they must record the IP address of the recipient and determine whether or not the receiver has reviewed, downloaded, or received the value that was transmitted.

c) Periodic evaluation

The users of the bank should be required to physically update their account once a month. This should be done by providing a detailed summary of the transactions that have occurred, mandating the change of the personal identification number (PIN), online banking ID, password, transaction password, verifying the address, mobile

number, and the quality of debit and credit cards that are being used. Users are able to have a closer relationship with their banks as a result of this, and they are able to obtain precise information regarding the accounts that they have been using.

1.5 OPERATIONAL RISK MANAGEMENT FRAMEWORKS IN BANKING SECTOR

Financial institutions and organizations rely on operational risk management frameworks, which offer a coordinated and comprehensive approach, in order to detect, assess, and reduce operational risks. These frameworks give a comprehensive and systematic approach. The progressive creation of these frameworks, which try to assist users through the complicated terrain of operational challenges, has been influenced by a number of factors, including international standards, legislative mandates, and best practices in the field. There are a number of significant models that are included in operational risk management frameworks, and each of these models has the objective of enhancing the resilience and sustainability of businesses in their own unique way.

The operational risk management framework that was developed by the Basel Committee on Banking Supervision (BCBS) is an essential component of risk governance. This framework has been instrumental in the formation of international banking regulations and has been instrumental in the development of risk governance. The Basel Committee on Banking Standards (BCBS) established operational risk as a distinct category of risk and outlined a three-pronged strategy within of its Basel II framework, which was subsequently expanded upon in Basel III. As described in the first pillar, which focuses on minimum capital requirements, financial institutions are required to keep a level of capital that is proportional to the operational risk that they are exposed to. Within the framework of the supervisory review pillar, which is the second pillar, regulators conduct an evaluation of the internal procedures that banks have in place for controlling operational risk? As a component of the third pillar, market discipline, which encourages openness, financial institutions are required to publicly disclose information regarding the risk management measures they employ. This all-encompassing approach not only makes it simpler to assign a numerical value to operational risk, but it also emphasizes how important it is to manage risk in a manner that is both integrated and comprehensive.

The International Organization for Standardization (ISO) 31000 Risk Management Standard provides a more comprehensive perspective on operational risk management. This standard is applicable to a wide variety of industries and is relevant to numerous industries. The International Organization for Standardization (ISO) 31000 defines risk as the "effect of uncertainty on objectives" and offers a strategy for managing risks that includes identifying risks, assessing risks, treating risks, monitoring risks, and communicating about risks. Despite the fact that this standard does not pertain specifically to banking, it does offer suggestions and ideas that organizations in the financial sector may find useful. The International company for Standardization (ISO) 31000 emphasizes the importance of embedding risk management into decision-making and governance processes, which in turn supports the spread of a risk-aware culture throughout a company.

Through the implementation of their Enterprise Risk Management (ERM) framework, organizations such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) have also made substantial contributions to the field of risk management. The COSO Enterprise Risk Management (ERM) framework was primarily developed to address hazards associated with financial reporting; however, it has now expanded its scope to encompass operational risk as well. The framework is comprised of eight components: the setting of goals, the identification of events, the assessment of risks, the response to risks, the control of activities, information and communication, and monitoring. These factors are incorporated into the COSO Enterprise Risk Management framework in order to assist organizations in better comprehending risk and ensuring that risk management is in accordance with their strategic objectives.

Enterprise-wide risk management systems can be established with the assistance of the COSO Enterprise Risk Management (ERM) framework when it is applied to operational risk. As seen by the emphasis placed on the internal environment, risk management strategies are influenced by the culture, ethics, and governance of the organizing institutions. Companies have the ability to predict and evaluate potential risks by utilizing event identification and risk assessment. The risk response component is responsible for directing the construction of plans to reduce, remove, or shift such dangers. Control actions, information and communication, and monitoring

are the means by which risk management techniques can be incorporated into day-to-day operations. Monitoring makes it possible to conduct ongoing reviews and improvements to the framework for risk management of the organization.

Despite the fact that the three frameworks discussed above offer a solid foundation for operational risk management, it is vital to modify their application so that it corresponds with the particular challenges that are encountered by various businesses and industries. In the banking industry, new aspects and models are becoming increasingly relevant. One famous example is the Advanced Measurement Approach (AMA), which was developed by the Basel Committee to enable large, internationally active banks to utilize their own models for estimating regulatory capital for operational risk. This approach was devised in order to facilitate the identification of operational risk. Using a combination of loss data from the past, hypothetical scenarios, and statistical modeling, the American Management Association (AMA) adopts a more sophisticated and institution-specific approach to evaluating operational risk than traditional approaches does. This methodology is more sophisticated than conventional methods.

Additionally, the Capability Maturity Model Integration (CMMI), which is widely used in the technology and software industries, may be utilized in the process of operational risk management. The Capability Maturity Model Integration (CMMI) assesses how well an organization has developed in a variety of process domains, including risk management. The progression of an organization through the maturity stages results in an improvement in its risk management capabilities. This improvement involves a transition from reactive and ad hoc approaches to proactive and efficient processes.

Regulatory agencies have been compelled to continually update and widen their recommendations as a result of the ever-changing nature of operational risk. As an illustration, the Federal Reserve System of the United States of America offers supervisory instructions on operational risk management. These instructions cover typical practices in the areas of governance, risk assessment, measurement, reporting, and scenario analysis. For the purpose of assessing operational risk, the European Banking Authority (EBA) is in charge of regulating the Internal Capital Adequacy

Assessment Process (ICAAP) in Europe. This authority is responsible for issuing recommendations.

There is a point of intersection between the rapidly growing field of cybersecurity risk management and operational risk management frameworks. As a response to the increasing sophistication and ubiquity of cyber threats, organizations are incorporating cybersecurity risk into their operational risk frameworks. The National Institute of Standards and Technology Cybersecurity Framework is congruent with concepts from operational risk management in general, despite the fact that it places a narrow emphasis on cybersecurity. There are five basic tasks that are a part of operational risk management, and they are as follows: identify, protect, detect, respond, and recover. These are the key components of it. These functions bring to light the importance of adopting a proactive and flexible approach to the discipline of cybersecurity. The banking industry, which serves as a focal point for the establishment of operational risk management frameworks, plays an essential role in enhancing the resilience of businesses across a wide range of industries. In addition to industry-wide standards such as the BCBS and ISO 31000, the construction of a robust risk management infrastructure is a collaborative endeavor that requires the utilization of industry-specific models such as AMA and CMMI respectively. The adoption of a risk-aware mindset and close engagement with regulatory bodies are two things that businesses need to do in order to establish a culture of resilience and adapt to new circumstances. In order to navigate the complex world of operational hazards, this will be of great assistance to them.

1.6 COMPONENTS OF OPERATIONAL RISKS IN E-BANKING SCENARIO

There are a lot of distinct components that make up operational risk in e-banking, and each of these factors has the potential to be both a threat and an opportunity. This risk is complicated for financial firms that provide digital financial services.

In order to develop a comprehensive plan for the management of operational risks that takes into account the intricacies of electronic banking, it is essential to have a solid understanding of these components. There are three primary categories of operational risk in online banking: technological, human, and procedural. Each of these categories

makes a substantial contribution to the one-of-a-kind set of challenges that banks are confronted with in the current environment.

➤ **Technology Risk:**

Electronic banking is dependent on technology for its basis, and digital systems, software programs, and the interconnection of electronic platforms all present a number of risks that can be exploited by financial institutions. Cybersecurity, which is a component of technical risk, is one of the most substantial concerns that must be addressed. Phishing attempts and ransomware are two examples of the types of cyber-attacks that are becoming increasingly complicated, and they pose a rising threat to the security of online banking operations. Given the constant evolution of cyber threats, it is imperative that financial institutions implement robust defenses, maintain continuous monitoring, and take preventative measures in order to safeguard consumer data, financial transactions, and the integrity of digital systems. As a result of infrastructure flaws, the risk associated with technology is increased. Due to the complex nature of the network that electronic banking activities are dependent upon, it is conceivable for the system to have faults, outages, and interruptions. There is a possibility that a single point of failure in the IT infrastructure could result in service interruptions, financial losses, and damage to the reputation of the company. Spending money on redundant and resilient systems, testing them frequently, and having disaster recovery plans in place are all examples of things that institutions should do in order to mitigate the impact of any potential technical failures.

Due to the rapid pace of technological advancement, there is also the possibility of it becoming obsolete in the near future. E-banking systems are always evolving in order to keep up with the trends and satiate the needs of its clients. When it comes to adopting cutting-edge technology such as artificial intelligence, blockchain, and open banking APIs, there are risks involved.

Compatibility challenges, integration issues, and the likelihood of unanticipated impediments are some of the things that must be considered. It is possible for financial institutions to ensure that the adoption of new technology is in accordance with their risk appetite and the requirements of regulatory agencies if they strike a balance between innovation and risk management.

➤ **People Risk:**

One of the most significant aspects of the operational risk associated with internet banking is the people engaged, which includes employees, customers, and anyone else who may be involved. When it comes to the digital environment, one of the most fundamental worries is the likelihood of mistakes made by employees or destructive operations carried out by insiders. In order to reduce the likelihood of risks that are generated by humans, the most effective method is to cultivate a culture inside the organization that is aware of cybersecurity through the implementation of training and awareness programs. By implementing stringent access limits, job separation, and monitoring systems, it is possible to reduce the risks that are present within the organization.

Customers are exposed to risks in the form of account takeovers, identity theft, and attempts at social engineering when the human aspect is introduced into the equation. In order to prevent customers from falling victim to a variety of fraudulent schemes and scams, it is necessary to educate and make them aware of the importance of maintaining excellent cyber security hygiene. Furthermore, in order to enhance the identification verification process and enhance the overall security posture of online banking platforms, financial institutions ought to implement biometric solutions, multi-factor authentication, and secure authentication protocols.

Increasing the use of external vendors and service providers raises the risk of errors caused by human intervention. In situations when you rely on third parties to undertake duties such as cloud hosting or payment processing, you expose yourself to the possibility of being dependent on those parties. In order to prevent disruptions in operations, breaches in data security, or failure to comply with legislation, it is essential to conduct an assessment of the security policies and resilience of third parties. There is a need for comprehensive due diligence, contractual agreements, and ongoing monitoring in order to effectively manage the risk of persons inside the ecosystem of e-banking.

➤ **Process Risk:**

All of the processes that are necessary to support the operations of an online bank include everything from the processing of transactions to the enrollment of customers

and the delivery of services. Errors, inefficiencies, and vulnerabilities are all examples of process risk that can arise in the realm of online banking due to deficiencies in these operating processes. One of the most important aspects of process risk is the possibility of some kind of fraudulent activity. As more and more financial transactions are moved to digital platforms, there has been an increase in the number of fraudulent operations, such as account takeovers, phishing attacks, and payment fraud. The implementation of systems for identifying and preventing fraud, monitoring transactions, and employing algorithms to identify anomalies is absolutely necessary in order to properly manage this process risk.

Compliance risk is one of the many critical components of process risk that must be considered. The regulatory environment within which online banking operates is in a constant state of flux and is subject to periodic adjustments. There are a lot of responsibilities that fall on the shoulders of financial institutions, including consumer protection, data security, anti-money laundering (AML) regulations, and know your customer (KYC) regulations. In the event that they fail to comply, institutions run the risk of incurring legal and regulatory penalties, as well as damage to their brand and their credibility. Therefore, in order to lessen the process risk that is associated with compliance, it is necessary to make investments in compliance management systems, to assess compliance on a regular basis, and to keep abreast of changes in legislation.

New digital channels and technologies bring up issues with data security, interoperability, and system integration. These issues develop as a result of the introduction of these products. In order for e-banking platforms to function correctly, data must be able to easily flow between channels. This, in turn, is dependent on the effective integration of various systems. The complexity of integration, on the other hand, makes it possible for there to be vulnerabilities in the system, inconsistencies in the data, and failures in the system. Performing exhaustive testing, carrying out periodic audits, and adhering to industry standards for interoperability are all essential steps that must be taken in order to effectively manage the process risk that is associated with the integration of technology.

One of the most important factors that determines the efficiency of operational procedures is the quality of the experience that customers have. All failures in the customer experience, whether it be the creation of an account, the transfer of funds, or

the resolution of a dispute, have the potential to result in dissatisfaction, the loss of customers, and damage to the reputation of the business. It is recommended that financial institutions prioritize the optimization of processes, make investments in user-friendly interfaces, and implement solutions that are centered on the client in order to enhance the overall operational resilience of electronic banking systems.

In order to effectively manage the several aspects that comprise the operational risk of e-banking, it is required to employ a strategy that incorporates multiple approaches. There are three primary categories of risk that are considered to be associated with the operation of an online bank: technology, people, and procedure. Banks and other financial institutions should take the initiative to strengthen their cyber security, increase the level of security expertise among their employees, and streamline their internal procedures in order to combat the ever-changing challenges that are associated with online banking in the present day. A balance between innovation and risk management is something that institutions need to find in order to enhance their defenses against operational risks and to develop a safe and resilient environment for online banking that inspires trust among stakeholders and customers.

1.7 MANAGING AND CONTROLLING RISKS IN E-BANKING

Following the completion of a risk assessment and the establishment of a risk tolerance, the management of the bank ought to take measures to manage and control risks. This phase of a risk management process includes activities such as the implementation of security policies and measures, the coordination of internal communication, the evaluation and improvement of products and services, the implementation of measures to ensure that risks associated with outsourcing are controlled and managed, the provision of disclosures and education to customers, and the development of contingency plans. It is also the responsibility of senior management to guarantee that the staff members who are responsible for enforcing risk limits have authority that is separate from the business unit that is responsible for the electronic banking or electronic money activity. It is possible for financial institutions to enhance their capacity to regulate and manage the numerous risks that are inherent in any activity by establishing policies and procedures in written documentation and making them accessible to all relevant staff members.

1. Security policies and measures

When it comes to protecting the authenticity, integrity, and confidentiality of data and operational procedures, security refers to the mix of systems, applications, and internal controls that are taken into consideration. The establishment and execution of appropriate security policies and security measures for the processes that take place within the bank, as well as for the communication that takes place between the bank and third parties, are essential to the achievement of proper security. Controlling the danger of assaults from both the outside and the inside on electronic banking and electronic money systems, as well as the risk to one's reputation that results from security breaches, can be accomplished through the implementation of security rules and practices. A security policy is a document that outlines the aims of management to support information security and offers an explanation of the security organization that the bank has in place. Additionally, it creates criteria that specify the limits of the bank's tolerance for security risks. It is possible that the policy will set mechanisms to review policy compliance, enforce disciplinary measures, and report security violations. Additionally, the policy may identify responsibilities for designing, implementing, and enforcing information security measures. Combinations of hardware and software tools, as well as staff management, are what constitute security measures.

These types of measures contribute to the construction of secure systems and operations. When it comes to security, senior management should view it as an all-encompassing process that is only as strong as the weakest link in the process. When it comes to preventing or mitigating the effects of external and internal attacks, as well as the misuse of electronic banking and electronic money, banks have a number of different security measures from which to select.

The use of encryption, passwords, firewalls, virus controls, and employee screening are all examples of actions that fall under this category. For the purpose of preventing unwanted observation, encryption is the process of encoding data that is clear text into cipher text through the application of cryptographic methods. Utilizing strategies such as passwords, pass phrases, personal identification numbers, hardware-based tokens, and biometrics are all methods that can be utilized to control access and positively identify people.

Internal systems that are connected to open networks like the Internet are protected by firewalls, which are combinations of hardware and software that screen and restrict access from the outside world to those systems. Using Internet technology, firewalls can also be used to segregate sections of internal networks, which are referred to as intranets. The use of firewall technology, provided that it is designed and executed appropriately, has the potential to be an efficient method of regulating access and protecting the confidentiality and integrity of data. It is important that the power and capabilities of this technology be commensurate to the level of sensitivity of the information that is being secured. This is because the creation of this technology can be difficult and expensive. The design should incorporate enterprise-wide security needs, clear procedures for operation, separation of roles, and the selection of trusted persons who are responsible for the configuration and operation of the firewall. A well-planned design should include all of these elements. In spite of the fact that firewalls are designed to screen incoming messages, they do not necessarily defend against virus-infected programs that are downloaded from the internet. A result of this is that management ought to implement procedures for prevention and detection in order to lessen the likelihood of a virus attack and the destruction of data, particularly with regard to remote banking. Controls for the network, regulations for end users, user training, and software that detects viruses are all examples of programs that can be implemented to reduce the likelihood of a virus infection.

Not all dangers to security come from the outside. Additionally, electronic banking and electronic money systems must to be protected, to the greatest extent possible, against activities that are not authorized by both present and previous employees. Background checks for new employees, temporary employees, and consultants, as well as internal controls and separation of duties, are critical precautions to take in order to safeguard the security of the system. This is similar to the operations that are already performing in the banking industry.

It is possible that extra security measures could be helpful in preventing attacks and misuse of electronic money, such as counterfeiting and money laundering. A few examples of such measures are the following: online interaction with the issuer or a central operator; monitoring and tracing of individual transactions; the maintenance of cumulative records in a central database; the utilization of tamper-resistant devices

incorporated into stored-value cards and merchant hardware; and the utilization of value limits and expiration dates on stored-value cards.

2. Internal communication

It is possible to manage and control various aspects of risks, including those related to operations, reputation, and the law, provided senior management explains to key personnel how the supply of electronic banking and electronic money is meant to complement the overall aims of the bank. At the same time, the technical team should describe to senior management in a clear and concise manner how the systems are specifically built to function, as well as the strengths and limitations of the systems. Incompatibility of multiple systems within a banking organization, problems with data integrity, reputational risk connected with client unhappiness that systems did not perform as expected, and credit and liquidity risk are all examples of operational risks that can be mitigated by the implementation of such procedures. All of the policies and procedures should be provided in written form in order to guarantee adequate communication inside the organization.

To further reduce the operational risks that are caused by a lack of personnel and management experience, senior management should implement a corporate strategy that encourages continuous education and the upgrading of skills and knowledge. This policy should be in line with the rate of technological innovation. During training, employees may be required to complete technical coursework and may also be given the opportunity to stay current on significant market changes.

3. Evaluating and upgrading

Performing a thorough analysis of products and services prior to their widespread implementation can also assist in mitigating the risks associated with operations and reputation. The purpose of testing is to verify that the systems and equipment are functioning appropriately and producing the anticipated outcomes. In the process of building new applications, pilot programs or prototypes can be of great assistance. It is also possible to lessen the likelihood of system slowdowns or interruptions by instituting procedures that require regular reviews of the capabilities of the hardware and software that is already in place.

4. Outsourcing

There is a rising trend in the industry for financial institutions to concentrate their strategic efforts on their core competencies and rely on third parties that specialize in activities that are outside the scope of the bank's expertise. Outsourcing does not absolve the bank of the ultimate duty for controlling risks that are associated with its operations, despite the fact that these arrangements may offer benefits such as cost reduction and economies of scale. As a consequence of this, financial institutions ought to implement rules that will reduce the risks that are associated with their dependence on external service providers. For instance, the management of a bank ought to keep a close eye on the operational and financial performance of their service providers; make certain that the contractual relations between the parties, as well as the expectations and obligations of each party, are clearly understood and are defined in written contracts that are enforceable; and keep a contingency arrangement in place so that they can switch service providers in a timely manner, if it becomes necessary to do so. It is of the utmost significance to ensure the safety of the sensitive information held the bank. There is a possibility that the outsourcing arrangement will require the bank to disclose confidential information to service providers. It is the responsibility of the management of the bank to evaluate the capability of the service provider to maintain the same level of security as if the operations were carried out in-house. This evaluation should be carried out by reviewing the policies and processes of the service provider that are designed to secure sensitive data. In addition, supervisors might want to have the authority to independently evaluate the service providers' operational and financial performance, as well as their level of expertise, when it is deemed necessary to do so.

5. Disclosures and customer education

Disclosures and education of customers are two ways in which a bank can reduce its exposure to legal and reputational risk. Disclosures and programs designed to educate clients about how to use new products and services, prices charged for services and products, and procedures for problem and error resolution can assist financial institutions in complying with laws and regulations pertaining to customer protection and privacy. There is a possibility that disclosures and explanations on the nature of a

bank's relationship to a linked website could assist in lowering the legal risk that a bank faces as a result of issues with the services or goods offered on linked websites.

6. Contingency planning

Through the development of contingency plans that outline the bank's course of action in the case of a disruption in the supply of electronic banking and electronic money services, a financial institution can reduce the likelihood of disruptions occurring inside its internal operations, as well as in the delivery of services or products. Data recovery, alternate data-processing capabilities, emergency personnel, and customer service assistance are all potential topics that could be addressed by the strategy. In order to guarantee that backup systems continue to function effectively, they should be evaluated on a regular basis. It is imperative that financial institutions make certain that their emergency operations are just as secure as their regular production activities. One of the most significant aspects of electronic banking and electronic money is the fact that it is dependent on third-party entities such as telecommunications companies, software suppliers, Internet service providers, and hardware makers. A requirement that such service providers have backup capability might be imposed by the management of the bank. In addition, management may take into consideration further compensatory actions that it can take in the event that service providers become compromised.

Among the potential components of such plans are short-term contracts with other providers and a strategy that outlines the manner in which the bank will deal with client losses that are related with the disruption in service. Banks should also examine whether or not it would be prudent to reserve the right to switch service providers in a timely manner in the event that it becomes necessary to do so.

It is also possible that contingency planning will help to prevent reputational risk that may arise from the acts of the bank itself, or from problems that may be experienced by another institution that provides electronic banking or electronic money products or services that are comparable to those offered by the present institution. For instance, financial institutions might want to set protocols to deal with consumer issues in the event that there are disruptions to the system.

1.8 REGULATORY LANDSCAPE OF E-BANKING IN INDIA

In India, a wide variety of industries are subject to the country's regulatory environment, which is both complicated and constantly evolving. Industry sectors that fall into this category include finance, healthcare, and telecommunications. The Reserve Bank of India (RBI) is the primary regulatory agency for the banking and electronic banking industries in India. This is something that sticks out when being discussed. There has been a Reserve Bank of India (RBI) in existence since 1935, and it is still functioning effectively now. The primary functions of the Federal Reserve System include the protection of depositors' money and the economy as a whole, as well as the formulation and implementation of monetary policy. The landscape of regulations is constantly shifting as a consequence of changes in the global economy, the introduction of new technology, and developments in the financial sector.

A comprehensive and ever-evolving regulatory framework has been established by the Reserve Bank of India (RBI) for electronic banking. While at the same time ensuring the safety and soundness of the entire financial system, the objective of these laws is to encourage the growth of online banking. The "Master Directions on Digital Payment Security Controls" document, which was published by the Reserve Bank of India (RBI), is an important document in the process of developing legislation pertaining to electronic banking. It outlines the security measures that should be implemented for digital payment systems in India. These directions cover a wide variety of security problems, including risk assessment, fraud detection and prevention, consumer education, and incident reporting. The Reserve Bank of India (RBI) is committed to promoting electronic transactions that are both safe and efficient.

Data privacy and security have been thrust to the forefront of the regulatory arena as a direct result of the proliferation of online banking. As part of the Personal Data Protection Bill, which is now under consideration, efforts are being made to lay a solid groundwork for the protection of individuals' individually identifiable information. Despite the fact that this law is not directly connected to online banking, its primary objective is to regulate the manner in which financial institutions handle personal information. This includes the information of individuals who make use of their debit cards or other digital payment methods. The legislation, if it were to

become law, would add to the existing regulatory framework, making it more likely that financial institutions will be required to strengthen their data protection practices and conform to stringent privacy standards.

A number of regulatory authorities, one of which being the Reserve Bank of India (RBI), have contributed to the formation of the current condition of online banking. The Securities and Exchange Board of India (SEBI) is in charge of regulating the securities industry, which includes online trading platforms and investing platforms. The Insurance Regulatory and Development Authority of India (IRDAI), which is also in charge of the insurance business in general, is the organizational body that is responsible for regulating the digital distribution of insurance products. These regulatory authorities ensure that all electronic transactions that take place on financial markets are in accordance with the rules and regulations that have been established by coordinating their efforts.

Criminal activity on the internet and fraudulent activity online each have their own unique set of challenges, which the legal framework works to address. In light of the Reserve Bank of India's (RBI) recent publication of laws concerning the framework for cybersecurity in banks, the RBI has mandated that financial institutions establish robust cybersecurity systems. Through the implementation of the Cyber Crisis Management Plan (CCMP) and the regulatory sandbox framework, the Reserve Bank of India (RBI) has adopted a proactive approach to addressing emerging cyber threats and fostering innovation in the realm of online banking. These actions demonstrate that the government is cognizant of the threat posed by digital dangers, which are constantly evolving, and the necessity of a legislative response that is both proactive and adaptable.

The Financial Stability and Development Council (FSDC), a high-level authority that is in line with global norms, is responsible for providing overall control of the macroeconomic and financial markets in India. Co-founded by the Ministry of Finance, the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), and the Insurance Regulatory and Development Authority of India (IRDAI), the Financial Sector Development Council (FSDC) was established with the purpose of coordinating the efforts of multiple financial regulators in order to ensure the continued growth and stability of the financial sector. Because of the incorporation of

e-banking into the financial ecosystem, the function of the Financial Stability Development Corporation (FSDC) in coordinating regulatory activities and maintaining systemic stability is becoming increasingly indispensable.

India's regulatory structure, which attempts to decrease risk, places a significant emphasis on the protection of consumers and the introduction of new financial services. The Pradhan Mantri Jan Dhan Yojana (PMJDY) program, which is being implemented by the government, is in accordance with the regulatory objective of expanding access to financial services for individuals who do not currently have them. Through the implementation of initiatives such as the Bharat Bill Payment System (BBPS) by the Reserve Bank of India (RBI), it has been possible to realize the goal of providing all segments of the population with improved access to digital financial services. In order to further the broad goals of financial inclusion and empowerment, regulatory measures such as the Unified Payments Interface (UPI) and the development of small finance institutions are being implemented. The use of regulatory sandboxes is a novel approach that can be taken to foster innovation in the domain of online banking, which is constantly evolving. Companies who specialize in financial technology and banks have the opportunity to utilize the regulatory sandbox framework that has been proposed by the Reserve Bank of India in order to test out new concepts for products, services, and solutions in a supervised setting. This initiative demonstrates a forward-looking regulatory policy by acknowledging the role of technological innovation in the financial industry and seeking to strike a balance between innovation and risk management. The regulatory authorities in India are also very active participants in international forums and are fast to adopt the most effective techniques from all across the world. In order to build robust anti-money laundering and countering the financing of terrorism (AML/CFT) regimes that are applicable to online banking, Indian authorities have taken inspiration from the recommendations made by the Financial Action Task Force (FATF) on AML and CFT. The regulation of virtual currencies and the prevention of financial crimes that cross international borders are global challenges that India may be better able to address through the use of strategies that involve information sharing and collaborations that span international borders. The Indian financial industry as a whole, including online banking, is subject to a regulatory structure that is both intricate and constantly evolving.

The Reserve Bank of India (RBI) is the primary regulatory agency in India. Its duties include the protection of the country's financial system, the formulation of policy, and the provision of recommendations. The landscape of regulation is defined by the harmony that exists between the promotion of innovation, the integration of financial resources, and risk management. The regulatory framework will be modified to meet emerging risks, technological advancements, and worldwide best practices as e-banking continues to advance. This is a reiteration of India's commitment to a robust, inclusive, and secure financial ecosystem.

1.9 INTERNET RISK MANAGEMENT PRACTICES IN INDIA

According to Mohan (2003), knowledge theorists contend that risk management incorporates all four of these notions: uncertainty, risk, equivocation, and mistake. Therefore, risk management contains all of these concepts. When there is a lack of knowledge, there is uncertainty, which cannot be predicted even by chance. When information is obtained, this uncertainty transforms into risk, and it is possible to evaluate the outcome of the situation. In this day and age of ever-increasing market knowledge and understanding of prospective outcomes, risk management provides a technique of managing risk in response to the situation. Equivocality is the result of competing understandings, which makes it impossible to make a conclusion about anything for a variety of reasons. This happens despite the fact that we have access to all of the information that we require. As a result of this, financial institutions and other organizations similar to them have established control systems to reduce the number of errors, information systems to diminish the impact of uncertainty, incentive systems to address agency issues in the risk-reward framework, and cultural systems to deal with ambiguity.

When it came to risk management, Indian banks initially depended on systems that developed alongside the country's regulatory framework and accounting standards. According to Mishra (1997), the increasing rate of deregulation and the related changes in consumer behavior make banks susceptible to mark-to-market accounting. This vulnerability extends to the banking industry. As a consequence of this, Indian banks are tasked with the responsibility of developing a uniform system for risk assessment and management that is not only compatible with the aims of the business but also flexible enough to accommodate changes in the market. In today's ever-

evolving market, it is essential for financial institutions to keep a close eye on the convergence of national regulatory frameworks, changes in international accounting standards, and most importantly, changes in the business practices of their clients. Therefore, it is of the utmost importance to adhere to the precise risk management guidelines that have been established by the RBI and the BIS.

1.10 STATEMENT OF AIM

A technological revolution is currently taking place in the banking industry in India. Emerging private sector banks and foreign banks, on the other hand, have a head start on public sector banks when it comes to the implementation of technological solutions. If these financial institutions wish to continue existing in today's highly competitive market, they will need to reduce their expenses and enhance their relationships with their customers by providing superior services. There is a possibility that the expansion of economies that provide financial services could be helped by new technical advances such as enhanced payment gateways, online and mobile banking, and mobile banking. In the past, many products and services were either not available or extremely difficult for banks to supply; but, as a result of technological improvements, this is no longer the case. Indian financial institutions have made headway in this area by allowing consumers to spend money instead of actual currency whenever and wherever they want. This tendency is more visible in private and international banks, but Indian financial institutions have made progress in this regard. There is a significant amount of space for automation within these institutions, which is likely due to the fact that public sector banks are behind in integrating technology. India is still in the early stages of adopting modern financial technology such as automated teller machines (ATMs), credit cards, online banking, and mobile banking, despite the fact that these technologies are more widely used in other countries. As a result of the intensifying competition, these establishments are required to devise novel approaches that will result in transactions that are both more profitable and less expensive. In spite of the fact that technology provides the most effective answer to these problems, there is a substantial amount of concern regarding the security of the transactions. The use of technology has been one of the most important factors that has enabled the expansion of service offerings and the improvement of the convenience of products and services for customers. E-banking transactions, on the other hand, do not include any face-to-face connection between

the bank and the customer, which is the primary reason why the majority of problems, such as credit card fraud and online fraud, for example, occur. However, despite the fact that technology does assist minimize certain risks, it also brings new risks. These new risks include risks to credit, markets, operations, strategy, legality, reputation, liquidity, and in many other areas. It is possible for modifications to one area of risk to have an effect on multiple other areas of risk due to the linked nature of these hazards. The operational risk that is associated with internet banking presents a new challenge for the Indian banking sector.

So, there for the title of our study is, “*RISK ANALYSIS OF E-BANKING OPERATIONS*”.

1.11 NEED AND SCOPE OF THE STUDY

Need of the Study

The need for studying risk analysis in e-banking operations is paramount in today's digital landscape. With the increasing reliance on online banking services, understanding and mitigating risks associated with these operations are crucial for ensuring the security and stability of financial systems. E-banking faces various threats, including cyber-attacks, data breaches, and fraud, which can result in financial losses and erosion of customer trust. By conducting a comprehensive risk analysis, financial institutions can identify potential vulnerabilities, implement effective security measures, and develop robust contingency plans to safeguard against threats. Such studies not only protect the interests of banks and their customers but also contribute to the overall resilience of the financial ecosystem in the digital age.

Scope of the Study

The scope of studying risk analysis in e-banking operations encompasses a wide range of aspects crucial for understanding and managing the risks inherent in digital financial transactions. It includes examining various types of risks such as cyber threats, data breaches, identity theft, transactional fraud, and operational vulnerabilities specific to e-banking platforms. Additionally, the scope extends to evaluating the effectiveness of existing security measures, identifying potential gaps or weaknesses in the current systems, and proposing strategies for enhancing the

resilience of e-banking operations against emerging threats. Furthermore, the study may involve analyzing regulatory frameworks, industry standards, and best practices related to risk management in e-banking to ensure compliance and alignment with established guidelines. Overall, the scope aims to provide a comprehensive understanding of the risks associated with e-banking and to offer insights into developing robust risk mitigation strategies for financial institutions operating in the digital realm.

1.12 OBJECTIVES OF THE STUDY

The present study aims to examine the selected operational risks in e-banking in the selected banks. In this broader framework, the following are the specific objectives of the study:

1. To study the various types of operational risks in e-banking.
2. To identify the factors responsible for operational risks in e-banking in the selected banks.
3. To examine the impacts of operational risks in e-banking on the functioning of the selected banks.
4. To identify the parameters for identification, monitoring and control of operational risk in e-banking.
5. To analyze the measures for overcoming the operational risks in e-banking in the selected banks.

1.13 HYPOTHESES OF THE STUDY

H1: There is a significant difference in the types of operational risks faced by various e-banking platforms.

H2: There is a significant impact of demographic factors on operational risks in e-banking scenario of the selected banks

H3: There is a statistically significant relationship between the measures implemented and the reduction of operational risks in e-banking within the selected banks.

H4: There is a significant effect of operational risks in e-banking on the overall functioning of the selected banks.

1.14 VARIABLES

Following are the variables of the study: -

Dependent Variables:

- Operational Risk Levels

Independent Variables:

- Technology Infrastructure
- Security Protocols
- User Behaviour

1.15 OPERATIONAL DEFINITION

1. **Risk Analysis:** The systematic process of identifying, assessing, and evaluating potential risks and uncertainties associated with electronic banking operations. It involves analyzing various factors such as cyber security threats, operational failures, regulatory compliance issues, financial risks, and reputation risks to understand their likelihood and potential impact on e-banking systems and services.
2. **E-Banking Operations:** The suite of electronic banking activities and services offered by financial institutions to customers through digital channels such as internet banking, mobile banking, and electronic fund transfers. E-banking operations encompass a wide range of activities, including account management, fund transfers, bill payments, loan applications, and investment transactions, conducted electronically without the need for physical presence at a bank branch.
3. **Risk Identification:** The process of systematically identifying and cataloging potential risks and vulnerabilities inherent in e-banking operations. This involves identifying various internal and external factors, events, and circumstances that

may pose risks to the integrity, confidentiality, availability, and reliability of e-banking systems and services.

4. **Risk Assessment:** The systematic evaluation of the likelihood and potential impact of identified risks on e-banking operations. Risk assessment involves analyzing factors such as the frequency of occurrence, severity of consequences, and effectiveness of existing controls and safeguards to determine the level of risk exposure and prioritize risk management efforts.
5. **Risk Mitigation:** The process of developing and implementing proactive measures and controls to reduce the likelihood and impact of identified risks on e-banking operations. Risk mitigation strategies may include implementing cyber security controls, enhancing operational processes, ensuring regulatory compliance, managing financial exposures, and enhancing reputation management practices to mitigate risks effectively.
6. **Regulatory Compliance:** The adherence to laws, regulations, and industry standards governing electronic banking activities and data privacy. Regulatory compliance ensures that financial institutions comply with applicable legal and regulatory requirements, such as the Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and the Cyber Security Framework developed by the National Institute of Standards and Technology (NIST), to mitigate regulatory risks and uphold the integrity and trustworthiness of e-banking operations.

1.16 LIMITATIONS OF THE STUDY

1. The complexity of e-banking systems, including interconnected networks, multiple digital platforms, and third-party service providers, poses significant challenges in operational risk analysis.
2. Analysing and understanding the intricate dependencies and interactions within e-banking systems can be daunting, leading to difficulties in identifying and assessing all potential operational risks comprehensively.

3. Operational risk in e-banking is heavily influenced by cyber threats, which are constantly evolving in sophistication and complexity.
4. Cybercriminals continually adapt their tactics to exploit vulnerabilities in e-banking systems, making it difficult for risk analysts to anticipate and mitigate emerging operational risks effectively.
5. E-banking despite robust technological controls, operational risks can arise from employee mistakes, negligence, or intentional misconduct.
6. Financial institutions operating in multiple jurisdictions must navigate a complex regulatory landscape, adhering to various laws, regulations, and industry standards governing e-banking activities and data privacy.

1.17 DELIMITATION OF THE STUDY

This study on the risk analysis of e-banking operations is delimited to examining the specific risks associated with online banking platforms, including cybersecurity threats, data privacy concerns, and operational vulnerabilities. The focus is on identifying and analyzing risks within the context of consumer interactions and the technological infrastructure of e-banking systems.

The study does not extend to traditional banking operations or the risks associated with physical banking channels. Additionally, the geographical scope is limited to e-banking practices within a specific region or country, and the study does not explore global e-banking risks or those related to emerging financial technologies such as cryptocurrencies.

1.18 PLAN OF WORK

CHAPTER 1: INTRODUCTION

This chapter sets the stage for the research by providing an overview of e-banking, its significance in the contemporary financial landscape, and the inherent risks associated with its operations. It outlines the research objectives, questions, and the scope of the study, establishing a clear foundation for subsequent chapters.

CHAPTER 2: REVIEW OF LITERATURE

This chapter delves into existing scholarly works and studies related to e-banking and risk management. It critically analyzes previous research findings, identifying gaps in the literature that the current study aims to address. It covers theoretical frameworks and models that underpin risk analysis in the context of e-banking.

CHAPTER 3: RESEARCH METHODOLOGY

This chapter details the research design, including the methods and techniques employed to collect and analyze data. It describes the sampling strategies, data sources, and tools used for gathering information on e-banking risks. It also discusses the validity and reliability of the chosen methods, ensuring a robust and credible research process.

CHAPTER 4: DATA ANALYSIS AND INTERPRETATION

This chapter presents the findings from the data collected, employing statistical and analytical tools to interpret the results. It provides a comprehensive analysis of the risks identified in e-banking operations, discussing their implications and how they align with or differ from the existing literature.

CHAPTER 5: CONCLUSION, RECOMMENDATIONS AND FUTURE SCOPE

This chapter summarizes the key findings of the study, drawing conclusions based on the data analysis. It discusses the practical implications of the research for e-banking operations and suggests recommendations for mitigating identified risks. It also highlights potential areas for future research, providing a pathway for ongoing investigation into e-banking risk management.

CHAPTER 2

REVIEW OF LITERATURE

Ekmath, Shankarrao (2007) the advancements that have been made in information and communication technology have made it possible for financial institutions to offer their electronic services to customers located in remote areas currently. Online banking, online bill payment, electronic financial transfers, and automated teller machines (ATMs) are all examples of technologies that are contributing to the development of electronic banking, often known as e-Banking. As the use of electronic banking services and e-commerce, which includes the use of electronic money, continues to expand, there is a possibility that opportunities for banks may significantly expand. In a short amount of time, online banking may emerge as the principal source for all matters pertaining to monetary matters. Conventional banking is frequently expanded upon by electronic banking, which makes use of the internet as a digital conduit for the provision of financial goods and services. In the present day, banking is being rethought and re-engineered with the assistance of information technology. It is reasonable to believe that in the future, customers will have access to even more advanced services as a result of the ongoing advancements in banking goods and procedures. In spite of the fact that the application of information technology in banking has the ability to bring about significant organizational and economic growth, there is also opportunity for the emergence of new kinds of risks. When it comes to the rapid expansion potential of online banking, there are both positive and negative aspects to consider.

Raman, Usha. (2008) The purpose of this essay is to provide a complete analysis of the current condition of operational risk management within the Indian banking industry in light of Basel II. When it comes to the projected coverage of banking assets and the method that is utilized for the calculation of operational risk capital, there is a broad comparison that can be made with the banking systems that are found in Asia, Africa, and the Middle East. When asked about their experiences with operational risk management, 22 Indian banks indicated that they were concerned about a lack of internal data, difficulty acquiring external loss data, and sophisticated modeling. These concerns were highlighted in response to a poll. It is clear from the

results of the survey that financial institutions must devote more time and resources to the implementation of Basel's advanced approach.

Rao, D. & Ghosh, Prodipta. (2008) Basel II's capital charge for operational risk has not only increased awareness as a result of recent catastrophic corporate failures, but it has also sparked a conversation regarding how to define and manage operational risk. The following is a discussion of the many methodologies that are currently being utilized for the purpose of operational risk measurement and modeling, followed by an analysis of the compelling arguments that are in favor of risk management that is both objective and efficient. The authors draw the conclusion that the banking industry in India is still in its early stages and faces obstacles in establishing a robust operational risk management system due to a lack of expertise in risk transfer and quantification. This conclusion is based on the findings of a survey that assessed the readiness of Indian banks to handle this type of risk.

Malhotra, Pooja (2010) this exploratory investigation was conducted with the intention of determining the current condition of online banking in India as well as the range of services that are offered by online banks. Another topic that will be investigated as part of this study is the breadth of services offered by online banking programs. In order to collect the data that was used in this study, researchers conducted a survey of bank websites in July of 2008. With regard to the sample, there are eighty-two banks that were operational in India as of the 31st of March in 2007. We make use of a multiple regression analysis in order to study the factors that determine the scope of online banking. According to the data, private and foreign online banks have surpassed their counterparts in the public sector in terms of providing a portfolio of online banking services that is more comprehensive and complex. The breadth of Internet banking services is determined by a number of critical aspects, including the size of the bank, its level of experience, the pattern of financing it uses, and the ownership of the bank. Constraints placed on the research and the results of the study The research has a number of limitations, including a limited sample size and an inability to generalize its findings to other factors (such as market, environmental, regulatory, and so on) that can influence the decisions that banks make about the provision of various online banking services. It is the purpose of this study to fill in significant information gaps regarding the current state of

internet banking in India. The results are expected to be of tremendous benefit to a variety of stakeholders, including the government, regulators, commercial banks, other financial institutions (such as cooperative banks that intend to provide internet banking), customers, and academics. The general public and the banking industry will be able to learn which financial institutions are not meeting the expectations of the general public in terms of providing a variety of goods and services, such as Internet banking. It would be beneficial for economists who are conducting research on growth drivers as well as those who are creating and manufacturing Internet banking services to become aware with the factors that influence the reach of these services. In addition, this paper contributes to the existing corpus of empirical research on the proliferation of financial innovations, including online banking, in a developing nation such as India.

Wu, Dexiang (2010) One of the numerous organizations that has shown interest in internet banking is the banking industry, which includes regulators, participants in the financial services industry, and consumers. In order to determine how well major banks in the United States and the United Kingdom manage the online banking services of their consumers, the purpose of this study is to investigate the situation. Moreover, we do risk assessments. The methods of principal component analysis (PCA) and data envelopment analysis (DEA) are used in this article in order to provide an assessment of the performance of online banking. The annual reports of significant banks in the United States and the United Kingdom from 2007 are combed through to extract information that pertains to both monetary and non-monetary elements. According to the results of the DEA, the vast majority of large banks are successfully operating. The individuals who are employed by financial institutions are ultimately the single most essential factor in determining their bottom lines. Many DEA models can be classified as either cost-oriented or online-oriented, which is in line with the findings of prior research that utilized data from other nations. Through the course of this research, we demonstrate how to evaluate the online banking services offered by significant banks by utilizing principal component analysis and decision analysis.

Habib, Sitwat et al., (2014) Taking a look at the corporate and banking sectors of Pakistan's operational risk management as it stands right now, the objective of this

article is to determine the reasons why certain businesses have implemented it while others have not. Enterprise risk management, also known as ERM, is a collection of rules and procedures that are aimed to reduce the occurrence of possible dangers to the assets and operations of a firm. The research approaches that are utilized are qualitative. The article indicates that businesses do not have the infrastructure that is required to undertake efficient risk management, which in turn inhibits the performance of the organization. The findings of this study bring to light the fact that, despite the fact that the banking sector in Pakistan possesses a certain level of comprehension regarding operational risk management, the corporate sector in Pakistan possesses a limited awareness of risk management. Furthermore, sample firms are hesitant to react due to the fear that their participation may demonstrate inefficiency. Performance of the organization, management of operational risks, management of enterprise risks, integrated approach, corporate and banking.

Petare, Purushottam (2014) The purpose of this article is to analyze the methodology that V. G. Imayev and other writers have utilized in order to evaluate operational risk by estimating the susceptibility of banks. In order to accomplish this, the article highlights the shortcomings of the techniques and approaches that are now in use. The authors called for modifications to be made to the approach that was developed by V. G. Imayev. These modifications would include alterations to the structure and distribution of indicator scales, as well as modifications to the computation of indicators that are utilized in assessments of bank operational risk susceptibility. The usage of Bayesian networks was incorporated into the proposal, which also included the development of a system for the management of operational risks.

Daryakin, A.A. et al., (2015) the purpose of this article is to analyze the methodology that V. G. Imayev and other writers have utilized in order to evaluate operational risk by estimating the susceptibility of banks. In order to accomplish this, the article highlights the shortcomings of the techniques and approaches that are now in use. The authors called for modifications to be made to the approach that was developed by V. G. Imayev. These modifications would include alterations to the structure and distribution of indicator scales, as well as modifications to the computation of indicators that are utilized in assessments of bank operational risk susceptibility. The

usage of Bayesian networks was incorporated into the proposal, which also included the development of a system for the management of operational risks.

Kujur, Teju et al., (2015) The introduction of electronic banking into the banking industry was done with the intention of enhancing customer satisfaction and, consequently, the profitability of the bank. The use of electronic banking is causing disruptions in the financial industry. It provides users with a multitude of benefits, including the ease of use, cost, and convenience of the transactions they conduct. With the assistance of electronic banking, financial institutions have the potential to become more efficient and competitive. This implies that both existing customers and potential customers will have an easier time completing transactions. On the other hand, it contributes to the problems that banking institutions and authorities have when it comes to the supervision of the financial system, as well as the formulation and implementation of macroeconomic policies. Customers in this day and age anticipate an online banking experience; yet, the adoption of e-banking by commercial banks raises issues over security and presents additional risks. Because of the fact that both legitimate and illicit banking operations have taken notice of the growing popularity of online banking, customers are susceptible to fraud, theft, and other similar threats. This is because online banking has become increasingly widespread. The purpose of this research is to investigate the ways in which e-banking has impacted banking performance and to identify the primary risks and security challenges that are associated with e-banking. This will allow bankers to better answer the concerns of their customers regarding the safety and security of their respective online banking services. Because of this, financial institutions will be able to provide clients a more secure online banking experience, which will enable them to retain their existing customers and successfully attract new ones.

Tandon, Deepak et al., (2015) there is no nation that is more important than its financial system when it comes to the institutional and functional methods of bringing about economic transformation. The financial sector serves as both the center and the barometer of a financial system. This sector is essential to the expansion of the nation's economy and acts as the framework upon which it is built. There are a variety of risks that represent significant dangers to the viability and performance of any bank that is now functioning in the current uncertain financial climate. These risks include

credit, market, operational, liquidity, interest rate, foreign currency, and others. To restate, finance is intrinsically fraught with danger. Risk management that is both efficient and effective is therefore of the utmost importance. The purpose of this study is to evaluate the degree to which Indian banks are able to effectively manage different types of risk by assessing the strategies and methodology that they employ for risk management. A secondary objective is to discuss the differences and similarities between the risk management strategies utilized by public, private, and multinational banks. As a consequence of this, financial institutions ought to be more cautious in their approach to risk-taking, make preparations for any unfavorable results by hedging their bets, and employ this method to their benefit in order to improve their industry management and competitiveness.

Sharifi, Sirus et al., (2016) The primary purpose of this essay is to investigate the relationship that exists between operational risk management (ORM), the size of banks, and ownership relationships in India. The industrialized world is currently recovering from a financial crisis that was brought on by an inadequate amount of regulation, thus this is really important. Strategy, methodology, and organizational structure: The surplus capital of Indian banks, which is greater than the minimum capital required for operational risk, is a good indicator of the ORM procedures that these institutions employ. The size of a bank is equal to total deposits plus advances. Over the course of the years 2010 to 2013, our sample consisted of 61 Indian banks. The authors conduct an empirical investigation into the relationship between bank size and excess capital by employing a panel data regression model. It has been determined through research that the surplus capital that Indian banks keep for the purpose of controlling operational risk is inversely proportionate to the size of the banks. In accordance with the inverse link, Basel regulations require smaller banks to keep a greater proportion of their spare capital than they require those that are larger. There is no association between the types of ownership (public, private, or foreign) and the amount of extra capital that banks have. This is because the goal of limiting operational risk is to ensure that the bank is being managed effectively. This research is crucial to Indian banks because of the significant amount of bad loan losses that have occurred and the implementation of Basel III criteria by the Reserve Bank of India, which is the central bank of the country. Taking into account the fact that around 33 percent of the savings of Indian households are included within deposits

kept with commercial banks and other types of financial institutions, this research does have social repercussions for the financial system of the country. There are significant concerns over the robustness of the Indian financial system; hence, the collapse of any bank might potentially have a disastrous impact on the economy of the country under consideration.

Shirley et al. on behalf of Ou Yang (2017) The goal of action research (AR) is to address problems that are actually occurring in the world while simultaneously improving scientific understanding. This has the ability to bridge the gap between rigorous research and its application in the industry. Taking this line of reasoning into consideration, the research project that we are working on advocates for returning to the fundamentals of augmented reality, which are problem-solving, taking action, and reflecting. While attempting to find a solution to the issue of operational risk management that a Taiwanese bank is experiencing, we employ a dialogical AR technique. Within the context of an augmented reality project, researchers and bank personnel are responsible for overseeing the generation of new information as a component of an attempt to manage operational risk. Across three AR cycles, our research demonstrates that practitioners are able to better detect a variety of operational hazards, and that there is a favorable association between ongoing knowledge production and the change of the current corporate culture. We also bring to your attention the scenarios in which managers could be encouraged to be responsive to new and different ways of thinking and behaving by the insights that are gained from reflective exchanges between academics and practitioners. Lastly, we offer some tips for successfully using dialogical augmented reality.

Chaturvedi, Ankita (2019) over the past few years, the financial services sector in India has experienced a significant expansion. E-commerce has developed into an indispensable business model as a consequence of this laudable expansion. The ability to conduct business online is no longer a luxury for banks; rather, it is a requirement in the current economy. E-business, often known as electronic business, refers to the process of converting a conventional business model into a networked online platform. The value chain business operations that are included include electronic procurement and supply chain management, electronic order processing, customer assistance, and partner cooperation. All of these activities are included in the value

chain. This research is to examine the potential benefits of e-business adoption for the banking sector, identify the hurdles to e-business adoption, and characterize the challenges that are encountered during the process of e-business adoption. After being selected at random from a number of branches in Jaipur, one hundred employees of ICICI Bank were asked to fill out a questionnaire and have their responses compiled.

M., Aravind (2020) during their use of internet banking, customers could have their financial interests jeopardized by processing errors, fraudulent activity, or other external incidents. This endeavor's objective is to conduct an analysis of the primary risk factors that influence the activities of customers who use online banking. The standard stimulus-response approach served as the basis for our investigation, which led to the identification of four primary risk constructs and fifteen risk stimuli that have the potential to hamper the operations of online banking. We have also found a few techniques to decrease the impact of potential threats through the research that we have done on the literature and through the focus groups that we have conducted. In this work, we constructed a stimulus-response model by establishing a connection between the operational risk of online banking and the risk mitigation strategies that are available. Additionally, we were able to confirm the proposed model through experimental testing by utilizing the responses of 742 individuals. According to the findings of covariance-based structural equation modeling (CB-SEM), the strategies that were discovered have a positive impact on lowering the risk associated with internet banking (IBR).

Mogos, Gabriela (2020) Despite the fact that e-banking and online banking have made banking significantly more comfortable in terms of delivery costs, speed, and ease, they have also generated a great deal of new issues. The rise of internet banking has resulted in a shift in mentality around risk, as well as the emergence of several new types of risk. Technology is both a source and an instrument of utmost significance when it comes to the process of risk reduction. Given that, despite the fact that it is an e-banking application, attacks are still a possibility, the purpose of this study is to evaluate the current level of the security of the e-banking application and to identify potential dangers to customers. Access control is one of the various countermeasures that have been recommended for assaults. Its purpose is to prevent eavesdropping by making it necessary to limit the individuals who are able to access

vital information. One other measure that you can take to safeguard yourself against SQL injection is to ensure that you are consistently utilizing the most recent modifications and fixes. It is possible for these attacks to compromise the entire software or to individually target a user, thereby compromising the sensitive information that they possess. Additionally, this study demonstrates how to use a variety of additional security measures in order to protect one's company and oneself from the negative effects of cybercrime.

Siyabi, Amira (2020) During the same time period as the Internet has been expanding, electronic banking has also expanded, which has resulted in the emergence of a multitude of new online services such as account creation, financial advice, and more (Kolodinsky et al., 2004). A number of different areas, including strategy, credit, market, liquidity, and others, are among those in which banks manage risk. The proliferation of internet banking, on the other hand, is not immune to the dangers that it faces. It is necessary for any firm, including e-banking service providers, to exercise control over the risks that are associated with conducting business online. According to Malisuwan (2006), the three primary areas of management for these e-banking risks are as follows: management and board supervision, security measures, and managed legal and reputational risk. These manageable areas are in accordance with the fourteen "risk management principles" established by the Electronic Banking Group (EBG) of the BCBS. According to Georgescu (2006), the competitive pressure to supply new creative commodities in extremely short time intervals makes it more difficult for management to do sufficient strategic assessments, risk analyses, and security evaluations. This is a problem since it makes it more difficult to conduct enough strategic assessments. As a result of the risks that are associated with online banks and the rapid expansion that they have experienced over the course of the past two decades, effective risk management methods have become increasingly important in the international banking sector. Our research indicates that concerns regarding security are of a very high magnitude, and it is heartening to learn that financial institutions are exerting a tremendous deal of effort to mitigate these risks. The major objective is to do research on the potential risks and consequences that Oman's internet banking services may have on an individual's general public. We begin by conducting a pilot study in which we conduct semi-structured interviews with four experienced employees of a leading bank in Oman in order to get a sense of their

thoughts on the management of risks associated with online banking. Following the completion of the pilot study, the questionnaire was developed and distributed to the most important banks in Oman in order to determine the degree to which they adhere to fundamental risk management ideas.

Barkha, Jadwani et al., (2022) there have been a number of organizations and people who have been significantly impacted by COVID-19 on a global scale. According to the statistics provided by the banks, both their corporate and retail customers have been affected by this epidemic. Banks are also required to transition to a model that incorporates a distributed staff. The lessons that were learned from the COVID-19 outbreak can be analyzed in order to meet the goal of rebuilding the operational risk management skills of other financial institutions. This study utilized a survey research approach that consists of standardized questions that were filled out by senior banking specialists in order to gain an understanding of the dispersed workforce model and the effectiveness of remote work, as well as to investigate the lessons that were learnt from COVID-19. Discoveries: A rapid acceleration of the digital revolution occurred as a result of the epidemic. The lockdown that was implemented as a result of the pandemic has made it possible for employees to work remotely, which has proven to be advantageous. This is partly due to the better digital capabilities that have been made available. However, improved monitoring is required in order to prevent issues that are associated with data, and we need to take action in order to address the issues that are associated with a dispersed workforce model. These issues include the fact that it hinders on-the-job learning, that it puts data at risk, and that it has an impact on the well-being of employees. Due to the fact that the COVID-19 pandemic is absolutely unprecedented, none of the scenario analyses could have possibly predicted it. A variety of structural issues that require addressing have been brought to light as a result of this specific issue. The lessons that were learned from this epidemic should be utilized by financial institutions in order to increase their resilience going forward onward.

Bezawada, Brahmaiah. (2022) This study will concentrate on the market risk and liquidity risk management tactics that are utilized by public and private sector banks in India that are a part of the scheduled commercial banks (SCB) during the course of a period of five years commencing in 2016–17 and concluding in 2020–21. The way

in which public sector banks (PSBs) and private sector banks (PVSBS) deal with market and liquidity risk is another thing that we are interested in observing. In addition to this, the research wants to investigate the risk management processes that SCBs have implemented and the methodologies that they have utilized. During the course of our investigation into risk management strategies, we chose six prominent PSBs and PVSBS to serve as representatives of each group. According to the findings of this research, SCBs are required to deal with a number of different issues, including credit risk, market risk (which includes fluctuations in interest rates, currency, commodities, and stock prices), liquidity risk, and operational management risk. According to the findings of the study, the annual reports on risk management strategies produced by PSBs are superior to those produced by PVSBS when comparing risk identification, assessment, and analysis with one another. In terms of policies and processes relevant to market and liquidity risk assessment, appraisal, monitoring, control, and risk taking, the findings indicate that PVSBS and PSBs are not considerably different from one another. Researchers that are interested in banking risk management will find this study to be both interesting and relevant to their research. For the purpose of this descriptive study, secondary data serves as the basis.

Salim, Archana. (2022) It is possible to claim that a vibrant banking sector is the motor that keeps an economy functioning for long periods of time. This sector is experiencing a significant expansion in India at the present time. Given the substantial technological improvements that are expected to take place over the next several years, the banking industry is going to go through a profound upheaval. Digital banking is the way of the future in the financial industry. Since the COVID-19 pandemic redesigned our daily lives, including our occupations, shopping habits, and banking practices, there have been significant changes in consumer habits. These changes have been brought about by the epidemic. In spite of the fact that online banking has made it simpler than ever before to gain access to a wide range of financial services, it has also introduced new challenges for conventional businesses, which is the topic that this article aimed to address. The findings of this study provide light on current developments that have occurred in the banking trade.

Laksana, Rio Dhani et al., (2023) The objective of this study is to investigate the perspectives of individuals who make frequent use of digital banking services with regard to the operational risks that banks face when providing these digital banking services. Within the framework of this investigation, a quantitative approach was utilized. Participants in the study were customers of participating banks who utilized online banking services. This population was the focus of the research. A total of two hundred forty bank employees from the Banyumas Regency in Central Java, Indonesia, took part in the survey. It was implemented using a method that is known as purposive sampling. For the purpose of banking risk management, it utilized five different indicators. What was discovered through the research: Residents in Banyumas generally agreed that the operational risks associated with internet banking were rather low. In light of this, another operational risk that financial institutions ought to take into consideration is the possibility of service outages, unsuccessful attempts to outsource, and internal fraud. The Technology Acceptance Model (TAM) is a popular information system theory that attempts to explain the reasons behind customers' desire to accept and make use of electronic technology. When users are presented with a novel system, they take into consideration a number of different variables before determining how and when to utilize the system, according to this idea. These include the usefulness of the system and the ease with which it can be utilized, in addition to external influences that have an effect on the beliefs, attitudes, and objectives of users who are utilizing the system. For the purpose of this study, digital banking was merged with consumers' perspectives on the operational risks that banks face when employing digital banking services. This was done since these perspectives are essential to understanding the digital banking sector. Among the limitations and implications of the study is the fact that it relied on only five indicators to quantify operational risks in the banking industry. These indicators were process, human, system, external, and legal. This indication for banking risk study is still lacking a number of components, particularly those that pertain to finance and marketing. Including study variables that investigate not only online banking apps but also other digital banking products such as mobile, phone, and SMS banking is recommended in order to widen the scope of future research. This is done in order to ensure that future research is more comprehensive.

Singh, Govind & Singh, Mr. (2023) within the context of the modern world, information technology is pervasive. There are a number of benefits associated with it, but there are also a great deal of challenges that restrict the further development of industry. In spite of this, it eventually evolved into an essential component of life. The expansion of it has also been remarkable from the past to the present day. Because of advancements in information technology, life has become less difficult. The use of information technology is necessary for the advancement of development. Electronic banking is referred to by a number of different names, including e-banking, online banking, phone banking, home banking, mobile e-banking, virtual banking, and Internet banking. All of these names refer to the same idea. This is what we mean when we say "E-Banking," which refers to banking that is done both online and over the phone. Both of these types of internet banking require the usage of passwords as an essential component. One of the most convenient ways for banks to advertise their products and services to prospective customers is through the use of online banking, which has emerged as a result of technological improvements and healthy competition among established banks. The rapid growth of online banking services comes with both positive and negative aspects to their proliferation.

Ujjval & Mancharkar, (2023) the implementation of digital banking in India has been a revolutionary movement that has brought about a major transformation in the manner in which financial services are delivered. The digitalization of banking in India has been facilitated by a number of factors, including the rise of the telecom industry, the development of new technologies, and the government's determination to achieve its aim of financial inclusion. It is highly likely that the digitalization of the banking industry will continue to be a significant contributor to the expansion of the Indian financial sector moving forward. As a result of the many different types of online banking services, each and every financial transaction is considerably influenced. Electronic banking services are now indispensable to the functioning of the banking industry in India. Banks should prioritize increasing customer awareness of online banking services as they continue to grow their operations. As the number of people using smartphones increases to become in line with global standards, the banking business will undoubtedly become increasingly digital. There will be additional shifts in the banking sector of India in the near future.

Yadav, Pooja et.al., (2023) An investigation into the challenges that banks in India have encountered in incorporating the most recent advancements in digital banking is presented in the abstract of this research. In addition to that, it provides a recap of these tendencies. The research makes use of analytical methodologies and secondary data in order to shed light on the potential advantages and disadvantages that are connected to the rising concept of digital banking within the Indian banking sector. Additionally, it is proposed that people make a smooth transition to digital banking, and the study offers insights into how these challenges might be overcome. In conclusion, the research paints a picture of a future in which digital banking in India will not only be accepted but also become the means of choice for carrying out transactions. It is predicted that a wide variety of stakeholders will benefit from this research. These stakeholders include academics, professionals working in the banking and insurance industries, financial advisors, as well as students and researchers who are interested in learning more about the development of digital banking in India.

Chaudhary, Mahima. (2024) In the context of the global arena, technological advancements have been accelerating at a rate that is deeply concerning. We are glad to say that the Internet is among the greatest in those. It can be concluded that the banking industry is likewise making the most of this opportunity. The development of online banking has been found to have increased by leaps and bounds over the course of the previous few years, according to this study that is based on financial transactions conducted online. Paying particular attention to the Indian economy, the utilization of online banking is still in the process of spreading out. The use of online banking is increasing at a good and respectable rate in India nowadays, which is expanding the scope of online banking. An increase in the number of people using the Internet is the primary factor that has led to the development of online banking. Through this initiative, we are able to have a better understanding of the origins of internet banking as well as the necessity of this service in today's world. This provides us with an understanding of the internet banking system in India. Through this, we are able to have a better understanding of the opportunities and problems that are involved with internet banking in India.

Frolov, Serhiy et.al., (2024) Through the construction of VAR models, the execution of Granger causality tests, the development of impulse response functions, and the

execution of variance analysis, this study explores the interaction between decentralized financial services and the traditional banking system. Banking data from the United States of America, India, and Great Britain were chosen for the purpose of putting the model into action. These indicators include the volume of commercial and industrial loans, the interest rate, the consumer price index, the total liabilities and capital of banks, aggregate deposits, the federal funds rate (for the United States), and the repo rate (for India). Through the use of the TVL indicator, which calculates the total value of all assets that are locked in DeFi protocols, the study analyzed data from the central banks of the nations that were specified between July 2018 and January 2024 respectively. The findings of the impulse response function (IRF) for countries illustrate the many ways in which TVL and bank indicators interact with one another. This reaction from the United States illustrates a stimulative monetary policy, which includes considerable decreases in the Federal Reserve's interest rate and increased commercial lending in order to stimulate economic activity. On the other hand, the objective of India's monetary stimulus, which is characterized by falling repo rates and an increase in the liabilities and deposits of the banking sector, is to strengthen the economy's resilience. The United Kingdom, on the other hand, takes a conservative approach to monetary policy, with significant rises in bank rates and uneven responses to lending and deposit policies, with the goal of ensuring financial stability. As a result of the analysis conducted across these countries, various influences of financial factors on TVL are highlighted. It is a reflection of the complexity of the financial system that the relationship between TVL and bank indicators is always altering in the United States. The degree to which India is sensitive to monetary policy, credit conditions, and inflation is a crucial factor that factors into TVL. Financial market dynamics in the United Kingdom are significantly influenced by choices made by the central bank, notably those concerning the bank rate.

Krishnan, K.Santhosh (2024) once the global financial crisis of 2007-2008 was over, the Indian economy saw a spectacular transformation. Following the implementation of the Demonetization program in 2016 and the Goods and Services Tax in 2017, the Indian economy underwent a total transformation into a new paradigm. In the meantime, the extraordinary COVID-19 outbreak has halted all progress and posed a significant challenge to the Indian economy. The country is working hard to contain the fallout of the global economic crisis, demonetization, and the Goods and Services

Tax (GST). In these four unusual occurrences that have occurred in India, the banking sector has played a crucial role in regulating and managing the deepening of the economic slump. As a result of this condition, the banks have been given a variety of unique loans without fully examining the documentation and the ability of individuals and enterprises to repay the loans. Due to the fact that non-performing assets (NPAs) are the best indicator of the soundness of a country's banking sector, it is necessary to conduct an analysis of the non-performing assets (NPAs) of the banking sectors in India in order to better manage the current financial crisis. In the current study, the contribution of the various groups that make up the banking industry to the Gross Domestic Product (GDP) and the growth pattern of the GDP throughout the period of time from 2010 to 2022 is investigated. The study also compared the impact of the recent unprecedented COVID-19 outbreak on the non-performing assets (NPAs) of banks with the impact of two other key economic policy events in India, namely the proclamation of demonetization (2016-2017) and the implementation of the Goods and Services Tax (2017-2018). Both of these events occurred in India. The Secondary Data that were acquired from the Annual Statistics website of the Reserve Bank of India for the period of 2001-2022 are the exclusive source of information for this study. In the course of the analysis of the study, the data concerning the nonperforming assets of the banking sector were taken into consideration. These nonperforming assets were grouped into three distinct groups, which included public sector banks, private sector banks, and foreign banks. In the study, a straightforward geometric approach was utilized to calculate an estimate of the average growth rate of non-performing assets in the banking industry. According to the findings of the study, the rate of increase of nonperforming assets (NPAs) in private and foreign banks was significantly lower than that of public sector banks. During the global economic crisis, the implementation of the Goods and Services Tax (GST), and the COVID-19 outbreak in India, the public sector banks have a greater proportion in the issuance of loans compared to the other banks.

Goyal, Sahil. (2024) Electronic commerce and the technology that underpins it are both areas in which businesses make investments. Applications for e-business, such as supply chain management and customer relationship management, encourage the development of novel product and service offerings, the maintenance of close relationships with customers, and the improvement of transaction efficiency and

scope economies. However, it is difficult for businesses to convert these advantages into revenues or economic value through their operations. There are a lot of businesses that have started out online but have not been successful in making a profit. Even in the midst of a recession, firms would continue to increase their spending on e-business, according to a survey conducted by AMR Research Inc. in the year 2001. Despite this, the returns that these investments have generated have been, at best, average.

Kumar, Abhishek. (2024) Online banking is rapidly becoming the standard in the developed world, and it is currently being adopted by a significant number of financial institutions in emerging countries all over the world. One of the primary reasons for this success is the multiple advantages that it may offer, not only to the banks but also to the people who use the services of financial institutions. In the case of financial institutions, it has the potential to offer a cost-effective method of conducting business and to deepen relationships with clients by providing superior services and innovative products that can be tailored to meet the specific requirements of consumers. Customers may have more options to choose from when it comes to the channels they may use to conduct their business, and they may also have more convenience when it comes to the times and places where they can use electronic banking. Over the course of the past ten years, India has been one of the countries that has experienced the most rapid adoption of information technology. This is mostly due to the country's capacity to offer software solutions to businesses located all over the world. This potential has provided a huge impetus for the domestic banking industry in India to implement the most recent technological advancements, particularly in the fields of Internet banking and e-commerce. Customer service is becoming more efficient, courteous, and quick as a result of the significant role that technology is playing in this regard. A user of internet banking is required to carry out a variety of transactions online, including checking the balance of their account and viewing their transaction history, paying bills, transferring funds between accounts, requesting credit card advances, ordering checks, managing investments, and trading stocks. According to the perspective of a bank, the utilization of the Internet is more effective than the utilization of other distribution mediums. This is due to the fact that banks are aiming to expand their customer base. Additionally, Internet delivery

provides a service that may be tailored to meet the preferences and requirements of each individual user.

Malusare, Lalita. (2024) The developed economy is supported by a banking system that is both efficient and comprehensive. The bank is the most significant component of the economy since it is responsible for one of the most crucial functions in the economy, which is the mobilization of resources. Throughout its history, the banking system has been subjected to a variety of shifts and circumstances, and as a result, it has become increasingly strong. Currently, it is undergoing a transformation by embracing digitalization. The adoption of digital technology is essential for every region of the world. Currently, every industry and nation is participating in the process of digitization. This includes the banking sector, which is required to adapt its conventional structure and accept the new technology in order to conduct business and participate in trade. In spite of the fact that the private sector is the first to adopt the new technology, it is steadily spreading to the various financial sectors. Computerization, digitalization, and the transition to digital banking have all been used by private sector banks in order to make the banking sector more efficient and effective toward the environment. Banks that are part of the public sector have also adopted digitization and are working toward being more environmentally conscious through banking. As a result, it is essential to have a clear understanding of whether or not the modifications will be advantageous to the customers and the bankers, in addition to the economy as a whole. Paperless banking and green banking are two new concepts that are making their way into the financial system as the banking industry is now in the process of transitioning into a new era. Currently, the banking system is considering whether or not it is possible to save the environment and protect the environment. In light of this, it is essential to conduct research on the efficiency of the newly developed technology in order to provide solutions to the issues that have arisen as a result of the most recent technical improvements. The technology behind paperless banking is based on electronic banking; nevertheless, there is a distinction in the driving force behind the financial industry. The only thing that is meant by the term "electronic banking" is the execution of banking functions through the use of electronic media. However, the term "paperless banking" refers to the numerous tools that are used to reduce the amount of paperwork that is created by the financial system. Electronic media, network and storage devices, and computer mechanisms are

all components of paperless banking technology. This technology allows for the operation of banking systems. The usage of electronic media is something that links electronic banking, green banking, and paperless banking together. This is a resemblance among these three types of banking. On the other hand, the meaning of each concept is distinct. This study aims to investigate the effectiveness of paperless technology in the Indian banking industry, with a particular focus on the nationalized banks located in Western Maharashtra.

Odedra, Jayshree. (2024) This study intends to evaluate the usage patterns and preferences about electronic banking (e-banking) services among persons belonging to Generation Y and Generation Z in the fascinating city of Ahmedabad, which is located in India. The financial landscape is undergoing significant transitions as a result of technological breakthroughs. As a result, it is becoming increasingly important for financial institutions and policymakers to have a comprehensive grasp of the specific behaviors and requirements of these demographic groups. The research makes use of a comprehensive survey approach, collecting data through the administration of structured questionnaires to a broad sample that is typical of inhabitants in Ahmedabad who belong to both Generation Y and Generation Z. This poll covers a variety of topics, such as the frequency with which people use online banking, the platforms that they prefer, the factors that influence adoption, and the levels of satisfaction with the e-banking services that are already available. The purpose of this study is to investigate important concerns such as the degree to which members of Generation Y and Generation Z are involved in the use of electronic banking, whether or not there are any noticeable differences in their preferences, and the factors that influence the decision-making processes of these generations. In order to gain relevant insights from the data that was collected, statistical analysis, which will include testing of hypotheses, will be utilized during the process. It is anticipated that the outcomes of this study will make a contribution to the current body of information concerning consumer behavior in relation to digital financial services. Additionally, the findings will provide significant information that will enable financial institutions in Ahmedabad to adjust their services to the specific requirements and expectations of Generation Y and Generation Z. This will result in the creation of an e-banking environment that is more welcoming and focused on the needs of all customers. The consequences of the study go beyond the realm of

academic research and provide useful information for policymakers and industry stakeholders who are looking to improve the experiences of online banking in order to correspond with the changing preferences of young people in this dynamic metropolitan setting.

S.Jayalakshmi, (2024) Increasing the productivity and efficiency of the financial services that are offered to customers has been made possible by technological advancements. Customers can take advantage of a variety of services provided by the banks, such as online banking, trade, payments, and financial transfers. The financial institutions provide a variety of services, such as online fund transfers, payments, trading, checking balances, and other comparable services like these. The lack of awareness of new technologies and the advantages they offer is one of the most significant obstacles that stands in the way of the development of electronic banking. technology such as point-of-sale (POS) machines, automated teller machines (ATMs), virtual banking, mobile banking, and virtual banking were among the first technology that banks implemented. FinTech companies have emerged as disruptors in the financial services industry as a result of their incorporation of a wide variety of cutting-edge technologies into their product and service offerings. The length of time that consumers spend dealing with bank staff may be extended by banks, and as a result, clients are expected to maintain a friendly approach. There is little doubt that this will be of assistance in both retaining existing customers and attracting new customers. Financial services and bank growth will be immediately improved, both domestically and internationally, as a result of this improvement. Information and Communication Technologies (ICT), electronic banking, point of sale (POS), and online banking are some of the keywords that might be used.

Shakyawar, et.al. (2024) There is no exception to the rule that artificial intelligence (AI) is transforming the financial business all over the world, and India is not an exception. A variety of banking services, including as customer service, risk management, fraud detection, and personalized financial advising, are undergoing a transformation as a result of the implementation of artificial intelligence (AI) technologies. The development of powerful machine learning algorithms, natural language processing, and data analytics are the factors that are responsible for these advancements. The purpose of this study is to provide a comprehensive examination

of the ways in which artificial intelligence (AI) is improving banking services in India. The study also examines the opportunities, barriers, and current state of the sector. Through a survey of recent research articles, industry reports, and case studies, we highlight the most significant applications of artificial intelligence in Indian banking. These applications include chatbots for customer service, predictive analytics for credit scoring, and algorithmic trading for investment management. In addition, we discuss the ethical concerns, the regulatory framework, and the potential societal implications that may arise from the implementation of AI in the banking sector in India. In conclusion, we offer insights on emerging patterns and potential routes for inquiry in order to fully harness artificial intelligence in the process of enhancing banking amenities and fostering financial inclusion in India.

Tiwari, Rishabh. (2024) As of right now, India is the country that is developing at the fastest rate in the entire world. Additionally, ever since the demonetization of the country in 2016, there has been a surge in the e-banking business of India. Within the context of the contemporary, digitalized world, electronic banking has developed into an indispensable component. This research was conducted with the intention of gathering information concerning the history of electronic banking in India, conducting an analysis of the current condition of electronic banking in India by means of surveys, and making an attempt to forecast the future of the electronic banking business in India. Within the scope of this study, we looked into seven different areas that are connected to electronic banking in India. Different ways of conducting business are also available. Numerous users in total Innovations in technology that have been implemented in online banking the total amount of money that has been transferred through electronic banking Regulations enacted by the government Through the dissemination of information to the general public regarding the many services that may be obtained through online banking The first step that we took in order to acquire the required information was to conduct a survey in the city of Pune and the areas that are immediately surrounding it. Following this, we conducted an analysis of the data and made an effort to forecast what the future might hold. Throughout the course of the survey, we enquired about a wide range of topics, such as the favorite banking method of the respondents and the number of transactions that they carried out on a weekly basis. After that, we put the information that we had gathered from the survey and the RBI through an analysis, and based on the

conclusions of that study, we attempted to make a prediction about the future in two stages.

Varadai, Suvarna et.al., (2024) By providing clients with the ability to carry out their day-to-day financial activities at their own convenience, digital payments have opened the door to a new spectrum of banking. Because of the widespread availability of mobile phones and the internet, digital payment systems are expanding at a rapid rate in developing countries such as our place of residence. Transactions in the banking industry have undergone tremendous transformations, shifting from traditional banking to convenience banking, which provides customers with the chance to transition towards a cashless and less cash society. In an effort to advance the concept of "Digital India," the government of India has implemented a number of initiatives that aim to promote and encourage the use of digital payment methods. During the course of the campaign, the government has expressed its desire to create a "Digitally Empowered" economy that is "Faceless, Paperless, and Cashless." Throughout the course of the past few years, the banking industry has gone through a number of significant phases of digital transformation. The increase in competition among state banks, private financial institutions, and foreign banks was a driving force behind this transformation. The primary objective is to make banking services more affordable and efficient, as well as accessible to all of the residents of the country. The purpose of this article is to investigate recent developments in digital payment systems, including their advantages, potential, performance, as well as the issues and obstacles that they face in India.

Yadav, Parmeshwar et.al. (2024) Internet banking has gained widespread acceptability on a global scale, both as a means of delivering banking services and as a strategic instrument for the development of businesses. It is also rapidly gaining ground in India, where an increasing number of banks are entering the fray. This idea implies that there may be some customers who are more open to embracing new technologies than others, and that the acceptance of e-banking services may expand gradually over time. This hypothesis is relevant to the setting of online banking. However, despite the fact that electronic banking (also known as e-banking) has experienced substantial growth in India over the past several years, there are still a significant number of clients who have not adopted these services. The research will

provide solutions to overcome these barriers and encourage more broad adoption of electronic banking methods in India. These recommendations will be based on the results of the survey. This presents a significant problem for marketers, as it satisfies customers' concerns about the safety of their financial transactions, which may lead to an increase in the number of people using online banking. For the purpose of data collection, a survey approach will be utilized, and a quantitative research design will be chosen.

RESEARCHGAP

The foregoing review of literature focused upon how to implement the provisions of Basel Accords, how to measure the operational risk, how to estimate the impact of operational risk on banks' profitability, how to shift from one approach to other approach for measuring the operational risk, etc., but no concerted effort has been made to study the components of operational risks in e-banking, factors responsible for such risks, their impacts on the functioning of the banks and measures for overcoming the operational risk in Indian banking sector. Therefore, the present study entitled "Risk Analysis of E-Banking Operations" is undertaken to fill the gaps in the existing literature.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 INTRODUCTION

In order to better identify and manage any risks inside electronic banking systems, research methodology pertaining to risk analysis for e-banking operations employs a systematic and rigorous approach. First steps in this process include cataloguing potential dangers to online banking, such as hacking, operational errors, lack of compliance, and fraud. After hazards are identified, it uses a number of analytical methods to determine how likely and severe they are. Effective mitigation solutions are developed by evaluating their possible impact and probability using qualitative and quantitative evaluations. In order to adjust to new dangers and enhance risk management procedures, the approach stresses the need of constant monitoring and evaluation. Financial institutions may improve their capacity to secure digital transactions and keep their e-banking operations secure and reliable by using a structured research technique.

3.2 THEORETICAL FRAMEWORK

In order to thoroughly address the many different types of risks that could arise from using electronic banking systems, a multi-faceted framework has been developed to guide risk analysis in these contexts. The ideas presented here come from a variety of theoretical sources, including systems theory, behavioral risk theory, operational risk theory, information security theory, compliance and regulatory frameworks, and risk management frameworks. These components are essential for e-banking risk management and knowledge, and together they provide a strong basis for successful risk reduction methods.

Information Security Theory forms the basis of the theoretical system for analyzing risks in online banking. The goal of this idea is to prevent the loss, misuse, modification, or disclosure of information assets. Confidentiality, integrity, and availability, or the CIA Triad, are its guiding values. Data integrity ensures that data is true and unmodified, availability assures that systems and information are available when required, and confidentiality ensures that only authorized individuals can access it. When it comes to online banking, these guidelines are vital for protecting sensitive

client information and financial transactions from hackers. The Bell-LaPadula and Biba models, among others, provide a theoretical foundation for developing efficient security controls in online banking systems by delving deeper into the topic of security maintenance and the prevention of illegal data tampering.

Risk Management Frameworks provide organized approaches to risk identification, evaluation, and management. This is where frameworks like ISO 31000 and the Risk Management Framework (RMF) come in handy. Risk assessment, mitigation, and ongoing monitoring are all part of the RMF's standardized approach to risk management. It lays forth a method for doing regular risk assessments, putting controls in place, and changing tactics as needed. In addition, ISO 31000 provides broad recommendations on how to incorporate risk management into business operations. A risk management plan that helps the company reach its goals and makes better decisions is something that should be emphasized. To guarantee thorough and effective risk management in online banking, these frameworks help institutions approach possible risks in a methodical way.

Operational Risk Theory oversees potential dangers caused by both internal and external factors, including processes, people, and systems. System failures, software defects, and human mistakes are all examples of operational risks that might arise in online banking, making this theory all the more pertinent in this context. For better understanding how to handle operational risks, financial institutions might refer to the Basel II and Basel III frameworks. Banks are now obligated to have sufficient capital reserves to compensate for any losses caused by operational failures, according to Basel II's introduction of operational risk management. The third Basel Accord expands upon this by strengthening the regulatory framework, with an emphasis on better risk management and stronger financial institution resilience. By using the principles of operational risk theory, online banking systems may be better assessed for security flaws and safeguards against threats to system functionality and operational procedures can be put in place.

Fraud Risk Theory offers a structure for comprehending and guarding against fraudulent actions in online banking. Specifically pertinent is the Fraud Triangle Theory, which incorporates opportunity, pressure, and reasoning. According to this idea, fraud happens when a person is in a position to conduct fraud, feels pressured or

motivated to do so, and can justify the act as appropriate. Applying this approach to the realm of online banking allows us to spot any weak spots and put safeguards in place to avoid fraud. Surveillance systems, fraud detection algorithms, and strong authentication procedures are all potential components of an efficient fraud prevention strategy. Financial organizations may improve system security and consumer asset protection by learning what causes fraud.

Compliance and Regulatory Frameworks are crucial for guaranteeing compliance with regulations and laws regarding online banking. According to the Regulatory Compliance Theory, one way to reduce the likelihood of facing legal or financial trouble is to follow all applicable rules and regulations. Data security standards and regulations like GDPR and PCI-DSS outline best practices for safeguarding consumer information and financial transactions. Organizations are obligated to establish safeguards to protect personal information in accordance with GDPR, which places an emphasis on data protection and privacy. To avoid breaches and ensure the security of payment card data, PCI-DSS establishes guidelines. In addition to improving general security and trust, these frameworks aid online banking firms in managing compliance risks and avoiding regulatory fines.

Behavioral Risk Theory investigates the ways in which human actions, including as cognitive biases and decision-making, influence risk. In order to create secure security measures and user interfaces for online banking, it is essential to comprehend behavioral risk. Users may engage in dangerous actions or make bad decisions due to cognitive biases like confirmation bias and overconfidence. The need of security awareness initiatives and user-centric design in reducing these risks is emphasized by Behavioral Risk Theory. Improved security and less user error may be achieved by financial organizations by studying user behavior patterns and addressing their interactions with e-banking systems.

Systems Theory takes a look at how an online banking system's parts work together. As a result, we can better understand the interplay between various components and the ways in which hazards might spread. A key tenet of systems theory is the significance of recognizing any weak spots by delving into the intricate web of interactions between different parts of a system. From this vantage point, e-banking risk management solutions may be more holistic, tackling systemic weaknesses and

strengthening the system as a whole. The overall stability and security of e-banking activities may be better anticipated and mitigated by financial institutions by examining the relationships between various system components.

3.3 RESEARCH DESIGN

To get a thorough grasp of the research issue, this study uses a research design that combines exploratory and descriptive techniques. It utilizes an exploratory-cum-descriptive strategy. The goal of the exploratory phase is to learn as much as possible about the topic under research by delving into it with as few assumptions as possible. This will hopefully lead to the identification of hitherto unseen variables, patterns, or discoveries. To collect first data and form initial hypotheses, this phase makes use of qualitative approaches like focus groups or interviews. After this, the descriptive phase uses organized approaches like surveys or statistical analysis to quantitatively and descriptively explain the discovered variables. This gives a thorough empirical description of the phenomena. The study provides a solid groundwork for future research or practical application by combining these two methods, which not only allow for a more nuanced understanding but also provide a detailed and accurate portrayal of the research topic.

3.4 POPULATION OF THE STUDY

The Indian banking industry, namely the State Bank Group, Nationalized Banks, and Private industry Banks, constitute the population for this research.

3.5 SAMPLING TECHNIQUE

In this investigation, the judgment sampling method is used. As a non-probability sampling method, judgment sampling (also called expert or purposive sampling) entails the researcher picking examples or participants with specific knowledge about the subject at hand. This strategy relies on the researcher's expert judgment to zero in on entities with relevant traits or perspectives for answering the research questions. The goal of judgment sampling is to intentionally choose individuals who are most likely to provide important and relevant data, as opposed to simple random sampling method which tries to guarantee that every person of the population has an equal chance of being picked. Exploratory research that aim to get in-depth insight from competent sources or that target a highly specialized audience benefit greatly from

this technique. Be mindful of the possible limits of judgment sampling, such as the danger of researcher bias and limited generalizability of the results, but it may increase the relevance of the data and produce rich, context-specific information. However, judgment sampling, when used with care, may provide useful insights that other sampling approaches may miss.

3.6 SAMPLE OF THE STUDY

State Bank of India (SBI), Telangana Grameena Bank (TGB) and AP Grameena Vikas Bank (APGVB) are selected from the category of State Bank group; and Bank of Baroda (BOB), Punjab National Bank (PNB), Union Bank of India (UBI), and Canara Bank (CANBK) are selected from the category of nationalized banks. On the other hand, HDFC Bank (HDFC), ICICI Bank (ICICI) and Axis Bank (AXIS) are selected from the category of private sector banks.

A total of 350 officials, or 35 from each of the participating banks in Hyderabad, Telangana, are chosen at simple random sampling method.

Table 3. 1 Gender of the respondents

Particulars	Frequency	Percentage
Male	220	62.86%
Female	130	37.14%
Total	350	100.0

Source: Primary Data

Based on the data shown in Table 3.1, which shows the distribution of respondents by gender, it can be seen that there are more males (62.86%) than females (37.14%). With men making up about two-thirds of the sample, there is a noticeable gender imbalance among the responses. There were 350 total responders, therefore these percentages should be considered representative of the group as a whole.

Table 3. 2 Experience of the respondents

Particulars	Frequency	Percentage
Less than 4 years	60	17.14%
5-8 years	110	31.43%
More than 8 years	180	51.43%
Total	350	100.0

Source: Primary Data

According to Table 3.2, which summarizes the respondents' job experience, 51.43 percent of them had eight years or more of experience. Among those with 5-8 years of experience, only 31.43% are in the minority, while just 17.14% have less than 4 years. Based on the distribution, it seems that most of the respondents are seasoned professionals. More than half of them have been in their industry for a long time. With 350 total replies, we can be confident that we have a good cross-section of expertise levels.

Table 3. 3 Qualification of the respondents

Particulars	Frequency	Percentage
Graduates	125	35.71%
Postgraduates	217	62.00%
Professional qualification	8	2.29%
Total	350	100.0

Source: Primary Data

Table 3.3 provides a summary of the respondents' educational credentials, showing that 62.00% of them had postgraduate degrees. A tiny percentage, 2.29%, has professional credentials, whereas 35.71% of the sample consists of graduates. Based on this distribution, it seems that the majority of the respondents had a lot of education. The 350 participants represent a broad but mostly postgraduate-educated demographic.

3.7 SOURCES OF DATA

Both primary and secondary sources of information were used for this investigation.

3.8 DATA COLLECTION PROCEDURE

An initial structured questionnaire with five-point Likert scales—"Strongly Disagree" (SD), "Disagree" (D), "Neutral" (N), "Agree" (A), and "Strongly Agree" (SA)—was used to gather the main results. In addition to questionnaires, other methods for gathering the necessary data included interviews and group discussions. The

secondary data, on the other hand, came primarily from publications put out by the Reserve Bank of India and the Indian Banks Association. These publications included the Indian Banking Year Book, the Report on Trends and Progress of Banking in India, the IBA Bulletins, and the RBI Monthly Bulletins. Other sources included journals and newspapers such as The Economic Times, The Financial Express, The Hindu, and Business Standard.

3.9 STATISTICAL TECHNIQUES USED

The data collected for the study are analyzed using SPSS (Version 18.0). Both descriptive and inferential statistical techniques are applied to interpret the responses effectively. Descriptive statistics such as percentages, means, standard deviations, and frequency distributions are used to summarize the demographic profile of respondents and to understand general response patterns.

For the purpose of coding the Likert scale responses, numerical weights are assigned as follows: Strongly Disagree (SD) = 1, Disagree (D) = 2, Neutral (N) = 3, Agree (A) = 4, and Strongly Agree (SA) = 5. This scaling method facilitates quantitative analysis and comparison of responses.

In addition to descriptive statistics, inferential statistical tools such as the Chi-square test, One-Way ANOVA, and Coefficient of Correlation are employed. The Chi-square test is used to examine the association between categorical variables and to determine whether significant relationships exist between demographic factors and operational risk perceptions. One-Way ANOVA is applied to identify significant differences in mean scores among different groups of respondents. The Coefficient of Correlation (Pearson's correlation) is used to measure the strength and direction of relationships between variables related to operational risk factors. These techniques help in testing hypotheses and drawing meaningful conclusions at the 5% level of significance.

3.10 RELIABILITY OF SCALE

The reliability of the data collection instrument is assessed using Cronbach's Alpha Coefficient. This statistical measure evaluates the internal consistency of the scale items. The computed Cronbach's alpha values for the subscales are as follows:

- Risk of customer transaction repudiation – 0.766

- Risk of insufficient customer security practices – 0.880
- Risk of hacking – 0.885
- Identification, monitoring, and control of operational risk – 0.884
- Overall scale reliability – 0.953

All the Cronbach's alpha values exceed the acceptable threshold of 0.60 at the 5% level of significance, indicating a high degree of internal consistency and reliability. Therefore, the scale used for measuring operational risk factors is considered reliable and suitable for further statistical analysis.

CHAPTER 4

DATA ANALYSIS AND INTERPRETATION

4.1 RESULTS OF HUMAN RESOURCE ORIENTED OPERATIONAL RISKS

This research delves into the causes of HR-oriented operational risks in e-banking, how these risks affected the banks' operations, and what the banks did to improve their security. It does this on a bank-by-bank and group-by-group basis.

4.1.1 RISK OF REPUDIATION OF CUSTOMERS' TRANSACTIONS

When clients ask for services and those services aren't provided on time, whether it's because of staff, technology, or some other issue, it's considered a repudiation. This section discusses the variables that contribute to the risk of client transaction repudiation, how it affects the banks' operations, and the steps taken to mitigate this risk in the chosen institutions, broken down by bank and by group.

1. Factors Responsible for Risk

State Bank Group

In Table 4.1, we can see that most people think that the following variables contribute to the possibility of customers' transactions at certain State Bank Group institutions being repudiated.

Table 4. 1 Factors Responsible for Risk of Repudiation of Customers' Transactions in Selected Banks of State Bank Group

Factors	SBI					TGB					APGVB				
	SD	D	N	A	SA	SD	D	N	A	SA	SD	D	N	A	SA
Absence of system for customers' authentication	10.0	7.5	2.5	25.0	55.0	2.5	22.5	2.5	45.0	27.5	5.0	5.0	7.5	30.0	52.5
Use of outdated hardware and	15.0	12.5	7.5	42.5	22.5	7.5	22.5	0	55.0	15.0	10.0	10.0	5.0	50.0	25.0

software system															
Cyber threats and vulnerabilities	15.0	20.0	0	32.5	32.5	7.5	22.5	0	52.5	17.5	7.5	7.5	2.5	40.0	42.5
Non-availability of sufficient balance in customer's account	0	17.5	2.5	47.5	32.5	10.0	22.5	0	55.0	12.5	5.0	20.0	12.5	30.0	32.5
Failure of the system to provide online services	15.0	30.0	0	22.5	32.5	10.0	17.5	0	50.0	22.5	15.0	12.5	0	40.0	32.5

Nationalized Banks

Most respondents agree or strongly agree that the following variables contribute to the possibility of customer transaction repudiation at the nationalized banks that were chosen for this study (Tables 4.2).

Table 4. 2 Factors Responsible for Risk of Repudiation of Customers' Transactions in Selected Nationalized Banks

Factors	UBI					BOB					PNB					CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Absence of system for customers' authentication	25	50	25	35	50	50	25	25	45	45	50	15	05	47	35	25	10	05	50	37

n																				
Use of outdat ed hardw are and softwa re system	7 .5	1 .5	0 .0	5 .5	2 .5	7 .5	5 .0	7 .5	7 .0	1 .0	2 .5	2 .0	7 .5	5 .0	1 .5	2 .5	1 .0	0 .0	5 .7	3 .0
Cyber threats and vulner abilitie s	7 .5	7 .5	5 .0	6 .5	1 .5	7 .5	1 .5	1 .0	3 .2	3 .7	5 .0	2 .0	1 .2	3 .7	2 .5	7 .5	1 .0	0 .0	5 .2	3 .0
Non- availa bility of suffici ent balanc e in custo mer's accou nt	1 .2	1 .2	5 .0	4 .5	2 .5	7 .5	7 .5	1 .0	5 .5	2 .0	0 .0	2 .5	1 .0	5 .0	1 .5	0 .0	1 .0	0 .0	7 .0	2 .0
Failur e of the system to	1 .5	1 .2	2 .5	4 .5	2 .5	2 .5	1 .0	5 .0	5 .5	2 .7	0 .5	2 .7	1 .5	4 .0	1 .7	1 .5	1 .0	0 .0	5 .0	2 .5

provide online services																			
-------------------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Private Sector Banks

In relation to the variables that pose a risk of client transaction repudiation at the chosen private sector banks, the majority of respondents (as indicated in Tables 4.3) agree or strongly agree.

Table 4. 3 Factors Responsible for Risk of Repudiation of Customers’ Transactions in Selected Private Sector Banks

Factors	AXIS					HDFC					ICICI				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Absence of system for customer s’ authentication	0	2.5	2.5	35.0	60.0	2.5	10.0	10.0	32.5	45.0	5.0	10.0	2.5	50.0	32.5
Use of outdated hardware and software system	7.5	2.5	7.5	45.0	37.5	2.5	10.0	7.5	55.0	25.0	2.5	7.5	2.5	62.5	25.0
Cyber threats and vulnerabilities	10.0	12.5	0	52.5	25.0	5.0	10.0	12.5	55.0	17.5	2.5	7.5	0	62.5	27.5
Non-availability of sufficient balance in customer’s account	15.0	17.5	5.0	35.0	27.5	5.0	12.5	22.5	40.0	20.0	0	15.0	7.5	50.0	27.5
Failure of the	7.5	15.0	0	45.0	32.5	7.5	7.5	12.5	45.0	27.5	2.5	17.5	7.5	50.0	22.5

system to provide online services															
-----------------------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Group-wise Comparison

In Table 4.4, we can see that most respondents in the chosen groups of banks agree or strongly agree on the characteristics that put consumers' transactions at risk of repudiation.

Table 4. 4 Factors Responsible for Risk of Repudiation of Customers Transactions in Selected Groups of Banks

Factors	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Absence of system for customer s' authentication	5. 8	11 .7	4. 2	33 .3	45 .0	4. 0	8. 5	2. 0	42 .0	43 .5	2. 5	7. 5	5. 0	39 .2	45 .8
Use of outdated hardware and software system	10 .8	15 .0	4. 2	49 .2	20 .8	5. 0	12 .5	5. 0	57 .0	20 .5	4. 2	6. 7	5. 8	54 .2	29 .2
Cyber threats and vulnerabilities	10 .0	16 .7	0. 8	41 .7	30 .8	6. 0	11 .5	6. 5	51 .0	25 .0	5. 8	10 .0	4. 2	56 .7	23 .3
Non-availability of sufficient balance in customer's account	5. 0	20 .0	5. 0	44 .2	25 .8	5. 5	14 .5	6. 0	53 .5	20 .5	6. 7	15 .0	11 .7	41 .7	25 .0
Failure of the system to provide online	13 .3	20 .0	0	37 .5	29 .2	8. 0	16 .0	5. 5	47 .0	23 .5	5. 8	13 .3	6. 7	46 .7	27 .5

services															
----------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

2. Impacts of Risk

State Bank Group

The majority of respondents agree or strongly agree that the risk of client transaction repudiation undermines the operation of the chosen banks of the State Bank Group, as indicated in Table 4.5.

**Table 4. 5 Impacts of Risk of Repudiation of Customers' Transactions in
Selected Banks of State Bank Group**

Impacts	SBI					TGB					APGVB				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Costs incurred in proving that no transaction took place	12.5	17.5	5.0	32.5	32.5	0	7.5	0	60.0	32.5	0	5.0	2.5	65.0	27.5
Loss of present and potential customers	10.0	20.0	2.5	35.0	32.5	2.5	7.5	2.5	67.5	20.0	2.5	12.5	5.0	55.0	25.0
Increase in costs associated with regeneration of customers' transactions	5.0	22.5	2.5	37.5	32.5	2.5	10.0	0	60.0	27.5	0	7.5	2.5	55.0	35.0
Potential adverse publicity in media	5.0	20.0	2.5	40.0	32.5	2.5	20.0	0	52.5	25.0	5.0	10.0	2.5	42.5	40.0
Significant deterioration in	0	15.0	5.0	50.0	30.0	2.5	22.5	0	52.5	22.5	22.5	5.0	5.0	27.5	40.0

the quality of the services																
--------------------------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Nationalized Banks

The effects of the potential rejection of client funds on the operations of the chosen nationalised banks are acknowledged by most respondents (Tables 4.6).

**Table 4. 6 Impacts of Risk of Repudiation of Customers' Transactions in
Selected Nationalized Banks**

Impacts	UBI					BOB					PNB					CANBK				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Costs incurred in providing that no transaction took place	0	1 2 . 5	0	7 2 . 5	1 5. 0	0	7 . 5	0	6 0 . 0	3 2. 5	2 . 5	7 . 5	2 . 5	5 7 . 5	3 0 . 0	5. 0	7 . 5	0	6 0 . 0	2 7 . 5
Loss of present and potential customers	7 . 5	7 . 5	5 . 0	5 7 . 5	2 2. 5	5. 0	7 . 5	5 . 0	4 7 . 5	3 5. 0	5 . 0	1 0 . 0	1 2 . 5	4 2 . 5	3 0 . 0	5. 0	1 7 . 5	0	5 7 . 5	2 0 . 0
Increase in costs associated with regeneration of customers' transactions	5 . 0	2 . 5	2 . 5	6 2 . 5	2 7. 5	0	1 0 . 0	5 . 0	5 2 . 5	3 2. 5	5 . 0	1 7 . 5	2 . 5	4 5 . 0	3 0 . 0	5. 0	5 . 0	2 . 5	5 2 . 5	3 5 . 0
Potential advers	2 . 5	7 . 5	2 . 5	5 7 . 0	3 0. 0	0	2 5 . 5	7 . 5	3 7 . 0	3 0. 0	7 . 5	1 2 . 0	5 . 0	4 2 . 0	3 2 . 0	7. 5	2 . 5	0	6 5 . 0	2 5 . 0

e publici ty in media				5			0		5			5		5	5				0	0
Signifi cant deterio ration in the quality of the service s	1 2 . 5	1 7 . 5	1 0 . 0	4 0 . 0	2 0. 0	2. 5	1 5 . 0	1 0 . 0	5 0 . 0	2 2. 5	5 . 0	2 2 . 5	5 2 . 5	1 7 . 5	5. 0	1 2 . 5	2 . 5	6 2 . 5	1 7 . 5	

Private Sector Banks

The majority of respondents agree or strongly agree that the risk of client transaction repudiation undermines the operation of the chosen private sector banks, as indicated in Tables 4.7.

Table 4. 7 Impacts of Risk of Repudiation of Customers Transactions in Selected Private Sector Banks

Impact s	AXIS					HDFC					ICICI				
	SD	D	N	A	SA	S D	D	N	A	SA	S D	D	N	A	SA
Costs incurre d in proving that no transact ion took place	5.0	7. 5	0	60 .0	27. 5	0	0	15 .0	40 .0	45. 0	2. 5	10 .0	5. 0	47 .5	35. 0
Loss of present and potentia l custom ers	5.0	22 .5	0	30 .0	42. 5	5. 0	10 .0	15 .0	60 .0	10. 0	0	12 .5	5. 0	42 .5	40. 0
Increas e in costs associat ed with regener	5.0	7. 5	0	52 .5	35. 0	0	0	20 .0	42 .5	37. 5	0	7. 5	5. 0	62 .5	25. 0

ation of customers' transactions															
Potential adverse publicity in media	5.0	17.5	0	50.0	27.5	0	2.5	20.0	45.0	32.5	2.5	10.0	7.5	65.0	15.0
Significant deterioration in the quality of the services	5.0	15.0	0	60.0	20.0	10.0	5.0	10.0	32.5	42.5	0	5.0	5.0	57.5	32.5

Group-wise Comparison

Table 4.8 shows that most respondents in the chosen categories of banks agree or strongly agree that the risk of repudiation of consumers' transactions has an effect.

Table 4. 8 Impacts of Risk of Repudiation of Customers' Transactions in Selected Groups of Banks

Impacts	State Bank Group					Nationalized Banks					Private Sector Banks				
	SD	D	N	A	SA	SD	D	N	A	SA	SD	D	N	A	SA
Costs incurred in proving that no transaction took place	4.2	10.0	2.5	52.5	30.8	2.0	9.5	2.0	60.5	26.0	2.5	5.8	6.7	49.2	35.8
Loss of present and potential customers	5.0	13.3	3.3	52.5	25.8	6.0	11.0	5.5	53.0	24.5	3.3	15.0	6.7	44.2	30.8
Increase in costs associated with	2.5	13.3	1.7	50.8	31.7	3.0	9.5	3.5	53.0	31.0	1.7	5.0	8.3	52.5	32.5

regeneration of customers' transactions															
Potential adverse publicity in media	4.2	16.7	1.7	45.0	32.5	3.5	11.0	4.0	56.5	25.0	2.5	10.0	9.2	53.3	25.0
Significant deterioration in the quality of the services	8.3	14.2	3.3	43.3	30.8	5.5	17.0	6.0	49.5	22.0	5.0	8.3	5.0	50.0	31.7

3. Risk Management Measures

State Bank Group

Table 4.9 shows that most people are in agreement or strongly agree on the security measures put in place to prevent customers' transactions at the group's chosen banks from being repudiated.

Table 4. 9 Measures for Overcoming the Risk of Repudiation of Customers Transactions in Selected Banks of State Bank Group

Measure s	SBI					TGB					APGVB				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Implementing security measure for enhancing customers' authentication	5.0	7.5	2.5	27.5	57.5	0	0	0	52.5	47.5	0	2.5	2.5	35.0	60.0
Introducing audit	12.5	5.0	0	50.0	32.5	0	5.0	0	77.5	17.5	5.0	7.5	5.0	52.5	30.0

trials for transactions															
Introducing more options for informing the customers about the transactions	10.0	2.5	0	40.0	47.5	0	7.5	2.5	67.5	22.5	12.5	12.5	7.5	35.0	32.5
Use of active and updated response procedures and plans	2.5	5.0	0	47.5	45.0	5.0	5.0	2.5	60.0	27.5	5.0	12.5	0	47.5	35.0
Use of most current version of content management system or other publicly accessible software's	2.5	5.0	0	40.0	52.5	5.0	12.5	5.0	47.5	30.0	5.0	5.0	5.0	45.0	40.0
Use of most current version of anti-virus and anti-malware systems	7.5	12.5	0	30.0	50.0	5.0	7.5	2.5	57.5	27.5	7.5	7.5	5.0	40.0	40.0
Consider cyber threats and	0	12.5	0	40.0	47.5	5.0	10.0	2.5	47.5	35.0	20.0	12.5	2.5	30.0	35.0

vulnerabilities as a part of operational risk																	
---	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Source: Survey

Nationalized Banks

The steps to mitigate the possibility of client transaction repudiation at the chosen nationalized banks have garnered widespread support, as shown in Table 4.10.

Table 4. 10 Measures for Overcoming the Risk of Repudiation of Customers’ Transactions in Selected Nationalized Banks

Measures	UBI					BOB					PNB					CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Implementing security measures for enhancing customers’ authentication	0	5.0	0	37.5	57.5	2.5	0	2.5	40.0	55.0	2.5	7.5	2.5	45.0	42.5	0	5.0	2.5	40.0	52.5
Introducing audit trials for transactions	2.5	7.5	5.0	52.5	32.5	2.5	5.0	7.5	60.0	25.0	7.5	2.5	5.0	47.5	37.5	1.0	5.0	0	57.5	27.5
Introducing more options for informing	7.5	12.5	0	42.5	37.5	0	7.5	2.5	57.5	32.5	0	2.5	5.0	42.5	30.0	0	10.0	0	52.5	37.5

the custo mers about the transa ctions																				
Use of active and updat ed respo nse proce dures and plans	2. 5	2 2. 5	2 .5 5	3 7. 5	3 5. 0	2. 5	1 2. 5	1 0. 0	5 7. 5	1 7. 5	2 .5 5	1 2. 5	5 .0 5	5 2. 5	2 7. 5	2. 5	1 2. 5	2 .5 5	4 5. 0	3 7. 5
Use of most curre nt versio n of conte nt mana geme nt syste m or publi cly acces sible softw are's	1 0. 0	1 0. 0	5 .0 0	5 2. 5	2 2. 5	0	2 2. 5	5. 0	5 2. 5	2 0. 0	7 .5 5	1 5. 0	5 .0 0	3 7. 5	3 5. 0	7. 5	7. 5	0	5 5. 0	3 0. 0
Use of most curre nt versio n of anti- virus and anti-	5. 0	1 0. 0	5 .0 0	5 0. 0	3 0. 0	5. 0	1 0. 0	5. 0	6 0. 0	2 0. 0	5 .0 0	1 5. 0	2 .5 5	4 0. 0	3 7. 5	2. 5	1 0. 0	0	5 2. 5	3 5. 0

malware system																				
Consider cyber threats and vulnerabilities as a part of operational risk	12.5	7.5	7.5	35.0	37.5	10.0	5.0	5.0	32.5	47.5	0	15.0	0	40.0	45.0	10.0	2.5	2.5	50.0	35.0

Private Sector Banks

In Table 4.11, we can see that most people are in agreement or highly in agreement with the steps taken by the chosen private sector banks to reduce the possibility of client transaction repudiation.

Table 4. 11 Measures for Overcoming the Risk of Repudiation of Customers' Transactions in Selected Private Sector Banks

Measures	AXIS					HDFC					ICICI				
	SD	D	N	A	SA	SD	D	N	A	SA	SD	D	N	A	SA
Implementing security measures for enhancing customers' authentication	2.5	10.0	0	30.0	57.5	2.5	5.0	5.0	35.0	52.5	0	0	5.0	47.5	47.5
Introducing audit trials for transactions	10.0	7.5	2.5	65.0	15.0	0	2.5	7.5	70.0	20.0	2.5	2.5	2.5	57.5	35.0
Introduce more	7.5	12.5	2.5	55.0	22.5	5.0	15.0	15.0	35.0	30.0	0	5.0	5.0	47.5	42.5

options for informing the customers about the transactions															
Use of active and updated response procedures and plans	10.0	12.5	0	50.0	27.5	5.0	7.5	15.0	45.0	27.5	2.5	2.5	5.0	50.0	40.0
Use of most current version of content management system or other publicly accessible software's	12.5	7.5	0	45.0	35.0	7.5	5.0	12.5	32.5	42.5	0	5.0	7.5	50.0	37.5
Use of most current version of anti-virus and anti-malware system	7.5	5.0	0	57.5	30.0	2.5	2.5	15.0	30.0	50.0	2.5	10.0	0	50.0	37.5
Consider cyber threats and vulnerabilities as part of operational risk	2.5	12.5	0	52.5	32.5	2.5	2.5	15.0	42.5	37.5	5.0	5.0	0	50.0	40.0

Group-wise Comparison

Table 4.12 shows that across all groupings of banks, the majority of respondents agree or strongly agree on the methods to overcome the risk of client transaction repudiation.

Table 4. 12 Measures for Overcoming the Risk of Repudiation of Customers’ Transactions in Selected Groups of Banks

Measures	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Implementing security measures for enhancing customers authentication	1.7	3.3	1.7	38.3	55.0	2.5	3.5	1.5	42.0	50.5	1.7	5.0	3.3	37.5	52.5
Introducing audit trials for transactions	5.8	5.8	1.7	60.0	26.7	5.0	4.0	4.0	55.0	32.0	4.2	4.2	4.2	64.2	23.3
Introduce more options for informing the customers about the transactions	7.5	7.5	3.3	47.5	34.2	2.5	12.0	3.0	50.5	32.0	4.2	10.8	7.5	45.8	31.7
Use of active and updated response procedures and plans	4.2	7.5	.8	51.7	35.8	4.0	15.0	4.5	47.0	29.5	5.8	7.5	6.7	48.3	31.7
Use of most current version of	4.2	7.5	3.3	44.2	40.8	6.5	13.0	3.0	48.5	29.0	6.7	5.8	6.7	42.5	38.3

content management system or other publicly accessible software's															
Use of most current version of anti-virus and anti-malware system	6.7	9.2	2.5	42.5	39.2	4.5	10.5	2.5	49.5	33.0	4.2	5.8	5.0	45.8	39.2
Consider cyber threats and vulnerabilities as a part of operational risk	8.3	11.7	1.7	39.2	39.2	7.0	8.0	3.5	40.5	41.0	3.3	6.7	5.0	48.3	36.7

4.1.2 RISK OF OUTDATED STAFF AND LACK OF MANAGEMENT EXPERTISE

Inadequate knowledge of the latest technology and its effects among staff members, as well as a lack of competence among senior-level employees, poses the risk that customers will not receive timely, high-quality service, which in turn could hurt the company's bottom line. In this part, we will examine the causes of the risk of inexperienced management and out-of-date employees, how it affects the operations of the banks in question, and the steps taken to mitigate this risk in each of the chosen institutions.

1. Factors Responsible for Risk

State Bank Group

Based on the data in Table 4.13, it is clear that most people think that the chosen banks in the group are at danger due to inexperienced managers and outmoded employees.

Table 4. 13 Factors Responsible for Risk of Outdated Staff and Lack of Management Expertise in Selected Banks of State Bank Group

Factors	SBI					TGB					APGVB				
	SD	D	N	A	S A	SD	D	N	A	SA	S D	D	N	A	S A
Outdated recruitment, selection, placement and promotion policies	2.5	15.0	2.5	42.5	37.5	2.5	20.0	5.0	45.0	27.5	0	0	2.5	55.0	42.5
Lack of proper and timely training and development facilities	2.5	15.0	5.0	35.0	42.5	0	5.0	2.5	65.0	27.5	5.0	2.5	7.5	57.5	27.5
Absence of challenging opportunities to the staff for growth	5.0	10.0	7.5	52.5	25.0	2.5	15.0	5.0	57.5	20.0	5.0	22.5	2.5	42.5	27.5
Lack of abilities to fully understand the new technology	7.5	17.5	2.5	32.5	40.0	0	20.0	5.0	55.0	20.0	2.5	15.0	7.5	55.0	20.0
Lack of abilities to fully understand the	7.5	15.0	0	50.0	27.5	2.5	17.5	2.5	50.0	27.5	10.0	5.0	5.0	47.5	32.5

need of technological up gradation																			
------------------------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Nationalized Banks

Table 4.14 shows that most people think that the chosen nationalized banks' danger of having out-of-date employees and incompetent management is due to the reasons mentioned.

Table 4. 14 Factors Responsible for Risk of Outdated Staff and Lack of Management Expertise in Selected Nationalized Banks

Factors	UBI					BOB					PNB					CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Outdated recruitment, selection placement and promotion policies	7.5	2.5	2.5	3.25	5.5	5.0	2.5	0	3.5	5.75	5.0	1.75	2.5	4.5	3.0	2.5	1.0	0	3.25	5.5
Lack of proper and timely training and devel	0	1.0	5.0	4.5	4.0	2.5	5.0	7.5	7.25	1.25	2.5	7.5	7.5	6.25	2.0	5.0	2.5	2.5	5.25	3.75

opme nt facilit ies																				
Abse nce of challe nging opportu nities to the staff for growt h	5. 0	1 5 . 0	0	5 5 . 0	2 5 . 0	2. 5	1 2 . 5	2 . 5	6 2 . 5	2 0. 0	1 0. 0	2 7 . 5	1 0 . 0	4 5 . 0	7. 5	5. 0	1 2 . 5	0	5 5 . 0	2 7 . 5
Lack of abiliti es to fully under stand the new techn ology	0	2 5 . 0	0	5 5 . 0	2 0 . 0	2. 5	1 2 . 5	5 . 0	5 7 . 5	2 2. 5	5. 0	3 2 . 5	7 . 5	5 0 . 0	5. 0	5. 0	1 2 . 5	0	5 7 . 5	2 5 . 0
Lack of abiliti es to fully under stand the need of techn ologi cal upgra dation	1 5. 0	7 . 5	0	4 7 . 5	3 0 . 0	7. 5	1 5 . 0	2 . 5	4 7 . 5	2 7. 5	7. 5	1 0 . 0	5 . 0	5 5 . 0	2 2. 5	5. 0	1 5 . 0	0	5 2 . 5	2 7 . 5

Private Sector Banks

Table 4.15 shows that most respondents agree or strongly agree that the groups' chosen banks are at danger due to inexperienced management and outmoded employees.

Table 4. 15 Factors Responsible for Risk of Outdated Staff and Lack of Management Expertise in Selected Private Sector Banks

Factors	AXIS					HDFC					ICICI				
	SD	D	N	A	S A	SD	D	N	A	SA	S D	D	N	A	S A
Outdated recruitment, selection placement and promotion policies	0	10 .0	0	42 .5	47 .5	5.0	5. 0	5. 0	27 .5	57. 5	0	12 .5	0	45 .0	42 .5
Lack of proper and timely training and development facilities	2.5	15 .0	0	62 .5	20 .0	5.0	10 .0	12 .5	45 .0	27. 5	5. 0	10 .0	0	45 .0	40 .0
Absence of challenging opportunities to the staff for growth	7.5	10 .0	0	60 .0	22 .5	5.0	7. 5	20 .0	37 .5	30. 0	0	20 .0	5. 0	45 .0	30 .0
Lack of abilities to fully understand and the	5.0	20 .0	2. 5	37 .5	35 .0	7.5	10 .0	20 .0	35 .0	27. 5	2. 5	15 .0	7. 5	52 .5	22 .5

new technol ogy															
Lack of abilities to fully underst and the need of technol ogical upgrada tion	2.5	12 .5	0	62 .5	22 .5	15. 0	5. 0	15 .0	42 .5	22. 5	5. 0	12 .5	2. 5	45 .0	35 .0

Group-wise Comparison

Table 4.16 shows that most respondents recognize the elements that put the specified groupings of banks at danger of having out-of-date personnel and incompetent management.

Table 4. 16 Factors Responsible for Risk of Outdated Staff and Lack of Management Expertise in Selected Groups of Banks

Factors	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Outdated recruitme nt, selection, placemen t and promotio n policies	1. 7	11. 7	3. 3	47. 5	35. 8	5. 0	10. 0	1. 5	35. 5	48. 0	1. 7	9.2	1.7	38. 3	49. 2
Lack of proper and timely training and develop ment facilities	2. 5	7.5	5. 0	52. 5	32. 5	4. 0	6.5	6. 0	56. 5	27. 0	4. 2	11. 7	4.2	50. 8	29. 2
Absence of challengi ng opportuni	4. 2	15. 8	5. 0	50. 8	24. 2	4. 5	17. 0	3. 0	54. 5	21. 0	4. 2	12. 5	8.3	47. 5	27. 5

ties to the staff for growth															
Lack of abilities to fully understand the new technology	3.3	17.5	5.0	47.5	26.7	3.5	19.5	2.5	55.5	19.0	5.0	15.0	10.0	41.7	28.3
Lack of abilities to fully understand the need of technological upgradation	6.7	12.5	2.5	49.2	29.2	7.5	10.5	1.5	50.5	30.0	7.5	10.0	5.8	50.0	26.7

2. Impacts of Risk

State Bank Group

Table 4.17 shows that most people are in agreement or strongly believe that the State Bank Group's chosen banks are at danger of having incompetent management and out-of-date employees negatively affect their operations.

Table 4. 17 Impacts of Outdated Staff and Lack of Management Expertise in Selected Banks of State Bank Group

Impacts	SBI					TGB					APGVB				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Poor implementation of new technology	5.0	7.5	0	37.5	50.0	2.5	2.5	0	37.5	57.5	10.0	0	0	50.0	40.0
Inability to provide ongoing support	0	22.5	2.5	50.0	25.0	2.5	10.0	2.5	65.0	20.0	10.0	2.5	5.0	47.5	35.0
Deficiencies in the system	5.0	10.0	2.5	50.0	32.5	12.5	17.5	2.5	47.5	20.0	5.0	17.5	5.0	45.0	27.5

Lack of reliability of the staff and system	5.0	25.0	0	37.5	32.5	15.0	17.5	0	47.5	20.0	7.5	17.5	5.0	42.5	27.5
Delay in customer service	5.0	10.0	0	45.0	40.0	7.5	17.5	0	45.0	30.0	7.5	12.5	5.0	62.5	12.5
Poor quality of customer service	0	22.5	5.0	40.0	32.5	2.5	12.5	0	60.0	25.0	10.0	15.0	2.5	42.5	30.0
High cost of providing service	5.0	22.5	0	42.5	30.0	5.0	25.0	0	52.5	17.5	15.0	22.5	2.5	40.0	20.0

Nationalized Banks

Table 4.18 shows that most people are in agreement or strongly agree that the chosen nationalized banks are at danger of having incompetent management and out-of-date employees negatively affect their operations.

Table 4. 18 Impacts of Risk of Outdated Staff and Lack of Management Expertise in Selected Nationalized Banks

Impacts	UBI					BOB					PNB					CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Poor implementation of new technology	5.0	2.5	0	4.5	50.0	0	2.5	2.5	3.5	5.5	5.0	1.0	2.5	4.5	4.0	2.5	1.5	0	4.5	4.0
Inability to provide ongoing support	5.0	7.5	2.5	5.0	30.0	2.5	2.5	2.5	6.0	3.5	5.0	7.5	5.0	6.5	1.5	7.5	5.0	0	6.0	2.5
Deficiencies in the system	7.5	1.2	2.5	5.0	27.5	2.5	1.2	5.0	5.0	3.0	2.5	1.0	1.0	5.2	2.5	0	1.2	0	6.7	2.0

Lack of reliability of the staff and system	10.0	10.0	0	65.0	15.0	7.5	17.5	2.5	45.0	27.5	10.0	17.5	2.5	45.0	2.5	10.0	2.5	60.0	25.0
Delay in customer service	10.0	15.0	2.5	4.5	30.0	5.0	12.5	5.0	45.0	32.5	7.5	15.0	10.0	4.5	2.5	5.0	0	62.5	27.5
Poor quality of customer service	7.5	17.5	2.5	5.0	22.5	0	5.0	0	70.0	25.0	7.5	10.0	7.5	5.5	2.5	0	7.5	62.5	30.0
High cost of providing service	15.0	7.5	0	5.0	22.5	10.0	7.5	5.0	50.0	27.5	10.0	7.5	7.5	4.0	3.5	2.5	17.5	0	37.5

Private Sector Banks

The majority of respondents agree or strongly agree that the chosen private sector banks are at danger of having out-of-date personnel and inadequate management, as indicated in Tables 4.19.

Table 4. 19 Impacts of Outdated Staff and Lack of Management Expertise in Selected Private Sector Banks

Impacts	AXIS					HDFC					ICICI				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Poor implementation of new technology	0	15.0	0	35.0	50.0	0	7.5	5.0	27.5	60.0	0	22.5	0	35.0	42.5
Inability to provide ongoing support	5.0	5.0	0	60.0	30.0	0	2.5	12.5	55.0	30.0	2.5	15.0	2.5	57.5	22.5
Deficiency	12	10	2.	45	30	2.	7.	25	47	17	5.	7.	0	60	27

es in the system	.5	.0	5	.0	.0	5	5	.0	.5	.5	0	5		.0	.5
Lack of reliability of the staff and system	5.0	15.0	0	45.0	35.0	5.0	25.0	7.5	42.5	20.0	2.5	22.5	7.5	37.5	30.0
Delay in customer service	10.0	7.5	0	57.5	25.0	12.5	5.0	17.5	52.5	12.5	0	17.5	2.5	42.5	37.5
Poor quality of customer service	2.5	10.0	0	55.0	32.5	5.0	5.0	17.5	45.0	27.5	0	27.5	2.5	37.5	32.5
High cost of providing service	7.5	12.5	0	55.0	25.0	0	12.5	22.5	35.0	30.0	0	7.5	2.5	47.5	42.5

Group-wise Comparison

The effects of the danger of out-of-date personnel and a lack of managerial competence on the operations of the chosen groups of banks are acknowledged by most respondents (Table 4.20).

Table 4. 20 Impacts of Risk of Outdated Staff and Lack of Management Expertise in Selected Groups of Banks

Impacts	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Poor implementation of new technology	5.8	3.3	0	41.7	49.2	3.0	8.5	1.5	42.0	45.0	0	15.0	1.7	32.5	50.8
Inability to provide ongoing support	4.2	11.7	3.3	54.2	26.7	4.5	6.0	3.0	59.5	27.0	2.5	7.5	5.0	57.5	27.5
Deficiencies in the system	7.5	15.0	3.3	47.5	26.7	3.5	11.5	4.5	52.5	28.0	6.7	8.3	9.2	50.8	25.0
Lack of reliability of the staff and system	9.2	20.0	1.7	42.5	26.7	6.0	14.0	1.5	53.0	25.5	4.2	20.8	5.0	41.7	28.3
Delay in	6.	13	1.	50	27	7.	12	4.	46	29	7.	10	6.	50	25

customer service	7	.3	7	.8	.5	5	.0	5	.5	.5	5	.0	7	.8	.0
Poor quality of customer service	4.2	16.7	2.5	47.5	29.2	3.5	11.0	2.5	57.5	25.5	2.5	14.2	6.7	45.8	30.8
High cost of providing service	8.3	23.3	0.8	45.0	22.5	8.5	12.0	2.5	45.5	31.5	2.5	10.8	8.3	45.8	32.5

3. Risk Management Measures

State Bank Group

The proposed solutions to the problem of inexperienced managers and out-of-date personnel in the chosen group banks have garnered widespread support, as indicated in Table 4.21.

Table 4. 21 Measures for Overcoming the Risk of Outdated Staff and Lack of Management Expertise in Selected Banks of State Bank Group

Measure s	SBI					TGB					APGVB				
	SD	D	N	A	S A	S D	D	N	A	S A	SD	D	N	A	S A
Use of modern techniques of recruitment, selection, placement and promotion of staff and management	7.5	2.5	2.5	35.0	52.5	5.0	5.0	0	40.0	50.0	2.5	0	2.5	50.0	45.0

ent															
Developing corporate view of training and development as an ongoing process	7.5	7.5	5.0	40.0	40.0	2.5	2.5	0	60.0	35.0	0	2.5	2.5	65.0	30.0
Providing training to staff and management at planning stage	5.0	12.5	2.5	20.0	60.0	2.5	2.5	0	65.0	30.0	12.5	15.0	0	32.5	40.0
Providing training to staff and management at implementation stage	5.0	7.5	5.0	40.0	42.5	5.0	10.0	2.5	47.5	35.0	7.5	15.0	2.5	47.5	27.5
Providing training to staff and management	5.0	10.0	0	27.5	57.5	5.0	12.5	2.5	37.5	42.5	22.5	10.0	5.0	25.0	37.5

ent at monitorin g and control stage																			
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Nationalized Banks

The steps to mitigate the danger of inexperienced managers and out-of-date personnel in the chosen nationalized banks have garnered widespread support, as shown in Table 4.22.

Table 4. 22 Measures for Overcoming the Risk of Outdated Staff and Lack of Management Expertise in Selected Nationalized Banks

Measu res	UBI					BOB					PNB					CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Use of moder n techni ques of recruit ment selecti on, placem ent and promot ion of staff and manag ement	0	0	0	5 0 0	50 .0	2 .5	0	2 .5	4 0 0	55 .0	5 0	5 0	5 0	5 5 0	3 0 0	7. 5	7 .5	0	4 0 0	4 5 0
Develo ping corpor ate view	2 .5	2 .5	5 0	6 2 .5	27 .5	2 .5	2. 5	5 0	5 0	40 .0	7 .5	1 5 0	0	5 5 0	2 2. 5	5. 0	5 .0	0	4 5 0	4 5 0

of trainin g and develo pment as an ongoin g proces s																				
Provid ing trainin g to staff and manag ement at planni ng stage	7 .5	2 0 .0	7 .5	3 7 .5	27 .5	0	1 0. 0	7 .5	5 0 .0	32 .5	7 .5	1 0 .0	5 .0	6 2 .5	1 5. 0	0	7 .5	0	5 7 .5	3 5 .0
Provid ing trainin g to staff and manag ement at imple mentat ion stage	5 .0	2 7 .5	7 .5	4 2 .5	17 .5	0	1 0. 0	5 .0	6 0 .0	25 .0	1 5 .0	5 .0	5 .0	5 7 .5	1 7. 5	0	1 5 .0	0	5 2 .5	3 2 .5
Provid ing trainin g to staff and manag ement	1 0 .0	2 .5	7 .5	4 7 .5	32 .5	1 0 .0	1 2. 5	0	5 5 .0	22 .5	5 .0	2 0 .0	7 .5	4 2 .5	2 5. 0	1 5. 0	7 .5	0	3 5 .0	4 2 .5

at monito ring and control stage																			
---	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Private Sector Banks

Table 4.23 shows that most people are in agreement or strongly in agreement on the steps that the chosen private sector banks may do to avoid having out-of-date employees and inadequate management.

Table 4. 23 Measures for Overcoming the Risk of Outdated Staff and Lack of Management Expertise in Selected Private Sector Banks

Measures	AXIS					HDFC					ICICI				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Use of modern techniques of recruitment, selection, placement and promotion of staff and management	5. 0	7. 5	0	30 .0	57 .5	0	0	7. 5	40 .0	52 .5	0	0	0	55 .0	45 .0
Developing corporate view of training and development as an ongoing process	10 .0	12 .5	0	52 .5	25 .0	0	2. 5	5. 0	65 .0	27 .5	0	2. 5	0	55 .0	42 .5
Providing training to staff and	5. 0	15 .0	0	50 .0	30 .0	0	10 .0	12 .5	42 .5	35 .0	2. 5	7. 5	2. 5	47 .5	40 .0

managem nt at planning stage															
Providing training to staff and managem nt at implement ation stage	2. 5	20 .0	2. 5	32 .5	42 .5	5. 0	20 .0	5. 0	37 .5	32 .5	2. 5	5. 0	7. 5	40 .0	45 .0
Providing training to staff and managem nt at monitorin g and control stage	10 .0	7. 5	0	55 .0	27 .5	10 .0	10 .0	5. 0	32 .5	42 .5	0	5. 0	0	47 .5	47 .5

Group-wise Comparison

Table 4.24 shows that on the measures to overcome the danger of out-of-date personnel and a lack of managerial skills, the majority of respondents in the chosen groups of banks agree or strongly agree.

Table 4. 24 Measures for Overcoming the Risk of Outdated Staff and Lack of Management Expertise in Selected Groups of Banks

Measures	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Use of modern techniques of recruitmen t, selection, placement and promotion of staff	5. 0	2. 5	1. 7	41 .7	49 .2	3. 0	4. 5	2. 0	46 .0	44 .5	1. 7	2. 5	2. 5	41 .7	51 .7

and manageme nt															
Developin g corporate view of training and developme nt as an ongoing process	3. 3	4. 2	2. 5	55 .0	35 .0	3. 5	6. 0	2. 5	50 .0	38 .0	3. 3	5. 8	1. 7	57 .5	31 .7
Providing training to staff and manageme nt at planning stage	6. 7	10 .0	.8	39 .2	43 .3	3. 5	11 .5	4. 0	50 .5	30 .5	2. 5	10 .8	5. 0	46 .7	35 .0
Providing training to staff and manageme nt at implement ation stage	5. 8	10 .8	3. 3	45 .0	35 .0	5. 0	15 .0	3. 5	50 .0	26 .5	3. 3	15 .0	5. 0	36 .7	40 .0
Providing training to staff and manageme nt at monitorin g and control stage	10 .8	10 .8	2. 5	30 .0	45 .8	8. 0	11 .0	3. 5	44 .0	33 .5	6. 7	7. 5	1. 7	45 .0	39 .2

4.2 RESULTS RELATED TO INFORMATION TECHNOLOGY (IT) ORIENTED OPERATIONAL RISKS

In this research, we examine the causes of IT-oriented operational risks in e-banking, how these risks affected the banks' operations, and what the institutions did to mitigate these risks.

4.2.1 Risk of Inadequate Customers' Security Practices

This risk arises when the bank fails to adequately protect its clients' personal information, which leads to a breach of trust and potential customer attrition to rival financial institutions. at this part, we will examine the causes of risk, how it affects the financial institutions' operations, and the steps taken to address the problem of insufficient consumer security measures at a few different banks.

1. Factors Responsible for Risk

State Bank Group

Tables 4.25 reveal that most respondents in the State Bank Group's sampled institutions agree or strongly agree that the following issues contribute to the danger of insufficient client security policies.

Table 4. 25 Factors Responsible for Risk of Inadequate Customers' Security Practices in Selected Banks of State Bank Group

Factors	SBI					TGB					APGVB				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Lack of reliability of information system	12.5	22.5	0	20.0	45.0	0	17.5	0	37.5	45.0	0	7.5	2.5	57.5	32.5
Lack of awareness about the compliance of security mechanism	2.5	7.5	5.0	52.5	32.5	0	15.0	0	52.5	32.5	2.5	0	2.5	62.5	32.5
Use of personal information by the customers (credit card)	7.5	10.0	2.5	42.5	37.5	2.5	25.0	7.5	30.0	35.0	7.5	15.0	0	42.5	35.0

numbers, bank account numbers) in non-secure electronic transmissions																
Access of confidential information of customer accounts by criminals	5.0	20.0	5.0	47.5	22.5	2.5	15.0	0	57.5	25.0	12.5	7.5	2.5	52.5	25.0	

Nationalized Banks

Table 4.26 shows that most respondents agreed or strongly agreed that the following variables contributed to the danger of weak client security policies in the nationalized banks that were chosen.

Table 4. 26 Factors Responsible for Risk of Inadequate Customers' Security Practices in Selected Nationalized Banks

Fact ors	UBI					BOB					PNB					CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Lack of reliability of information system	5.0	5.0	0	5.0	4.0	5.0	7.5	0	4.5	4.0	5.0	1.5	1.0	4.5	3.0	2.5	1.5	2.5	3.5	5.0
Lack of awareness about	5.0	2.5	2.5	6.0	3.0	5.0	2.5	1.0	5.5	3.0	2.5	1.5	1.0	5.0	2.0	0	1.5	0	5.5	3.0

the compliance of security mechanism																				
Use of personal information by the customers (credit card numbers, bank account numbers) in non-secure electronic transmissions	5 . 0	1 2. 5	2. 5	4 5. 0	3 5. 0	5. 0	1 7. 5	2 0. 0	4 2. 5	1 5. 0	5 . 0	7. 5	2 0. 0	4 7. 5	2 0. 0	2 . 5	7. 5	0	6 0. 0	3 0. 0
Access of confidential information of customer accounts by	7 . 5	7. 5	1 2. 5	4 5. 0	2 7. 5	1 2. 5	7. 5	1 0. 0	5 2. 5	1 7. 5	5 . 0	2 2. 5	1 2. 5	4 0. 0	2 0. 0	2 . 5	1 0. 0	2 . 5	5 5. 0	3 0. 0

crimi nals																			
---------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Private Sector Banks

Table 4.27 shows that in a subset of private sector banks, most respondents agree or strongly agree that certain characteristics contribute to the risk of insufficient client security policies.

Table 4. 27 Factors Responsible for Risk of Inadequate Customers' Security Practices in Selected Private Sector Banks

Factors	AXIS					HDFC					ICICI				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Lack of reliability of information system	5.0	2.5	2.5	37.5	52.5	5.0	5.0	10.0	27.5	52.5	0	5.0	0	65.0	30.0
Lack of awareness about the compliance of security mechanism	5.0	12.5	0	47.5	35.0	5.0	5.0	17.5	45.0	27.5	0	12.5	5.0	60.0	22.5
Use of personal information by the customers (credit card numbers, bank account numbers) in non-secure electronic	5.0	15.0	0	57.5	22.5	5.0	12.5	15.0	42.5	25.0	0	7.5	5.0	45.0	42.5

transmissions															
Access of confidential information of customer accounts by criminals	15.0	7.5	0	50.0	27.5	7.5	15.0	7.5	35.0	35.0	0	15.0	10.0	45.0	30.0

Group-wise Comparison

Table 4.28 shows that in all the nationalized banks that were chosen, the majority of respondents agree or strongly agree that certain characteristics contribute to the danger of insufficient client security policies.

Table 4. 28 Factors Responsible for Risk of Inadequate Customers' Security Practices in Selected Groups of Banks

Factors	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Lack of reliability of information system	4.2	15.8	.8	38.3	40.8	3.5	9.0	3.5	43.0	41.0	3.3	4.2	4.2	43.3	45.0
Lack of awareness about the compliance of security mechanism	1.7	7.5	2.5	55.8	32.5	2.5	6.5	6.5	56.5	28.0	3.3	10.0	7.5	50.8	28.3
Use of personal information by the customer	5.8	16.7	3.3	38.3	35.8	4.5	12.0	10.0	46.5	27.0	3.3	11.7	6.7	48.3	30.0

s (credit card numbers, bank account numbers) in non-secure electronic transmissions															
Access of confidential information of customers' accounts by criminals	6.7	14.2	2.5	52.5	24.2	6.0	11.5	9.0	46.5	27.0	7.5	12.5	5.8	43.3	30.8

2. Impacts of Risk

State Bank Group

Table 4.29 shows that most respondents agree or strongly agree that the chosen Group banks are vulnerable to the effects of insufficient client security policies on their operations.

Table 4. 29 Impacts of Risk of Inadequate Customers' Security Practices in Selected Banks of State Bank Group

Impacts	SBI					TGB					APGVB				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Financial loss through unauthorized transactions	5.0	7.5	2.5	50.0	35.0	0	12.5	2.5	37.5	47.5	5.0	7.5	2.5	57.5	27.5
Potential adverse publicity about the	5.0	12.5	2.5	45.0	35.0	0	12.5	5.0	47.5	35.0	10.0	2.5	2.5	42.5	42.5

bank															
Loss of existing and potential customers	0	15.0	2.5	40.0	42.5	2.5	20.0	5.0	35.0	37.5	10.0	10.0	2.5	35.0	42.5

Nationalized Banks

The majority of respondents agree or strongly agree that the chosen nationalized banks are at danger due to insufficient consumer security policies, as indicated in Table 4.30.

Table 4. 30 Impacts of Risk of Inadequate Customers' Security Practices in Selected Nationalized Banks

Imp acts	UBI						BOB					PNB				CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Financial loss through unauthorized transactions	0	5.0	0	70.0	25.0	2.5	2.5	2.5	42.5	5.0	5.0	1.0	5.0	60.0	2.0	0	2.5	0	57.5	4.0
Potential adverse publicity about the bank	5.0	10.0	5.0	47.5	32.5	2.5	1.0	7.5	57.5	2.5	0	1.0	7.5	47.5	2.5	7.5	2.5	5.5	5.0	32.5
Loss of exis	5.0	12.5	7.5	52.5	22.5	2.5	0	7.5	50.0	4.0	0	1.7	1.0	5.0	17.5	0	7.5	0	5.0	37.5

ting and pote ntial cust ome rs											5								
---	--	--	--	--	--	--	--	--	--	--	---	--	--	--	--	--	--	--	--

Private Sector Banks

The majority of respondents agree or strongly agree that the chosen private sector banks are at danger of weak client security policies, as indicated in Table 4.31.

Table 4. 31 Impacts of Risk of Inadequate Customers' Security Practices in Selected Private Sector Banks

Impacts	AXIS					HDFC					ICICI				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Financial loss through unauthorized transactions	2.5	2.5	0	42.5	52.5	2.5	2.5	20.0	35.0	40.0	2.5	7.5	5.0	30.0	55.0
Potential adverse publicity about the bank	5.0	10.0	2.5	50.0	32.5	2.5	7.5	10.0	47.5	32.5	0	5.0	10.0	60.0	25.0
Loss of existing and potential	7.5	12.5	0	47.5	32.5	5.0	12.5	22.5	25.0	35.0	0	7.5	5.0	47.5	40.0

customer s															
---------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Group-wise Comparison

Table 4.32 shows that most respondents agree or strongly agree that the specified categories of banks are vulnerable to the effects of insufficient client security policies.

Table 4. 32 Impacts of Risk of Inadequate Customers' Security Practices in Selected Groups of Banks

Impacts	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	SA	S D	D	N	A	SA	S D	D	N	A	SA
Financial loss through unauthorized transactions	3.3	9.2	2.5	48.3	36.7	1.5	6.0	3.0	53.5	36.0	2.5	4.2	8.3	35.8	49.2
Potential adverse publicity about the bank	5.0	9.2	3.3	45.0	37.5	2.5	11.0	9.0	50.0	27.5	2.5	7.5	7.5	52.5	30.0
Loss of existing and potential customers	4.2	15.0	3.3	36.7	40.8	2.5	9.0	6.5	51.5	30.5	4.2	10.8	9.2	40.0	35.8

3. Risk Management Measures

State Bank Group

Table 4.33 shows that most respondents are in favor of the actions to address the potential danger of insufficient client security policies in all of the group's chosen institutions.

Table 4. 33 Measures for Overcoming the Risk of Inadequate Customers’ Security Practices in Selected Banks of State Bank Group

Measures	SBI					TGB					APGVB				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Providing information to the customers on the importance of safeguarding information in non-secure transactions.	5.0	2.5	0	32.5	60.0	0	0	0	47.5	52.5	2.5	2.5	0	60.0	35.0
Incorporating security measures into products and services	2.5	5.0	0	40.0	52.5	0	0	0	70.0	30.0	2.5	7.5	2.5	47.5	40.0
Enforcing necessary level of secrecy at each stage of data processing	2.5	0	0	45.0	52.5	2.5	7.5	0	52.5	37.5	12.5	10.0	2.5	32.5	42.5

and preventing unauthorized disclosure															
Providing direction for all future security activities within the organization	5.0	5.0	2.5	47.5	40.0	2.5	12.5	2.5	57.5	25.0	2.5	20.0	2.5	50.0	25.0
Addressing specific security issues that management feels more detailed explanation	5.0	7.5	0	42.5	45.0	0	12.5	2.5	40.0	45.0	5.0	10.0	2.5	47.5	35.0
Building a comprehensive structure and ensuring that all employees understand how they have to comply with these security issues	2.5	7.5	0	45.0	45.0	0	12.5	0	47.5	40.0	10.0	5.0	0	55.0	30.0
Presenting the management's decisions that are specific to	0	2.5	0	45.0	52.5	5.0	7.5	2.5	42.5	42.5	10.0	7.5	2.5	52.5	27.5

the computing networks, applicatio ns and data																	
---	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Nationalized Banks

All of the chosen nationalized banks have procedures in place to mitigate the risk of insufficient client security practices, as indicated in Table 4.34.

Table 4. 34 Measures for Overcoming the Risk of Inadequate Customers’ Security Practices in Selected Nationalized Banks

Meas ures	UBI					BOB					PNB					CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Provid ing infor matio n to the custo mers on the import ance of safegu arding infor matio n in non- secure transa ctions	2. 5	5 . 0	0	4 2 . 5	50 .0	2 . 5	0	5 . 0	3 0 . 0	6 2 . 5	0	1 0 . 0	2 . 5	6 0 . 0	2 7 . 5	0	2 . 5	2 . 5	5 5 . 0	4 0 . 0
Incorp oratin g securit y measu res into	5. 0	1 5 . 0	0	5 5 . 0	25 .0	0 . 5	2 . 5	2 . 5	6 0 . 0	3 5 . 0	5. 0	1 7 . 5	1 0 . 0	4 5 . 0	2 2 . 5	2 . 5	7 . 5	2 . 5	5 0 . 0	3 7 . 5

products and services																				
Enforcing necessary level of secrecy at each stage of data processing and preventing unauthorized disclosure	2.5	12.5	7.5	45.0	32.5	5.0	2.5	12.5	50.0	30.0	10.0	12.5	10.0	40.0	27.5	5.0	15.0	2.5	40.0	37.5
Providing directions for all future security activities within the organization	7.5	10.0	10.0	40.0	32.5	2.5	7.5	5.0	52.5	32.5	2.5	20.0	2.5	50.0	25.0	5.0	2.5	0	47.5	45.0
Addressing specific security issues that manag	5.0	10.0	2.5	50.0	32.5	2.5	10.0	2.5	55.0	30.0	7.5	7.5	2.5	57.5	25.0	2.5	2.5	2.5	62.5	30.0

ement feels more detaile d explan ation																				
Buildi ng a compr ehensi ve struct ure and ensuri ng that all emplo yees unders tand how they have to compl y with these securit y issues	5. 0	2 0 . 0	7 . 5	4 0 . 0	27 .5	5 . 0	7 . 5	5 . 0	4 7 . 5	3 5 . 0	5. 0	2 . 5	2 . 5	6 5 . 0	2 5 . 0	0	1 5 . 0	0	5 7 . 5	2 7 . 5
Presen ting the manag ement' s decisi on that are specifi c to the comp uting netwo rks,	5. 0	1 7 . 5	0	5 0 . 0	27 .5	7 . 5	5 . 0	2 . 5	5 7 . 5	2 7 . 5	5. 0	1 2 . 5	1 0 . 0	5 2 . 5	2 0 . 0	1 0 . 0	5 . 0	0	3 2 . 5	5 2 . 5

applic ations and data																			
---------------------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Private Sector Banks

Table 4.35 shows that most people are in favor of the actions taken by the chosen private sector banks to address the possibility of insufficient customer security procedures.

Table 4. 35 Measures for Overcoming the Risk of Inadequate Customers’ Security Practices Selected Private Sector Banks

Measures	AXIS					HDFC					ICICI				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Providing information to the customers on the importance of safeguarding information in non-secure transactions	5.0	2.5	0	37.5	55.0	0	0	12.5	40.0	47.5	0	2.5	0	60.0	37.5
Incorporating security measures into products and services	0	20.0	0	50.0	30.0	2.5	0	2.5	62.5	32.5	2.5	5.0	0	57.5	35.0
Enforcing necessary level of secrecy at each stage of data processing	5.0	10.0	0	47.5	37.5	2.5	7.5	5.0	55.0	30.0	0	7.5	2.5	67.5	22.5

g and preventin g unauthori zed disclosure															
Providing directions for all future security activities within the organization	7.5	12.5	0	50.0	30.0	2.5	10.0	2.5	60.0	25.0	0	5.0	5.0	47.5	42.5
Addressin g specific security issues that managem ent feels more detailed explanati on	0	20.0	0	42.5	37.5	0	10.0	20.0	37.5	32.5	0	7.5	10.0	52.5	30.0
Building a comprehe nsive structure and ensuring that all employee s understand how they have to comply with these security issues	7.5	15.0	5.0	40.0	32.5	7.5	5.0	12.5	47.5	27.5	0	7.5	5.0	45.0	42.5
Presentin g the managem ent's decisions	7.5	5.0	10.0	42.5	35.0	7.5	5.0	10.0	42.5	35.0	0	12.5	7.5	42.5	37.5

that are specific to the computing networks, applications and data															
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Group-wise Comparison

Table 4.36 shows that most respondents in the chosen categories of banks agree or strongly agree with the strategies to overcome the danger of weak client security standards.

Table 4. 36 Measures for Overcoming the Risk of Inadequate Customers' Security Practices in Selected Groups of Banks

Measures	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Providing information to the customers on the importance of safeguarding information in non-secure transactions	2.5	1.7	0	46.7	49.2	2.0	4.5	2.5	45.0	46.0	1.7	1.7	4.2	45.8	46.7
Incorporating security measures into products and services	1.7	4.2	0.8	52.5	40.8	2.5	9.5	4.0	53.0	31.0	1.7	8.3	0.8	56.7	32.5
Enforcing necessary level of secrecy at	5.8	5.8	0.8	43.3	44.2	4.5	10.5	7.0	42.5	35.5	2.5	8.3	2.5	56.7	30.0

each stage of data processing and preventing unauthorized disclosure															
Providing directions for all future security activities within the organization	3.3	12.5	2.5	51.7	30.0	4.0	10.5	4.5	46.5	34.5	3.3	9.2	2.5	52.5	32.5
Addressing specific security issues that management feels more detailed explanation	3.3	10.0	1.7	43.3	41.7	4.0	9.5	2.0	52.5	32.0	0	12.5	10.0	44.2	33.3
Building a comprehensive structure and ensuring that all employee understand how they have to comply with these security issues	4.2	8.3	0	49.2	38.3	3.0	12.0	3.5	49.0	32.5	5.0	9.2	7.5	44.2	34.2
Presenting the management's decisions that are specific to	5.0	5.8	1.7	46.7	40.8	6.0	9.0	3.0	51.0	31.0	5.8	10.8	6.7	42.5	34.2

the actual computers , networks, applications and data															
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

4.2.2 Risk of Hacking

There is a possibility of hacking if the user tried to enter the system with an invalid permission (password or username) and was denied access. To rephrase, hacking occurs when an unauthorized user obtains access to a system in a way that the owner of the system did not intend. This section delves into the examination of risk variables, their effects on bank operations, and the steps taken to mitigate hacking threats at specific banks, both individually and collectively.

1. Factors Responsible for Risk

State Bank Group

Table 4.37 shows that most respondents agree or strongly agree that the following variables contribute to the group's chosen banks' vulnerability to hacking.

Table 4. 37 Factors Responsible for Risk of Hacking in Selected Banks of State Bank Group

Factors	SBI					TGB					APGVB				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Easy entry of hackers into the system	5. 0	15 .0	2. 5	25 .0	52 .5	2. 5	12 .5	0	40 .0	45 .0	2. 5	2. 5	2. 5	52 .5	40 .0
Breach with confidentiality of customers	10 .0	10 .0	0	52 .5	27 .5	0	7. 5	2. 5	57 .5	32 .5	2. 5	12 .5	2. 5	27 .5	55 .0
Illegal obstruction of unauthorized	15 .0	17 .5	0	35 .0	32 .5	0	17 .5	2. 5	52 .5	27 .5	2. 5	15 .0	7. 5	45 .0	30 .0

person(s)																
Introducing virus into the system	12.5	15.0	2.5	47.5	22.5	0	20.0	2.5	67.5	10.0	15.0	15.0	0	35.0	35.0	
Bank's system deliberately crashed	7.5	22.5	0	37.5	32.5	5.0	25.0	2.5	45.0	22.5	12.5	15.0	7.5	45.0	20.0	
Bank's data corrupted intentionally	15.0	15.0	0	42.5	27.5	5.0	25.0	5.0	42.5	22.5	15.0	10.0	7.5	35.0	32.5	

Nationalized Banks

Table 4.38 shows that most respondents hold the view that the following variables contribute to the danger of hacking in the nationalized banks that were chosen.

Table 4. 38 Factors Responsible for Risk of Hacking in Selected Nationalized Banks

Factors	UBI					BOB					PNB					CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Easy entry of hackers into the system	10.0	5.0	0	4.0	4.5	2.5	2.5	2.5	3.75	5.0	7.5	2.5	2.5	4.5	4.25	2.5	5.0	0	5.25	4.0
Breach with confidentiality of customers	5.0	5.0	2.5	5.0	3.25	2.5	5.0	2.5	6.25	2.5	2.5	1.5	2.5	6.25	1.75	7.5	1.0	0	5.75	2.5
Illegal obstruction of unauthorized persons	5.0	1.25	7.5	4.0	3.5	0	1.25	7.5	6.5	1.5	5.0	1.25	7.5	5.0	2.5	2.5	1.5	0	5.75	2.5

n(s)																				
Introducing virus into the system	22.5	7.5	2.5	4.5	2.5	2.5	2.5	2.5	3.7	3.2	7.5	2.0	2.5	4.2	2.7	7.5	5.0	0	6.2	2.5
Bank's system deliberately crashed	15.0	1.7	7.5	4.2	1.7	12.5	1.2	2.5	4.7	2.5	7.5	7.5	5.0	4.2	3.7	7.5	2.2	0	5.0	2.0
Bank's data corrupted intentionally	12.5	1.2	0.5	5.0	2.0	10.0	1.0	2.5	5.5	2.5	12.5	1.0	5.0	3.7	3.5	7.5	1.0	0	5.5	2.7

Private Sector Banks

Table 4.39 shows that most respondents agree or strongly agree that the following variables contribute to the chosen nationalized banks' vulnerability to hacking.

Table 4. 39 Factors Responsible for Risk of Hacking in Selected Private Sector Banks

Factors	AXIS					HDFC					ICICI				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Easy entry of hackers into the system	5.0	2.5	0	32.5	60.0	0	5.0	10.0	37.5	47.5	0	5.0	0	55.0	40.0
Breach with confidentiality of customers	5.0	5.0	0	62.5	27.5	0	10.0	17.5	42.5	30.0	0	7.5	2.5	65.0	25.0
Illegal obstruction of unauthorized	5.0	12.5	2.5	47.5	32.5	5.0	10.0	15.0	35.0	35.0	0	10.0	7.5	62.5	20.0

person(s)															
Introducing virus into the system	10 .0	20 .0	0	55 .0	15 .0	7. 5	12 .5	12 .5	40 .0	27 .5	5. 0	15 .0	0	57 .5	22 .5
Bank's system deliberately crashed	12 .5	10 .0	0	47 .5	30 .0	7. 5	12 .5	17 .5	32 .5	30 .0	5. 0	12 .5	2. 5	52 .5	27 .5
Bank's data corrupted intentionally	5. 0	7. 5	0	45 .0	42 .5	7. 5	10 .0	17 .5	32 .5	32 .5	2. 5	15 .0	7. 5	47 .5	27 .5

Group-wise Comparison

The majority of respondents in the chosen groups of banks agree or strongly agree about the elements responsible for the danger of hacking, as indicated in Table 4.40.

Table 4. 40 Factors Responsible for Risk of Hacking in Selected Groups of Banks

Factors	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Easy entry of hackers into the system	3. 3	10 .0	1. 7	39 .2	45 .8	5. 5	4. 0	1. 5	44 .0	45 .0	1. 7	4. 2	3. 3	41 .7	49 .2
Breach with confidentiality of customers	4. 2	10 .0	1. 7	45 .8	38 .3	4. 5	9. 0	2. 0	59 .5	25 .0	1. 7	7. 5	6. 7	56 .7	27 .5
Illegal obstruction of unauthorized person(s)	5. 8	16 .7	3. 3	44 .2	30 .0	3. 5	15 .0	5. 5	53 .5	22 .5	3. 3	10 .8	8. 3	48 .3	29 .2
Introducing virus into the system	9. 2	16 .7	1. 7	50 .0	22 .5	8. 0	15 .5	2. 5	46 .0	28 .0	7. 5	15 .8	4. 2	50 .8	21 .7
Bank's system deliberately crashed	8. 3	20 .8	3. 3	42 .5	25 .0	11 .5	14 .5	3. 5	45 .0	25 .5	8. 3	11 .7	6. 7	44 .2	29 .2

Bank's data corrupted intentionally	11.7	16.7	4.2	40.0	27.5	10.0	14.5	2.0	48.0	25.5	5.0	10.8	8.3	41.7	34.2
-------------------------------------	------	------	-----	------	------	------	------	-----	------	------	-----	------	-----	------	------

2. Impacts of Risk

State Bank Group

Table 4.41 shows that most respondents agree or strongly agree that the danger of hacking affects the operation of the group's chosen banks.

Table 4. 41 Impacts of Risk of Hacking in Selected Banks of State Bank Group

Impacts	SBI					TGB					APGVB				
	SD	D	N	A	SA	SD	D	N	A	SA	SD	D	N	A	SA
Loss of data of account holders	5.0	15.0	0	30.0	50.0	2.5	12.5	2.5	47.5	35.0	0	12.5	0	62.5	25.0
Theft or tempering with customer's information	5.0	20.0	0	40.0	35.0	2.5	12.5	2.5	65.0	17.5	10.0	17.5	2.5	40.0	30.0
Infringing customer's privacy and its legal implications	7.5	7.5	2.5	47.5	35.0	0	7.5	0	62.5	30.0	0	0	7.5	52.5	40.0
Disability of significant portion of bank's internal computer system	2.5	12.5	0	57.5	27.5	2.5	5.0	0	65.0	27.5	5.0	7.5	0	45.0	42.5
Costs associate	12.5	20.0	0	40.0	27.5	2.5	7.5	2.5	55.0	32.5	5.0	15.0	10.0	52.5	17.5

d with repairing the system															
Perceived insecurity of bank's system	17.5	12.5	0	35.0	35.0	2.5	12.5	2.5	42.5	40.0	15.0	7.5	2.5	57.5	17.5

Nationalized Banks

Table 4.42 shows that most people are in agreement or highly in agreement on how the danger of hacking affects the operation of the chosen nationalized banks.

Table 4. 42 Impacts of Risk of Hacking in Selected Nationalized Banks

Impacts	UBI					BOB					PNB					CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Loss of data of account holders	0	12.5	2.5	3.5	4.5	2.5	5.0	2.5	5.5	3.5	2.5	7.5	5.0	5.5	2.5	0	7.5	0	6.0	3.2.5
Theft or tempering with customers' information	5.0	12.5	2.5	5.0	3.0	0	7.5	0	6.0	2.5	5.0	1.0	7.5	4.5	3.0	7.5	2.0	0	4.5	3.0
Infringing customers' privacy and its legal implications	0	5.0	0	4.5	5.5	0	5.0	7.5	5.0	3.5	0	7.5	2.5	5.5	3.5	0	7.5	0	4.5	5.0

Disability of significant portion of bank's internal computer system	25	50	0	62.5	30	25	0	0	70	27.5	75	10	75	50	25	0	10	0	65	25
Costs associated with repairing the system	25	25	0	47.5	25	0	50	75	62.5	25	50	15	10	40	30	25	10	0	57.5	30
Perceived insecurity of bank's system	75	17.5	0	45	30	0	17.5	25	50	30	50	17.5	50	40	32.5	25	12.5	0	65	20

Private Sector Banks

The effects of the hacking risk on the operations of the chosen private sector banks are acknowledged by most respondents (Table 4.43).

Table 4. 43 Impacts of Risk of Hacking in Selected Private Sector Banks

Impacts	AXIS					HDFC					ICICI				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Loss of data of account holders	0	150	0	400	450	0	150	125	250	475	25	75	0	575	325
Theft or tempering with customers' informati	25	225	0	425	325	75	100	200	425	200	0	175	25	575	225

on															
Infringing customers' privacy and its legal implications	10.0	5.0	0	47.5	37.5	0	5.0	17.5	25.0	52.5	2.5	10.0	0	47.5	40.0
Disability of significant portion of bank's internal computer system	0	0	0	80.0	20.0	0	2.5	25.0	40.0	32.5	0	7.5	0	52.5	40.0
Costs associated with repairing the system	2.5	12.5	0	47.5	37.5	2.5	2.5	22.5	35.0	37.5	0	7.5	5.0	62.5	25.0
Perceived insecurity of bank's system	10.0	15.0	2.5	32.5	40.0	5.0	7.5	22.5	27.5	37.5	2.5	20.0	5.0	37.5	35.0

Group-wise Comparison

The effects of the hacking risk on the operations of the chosen bank groups are acknowledged by most respondents (Table 4.44).

Table 4. 44 Impacts of Risk of Hacking in Selected Groups of Banks

Impacts	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Loss of data of account holders	2.5	13.3	.8	46.7	36.7	1.0	8.5	2.5	51.5	36.5	.8	12.5	4.2	40.8	41.7
Theft or tempering with customers' information	5.8	16.7	1.7	48.3	27.5	4.0	11.5	4.5	53.5	26.5	3.3	16.7	7.5	47.5	25.0
Infringing	2.	5.	3.	54	35	1.	7.	2.	45	44	4.	6.	5.	40	43

customers' privacy and its legal implications	5	0	3	.2	.0	5	0	5	.0	.0	2	7	8	.0	.3
Disability of significant portion of bank's internal computer system	3.3	8.3	0	55.8	32.5	3.5	8.0	3.0	59.0	26.5	0	3.3	8.3	57.5	30.8
Costs associated with repairing the system	6.7	14.2	4.2	49.2	25.8	3.0	16.5	5.0	48.5	27.0	1.7	7.5	9.2	48.3	33.3
Perceived insecurity of bank's system	11.7	10.8	1.7	45.0	30.8	4.0	20.0	1.5	49.0	25.5	5.8	14.2	10.0	32.5	37.5

3. Risk Management Measures

State Bank Group

Table 4.45 shows that most respondents are in favor of the actions proposed to reduce the group's banks' vulnerability to hacking.

Table 4. 45 Measures for Overcoming the Risk of Hacking in Selected Banks of State Bank Group

Measure s	SBI					TGB					APGVB				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Regular review of market place developments	2.5	7.5	2.5	40.0	47.5	0	7.5	2.5	37.5	52.5	2.5	5.0	0	57.5	35.0
Sufficient staff with information	0	12.5	0	52.5	35.0	0	7.5	2.5	45.0	45.0	2.5	0	5.0	50.0	42.5

security expertise															
Penetration testing for vulnerabilities	0	12.5	0	42.5	45.0	0	7.5	2.5	40.0	50.0	15.0	12.5	5.0	42.5	25.0
Active use of system based security management and monitoring tools	2.5	10.0	0	62.5	25.0	0	12.5	0	52.5	35.0	10.0	2.5	2.5	57.5	27.5
Surveillance to detect anomalies in usage	0	7.5	0	47.5	45.0	2.5	12.5	0	52.5	32.5	15.0	5.0	0	47.5	32.5
Strong business information security controls	2.5	17.5	0	42.5	37.5	2.5	15.0	0	52.5	30.0	2.5	12.5	10.0	42.5	32.5
Strategic approach to data security	2.5	17.5	0	40.0	40.0	7.5	10.0	2.5	42.5	37.5	12.5	15.0	0	40.0	32.5
Proper authorization of end users	5.0	7.5	0	45.0	42.5	2.5	12.5	0	60.0	25.0	12.5	7.5	10.0	45.0	25.0
Building security control best practices into the system and networks	5.0	2.5	0	50.0	42.5	10.0	15.0	0	42.5	32.5	7.5	10.0	5.0	42.5	35.0
Development of Communication Security Measures:															
Firewalls	2.5	2.5	2.5	65.0	27.5	10.0	10.0	2.5	47.5	30.0	5.0	5.0	2.5	47.5	40.0
Password management	2.5	10.0	2.5	40.0	45.0	10.0	7.5	2.5	42.5	37.5	0	7.5	17.5	37.5	37.5

Encryption techniques	2.5	10.0	2.5	52.5	32.5	2.5	17.5	2.5	50.0	27.5	5.0	12.5	10.0	32.5	40.0
Collaborating websites with other banks	10.0	20.0	2.5	27.5	40.0	2.5	15.0	0	40.0	42.5	5.0	7.5	2.5	42.5	42.5
Authentication	0	10.0	0	55.0	35.0	0	15.0	0	50.0	35.0	12.5	5.0	7.5	30.0	45.0
Personal Identification Number	5.0	10.0	0	35.0	50.0	2.5	17.5	0	47.5	32.5	5.0	10.0	7.5	40.0	37.5
Hardware basket tokens	5.0	10.0	2.5	47.5	35.0	2.5	7.5	0	60.0	30.0	10.0	7.5	2.5	37.5	42.5
Virus controls	2.5	15.0	2.5	37.5	42.5	0	10.0	0	52.5	37.5	10.0	17.5	2.5	27.5	42.5
Biometrics	5.0	10.0	5.0	35.0	45.0	2.5	7.5	0	55.0	35.0	12.5	15.0	7.5	30.0	35.0
Employees screening	10.0	7.5	2.5	20.0	60.0	0	12.5	0	47.5	40.0	15.0	12.5	5.0	32.5	35.0

Nationalized Banks

Table 4.46 shows that most people are in favor of the actions taken by the chosen nationalized banks to reduce the likelihood of hacking.

Table 4. 46 Measures for Overcoming the Risk of Hacking in Selected Nationalized Banks

Measures	UBI					BOB					PNB					CANBK				
	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A	S D	D	N	A	S A
Regular review of market place developments	2.5	5.0	0	5.0	37.5	2.5	10.0	7.5	4.5	37.5	10.0	2.5	2.5	5.5	32.5	0	7.5	0	5.0	42.5

Sufficient staff with information security expertise	2.5	7.5	2.5	6.25	2.5	10.0	2.5	7.5	6.5	15.0	5.0	7.5	7.5	5.0	3.0	2.5	1.25	0	6.0	2.5
Penetration testing for vulnerabilities	7.5	1.5	2.5	4.5	3.0	2.5	2.5	1.0	4.25	4.25	0	7.5	2.5	5.25	3.75	0	1.0	0	5.0	4.0
Active use of system based security management and monitoring tools	5.0	1.25	5.0	6.25	1.5	2.5	2.5	1.0	6.0	2.5	0	1.75	2.5	5.5	2.5	2.5	7.5	0	6.0	3.0
Surveillance to detect anomalies in usage	17.5	5.0	2.5	6.0	1.5	0	1.5	2.5	5.5	2.75	5.0	1.25	0	5.25	3.0	2.5	5.0	0	4.75	4.5
Strong business information security controls	2.5	1.25	5.0	5.5	2.5	5.0	1.25	7.5	5.0	2.5	1.5	7.5	1.0	4.0	2.75	5.0	0	0	7.0	2.5
Strategic	10.0	2.0	5.0	4.5	2.0	5.0	1.0	2.0	5.5	2.7	1.0	1.5	2.0	4.2	3.0	7.0	1.0	0	3.7	4.5

approach to data security		.0	0	.0	0		.0	5	.0	5	0	.0	5	.5	.0	5	.0		.5	.0
Proper authorization of end users	2.5	12.5	2.5	50	32.5	0	7.5	10	45	37.5	7.5	12.5	0	42.5	37.5	10	7.5	0	55	27.5
Building security control best practices into the system and networks	5.0	5.0	5.0	60	25.0	2.5	10	5.0	62.5	20.0	5.0	25.0	5.0	40	25.0	0	5.0	0	60	35.0
Development of Communication Security Measures:																				
Firewalls	2.5	2.5	5.0	62.5	27.5	2.5	15	5.0	57.5	20.0	2.5	15.0	2.5	32.5	47.5	0	7.5	0	50	42.5
Password management	5.0	10	2.5	62.5	20.0	2.5	12.5	5.0	42.5	37.5	12.5	5.0	0	35	47.5	0	17.5	0	35	47.5
Encryption techniques	2.5	17.5	2.5	45	35.0	5.0	12.5	10	42.5	30.0	5.0	7.5	10	30	47.5	7.5	12.5	0	35	45
Collaborating websites with other banks	12.5	12.5	7.5	52.5	15.0	2.5	7.5	7.5	55	27.5	2.5	5.0	5.0	45	42.5	0	5.0	0	60	35.0
Authentication	10.0	17.5	2.5	37.5	32.5	0	17.5	7.5	42.5	32.5	0	12.5	7.5	20	60	0	10	2.5	55	35.0

Personal Identification Number	7.5	10.0	50.0	50.0	27.5	2.5	15.0	7.5	42.5	32.5	0	27.5	0	22.5	50.0	0	5.0	0	50.0	45.0
Hardware basket tokens	5.0	0	2.5	67.5	25.0	7.5	17.5	10.0	42.5	22.5	5.0	10.0	2.5	30.0	52.5	7.5	10.0	2.5	57.5	22.5
Virus controls	7.5	10.0	0	55.0	27.5	7.5	12.5	5.0	50.0	25.0	2.5	10.0	5.0	27.5	50.0	0	5.0	0	62.5	32.5
Biometrics	0	15.0	7.5	57.5	20.0	2.5	25.0	5.0	47.5	20.0	5.0	5.0	12.5	32.5	4.0	7.5	5.0	0	45.0	42.5
Employees screening	17.5	2.5	0	57.5	22.5	5.0	22.5	5.0	32.5	35.0	7.5	15.0	0	30.0	47.5	5.0	10.0	0	52.5	32.5

Private Sector Banks

The steps to mitigate the danger of hacking in the chosen private sector banks have received widespread support from respondents (Table 4.47).

Table 4. 47 Measures for Overcoming the Risk of Hacking in Selected Private Sector Banks

Measure s	AXIS					HDFC					ICICI				
	S D	D	N	A	SA	S D	D	N	A	SA	SD	D	N	A	S A
Regular review of market place developments	2.5	5.0	0	35.0	57.5	2.5	2.5	12.5	35.0	47.5	0	2.5	0	45.0	52.5
Sufficient staff with information security expertise	5.0	10.0	2.5	47.5	35.0	0	12.5	17.5	40.0	30.0	0	2.5	2.5	47.5	47.5
Penetration testing	5.0	10.0	0	47.5	37.5	5.0	7.5	10.0	35.0	42.5	0	7.5	2.5	52.5	37.5

for vulnerabil ities															5
Active use of system based security management and monitoring tools	10.0	5.0	0	57.5	27.5	5.0	5.0	12.5	52.5	25.0	7.5	5.0	7.5	45.0	35.0
Surveillance to detect anomalies in usage	2.5	10.0	0	62.5	25.0	0	2.5	17.5	40.0	40.0	2.5	7.5	5.0	42.5	42.5
Strong business information security controls	12.5	7.5	0	55.0	25.0	2.5	2.5	15.0	47.5	32.5	0	7.5	7.5	47.5	37.5
Strategic approach to data security	2.5	7.5	0	62.5	27.5	0	2.5	15.0	47.5	35.0	0	7.5	2.5	52.5	37.5
Proper authorization of end users	5.0	17.5	0	50.0	27.5	0	2.5	15.0	30.0	52.5	2.5	5.0	5.0	50.0	37.5
Building security control best practices into the system and network	2.5	10.0	0	67.5	20.0	2.5	10.0	12.5	42.5	32.5	2.5	10.0	2.5	52.5	32.5
Development of Communication Security Measures:															
Firewalls	2.5	12.5	0	57.5	27.5	2.5	2.5	15.0	45.0	35.0	2.5	0	5.0	55.0	
Password management	7.5	12.5	0	50.0	30.0	7.5	5.0	20.0	37.5	30.0	0	2.5	5.0	42.5	
Encryption techniques	10.0	7.5	0	42.5	40.0	12.5	7.5	7.5	55.0	17.5	0	10.0	2.5	45.0	
Collaborating	7.5	12.5	0	37.5	42.5	7.5	7.5	15.0	42.5	27.5	2.5	15.0	7.5	32.5	

websites with other banks														
Authentication	7.5	10.0	2.5	52.5	27.5	5.0	0	12.5	50.0	32.5	2.5	12.5	2.5	42.5
Personal Identification Number (PIN)	5.0	12.5	0	45.0	37.5	2.5	7.5	5.0	52.5	32.5	0	5.0	2.5	47.5
Hardware basket tokens	7.5	5.0	2.5	50.0	35.0	0	7.5	10.0	45.0	37.5	0	15.0	7.5	47.5
Virus controls	7.5	17.5	0	35.0	40.0	0	12.5	10.0	47.5	30.0	5.0	2.5	7.5	37.5
Biometrics	10.0	10.0	2.5	45.0	32.5	7.5	2.5	7.5	47.5	35.0	0	10.0	2.5	45.0
Employees screening	12.5	0	0	50.0	37.5	10.0	7.5	10.0	35.0	37.5	0	12.5	5.0	42.5

Group-wise Comparison

The steps to mitigate the danger of hacking in the chosen categories of banks have received widespread support from respondents (Table 4.48).

Table 4. 48 Measures for Overcoming the Risk of Hacking in Selected Groups of Banks

Measures	State Bank Group					Nationalized Banks					Private Sector Banks				
	S D	D	N	A	SA	S D	D	N	A	SA	S D	D	N	A	S A
Regular review of market place developments	1.7	6.7	1.7	45.0	45.0	3.5	6.0	2.0	51.0	37.5	1.7	3.3	4.2	38.3	52.5
Sufficient staff with information	0.8	6.7	2.5	49.2	40.8	4.5	8.5	5.0	57.0	25.0	1.7	8.3	7.5	45.0	37.5

security expertise															
Penetration testing for vulnerabilities	5.0	10.8	2.5	41.7	40.0	2.0	8.0	3.5	47.5	39.0	3.3	8.3	4.2	45.0	39.2
Active use of system based security management and monitoring tools	4.2	8.3	.8	57.5	29.2	2.0	10.0	4.0	57.5	26.5	7.5	5.0	6.7	51.7	29.2
Surveillance to detect anomalies in usage	5.8	8.3	0	49.2	36.7	5.0	11.5	3.0	51.5	29.0	1.7	6.7	7.5	48.3	35.8
Strong business information security controls	2.5	15.0	3.3	45.8	33.3	5.5	11.0	5.0	51.5	27.0	5.0	5.8	7.5	50.0	31.7
Strategic approach to data security	7.5	14.2	.8	40.8	36.7	6.5	14.5	4.0	45.0	30.0	.8	5.8	5.8	54.2	33.3

y															
Proper authorization of end users	6.7	9.2	3.3	50.0	30.8	4.5	12.0	5.0	46.5	32.0	2.5	8.3	6.7	4.3	3.9.2
Building security control best practices into the system and network	7.5	9.2	1.7	45.0	36.7	5.0	12.5	3.0	53.0	26.5	2.5	10.0	5.0	5.4.2	2.8.3
Development of Communication Security Measures															
Firewalls	5.8	5.8	2.5	53.3	32.5	1.5	9.0	2.5	54.0	33.0	2.5	5.0	6.7	5.2.5	3.3.3
Password management	4.2	8.3	7.5	40.0	40.0	4.0	11.0	2.0	46.0	37.0	5.0	6.7	8.3	4.3.3	3.6.7
Encryption techniques	3.3	13.3	5.0	45.0	33.3	4.5	13.0	5.5	38.5	38.5	7.5	8.3	3.3	4.7.5	3.3.3
Collaborating websites with other banks	5.8	14.2	1.7	36.7	41.7	3.5	9.5	5.5	49.5	32.0	5.8	1.7	7.5	3.7.5	3.7.5
Authentication	4.2	10.0	2.5	45.0	38.3	3.0	14.5	4.5	37.5	40.5	5.0	7.5	5.8	4.8.3	3.3.3
Personal Identification	4.2	12.5	2.5	40.8	40.0	3.0	15.5	3.5	39.0	39.0	2.5	8.3	2.8	4.8	3.8

Number													5	3	3
Hardware basket tokens	5. 8	8.3	1. 7	48. 3	35. 8	5. 5	10. 5	4. 5	48. 0	31. 5	2. 5	9. 2	6 . 7	4 7. 5	3 4. 2
Virus controls	4. 2	14. 2	1. 7	39. 2	40. 8	3. 5	10. 0	3. 0	49. 0	34. 5	4. 2	1 0. 8	5 . 8	4 0. 0	3 9. 2
Biometri cs	6. 7	10. 8	4. 2	40. 0	38. 3	3. 0	12. 0	6. 5	44. 0	34. 5	5. 8	7. 5	4 . 2	4 5. 8	3 6. 7
Employe es screening	8. 3	10. 8	2. 5	33. 3	45. 0	8. 0	12. 0	2. 5	43. 0	34. 5	7. 5	6. 7	5 . 0	4 2. 5	3 8. 3

4.3 HYPOTHESIS TESTING

H1: There is a significant difference in the types of operational risks faced by various e-banking platforms.

Table 4. 49 Coefficient of correlation among the types of operational risks faced by various e-banking platforms.

Operational risks	E-banking platforms.	
	N	R
HR-oriented operational risks	350	.844
IT-oriented operational risks	350	.836

The results presented in Table 4.49 reveal a significant correlation between the types of operational risks faced by various e-banking platforms. Specifically, the coefficient of correlation for HR-oriented operational risks is 0.844, while the correlation for IT-oriented operational risks is 0.836. These high correlation values indicate a strong relationship between the operational risks and the e-banking platforms, suggesting that both HR and IT-oriented risks are prevalent across different platforms. This supports the hypothesis (H1) that there is a significant difference in the types of operational risks encountered by various e-banking platforms. The data highlights the importance of addressing these risks to ensure the security and efficiency of e-banking operations.

H2: There is a significant impact of demographic factors on operational risks in e-banking scenario of the selected banks

Table 4. 50 ANOVA Result of demographic factors on operational risks in e-banking scenario of the selected banks

Source	Sum of Squares	df	Mean Squares	Cal. F	Crit. F	p-value
Between-group	138.652	3	46.217	1.39	2.58	0.239
Within-group	5079.989	347	32.774			
Total	5218.642	350				

The analysis presented in Table 4.50 evaluates the impact of demographic factors on operational risks in the e-banking scenario of the selected banks using ANOVA. The results indicate that the calculated F-value (1.39) is less than the critical F-value (2.58), with a p-value of 0.239. Since the p-value is greater than the standard significance level of 0.05, the results suggest that the impact of demographic factors on operational risks is not statistically significant. Thus, the hypothesis (H2) that demographic factors have a significant impact on operational risks in the e-banking scenario of the selected banks is not supported by the data. This finding implies that demographic factors may not play a critical role in influencing operational risks within the context of e-banking in the selected banks.

H3: There is a statistically significant relationship between the measures implemented and the reduction of operational risks in e-banking within the selected banks.

Table 4. 51 ANOVA Result Comparing Respondents' Expression on Prevalence of Drug Relapse Based on Educational Attainment

Source	Sum of Squares	df	Mean Squares	Cal. F	Crit. F	p-value
Between-group	255.535	3	63.884	1.98	2.27	0.113
Within-group	4963.106	347	32.228			
Total	5218.642	350				

Table 4.51 presents the ANOVA results analyzing the relationship between the measures implemented to reduce operational risks in e-banking and the respondents'

perceptions, grouped by educational attainment. The calculated F-value (1.98) is lower than the critical F-value (2.27), with a p-value of 0.113. Since the p-value is greater than the standard significance level of 0.05, the results indicate that there is no statistically significant relationship between the measures implemented and the reduction of operational risks based on the educational attainment of the respondents. Therefore, the hypothesis (H3) that there is a statistically significant relationship between the measures implemented and the reduction of operational risks in e-banking within the selected banks is not supported by the data.

H4: There is a significant effect of operational risks in e-banking on the overall functioning of the selected banks.

Table 4. 52 Operational risks in e-banking Influencing the overall functioning of the selected banks (Chi-Square Test)

Factor	Calculated Value	Table value	D.F	Remarks
Operational risks in e-banking	13.301	12.592	6	Significant at 5% level

Table 4.52 displays the results of the Chi-Square test assessing the influence of operational risks in e-banking on the overall functioning of the selected banks. The calculated Chi-Square value is 13.301, which exceeds the table value of 12.592 at 6 degrees of freedom (D.F.). Since the calculated value is higher than the critical value at the 5% significance level, the result is statistically significant. This finding indicates that operational risks in e-banking have a significant impact on the overall functioning of the selected banks, supporting the hypothesis that such risks play a crucial role in affecting bank operations.

CHAPTER 5

CONCLUSION, RECOMMENDATIONS AND FUTURE SCOPE

5.1 CONCLUSION

Keeping strong security and operational resilience in the digital banking environment is complicated and crucial, as shown by the risk analysis of e-banking activities, which presents a multidimensional picture. The expansion of online banking has revolutionized the banking industry by making services more accessible, convenient, and efficient. The security, privacy, and accessibility of financial services are all at danger due to new threats brought about by the rapid development of digital technologies. Cyber threats, technological failures, operational vulnerabilities, and regulatory compliance issues are the main risks of online banking. To protect customers and financial institutions, these risks need to be carefully understood and managed strategically.

A major concern in the field of online banking is the prevalence of cyber threats such as phishing, malware, and ransomware. These dangers take advantage of security holes in online platforms to steal personal financial information, which might cause huge losses and damage to consumers' faith in the system. Given the complexity of these cyberattacks, it is crucial to have a multi-pronged strategy for cybersecurity that includes advanced threat detection systems, frequent security audits, and thorough user education. To successfully reduce these threats, financial institutions should update their security systems often and invest in new technology.

There is a substantial danger to e-banking operations from technological breakdowns. Customers may experience annoyance and even financial losses as a result of system outages, software defects, and hardware problems that interrupt banking services. Thorough testing, routine maintenance, and solid disaster recovery strategies are necessary to guarantee the dependability and durability of digital systems. To keep services running smoothly in the face of unforeseen technical problems, institutions should set up failover procedures and backup systems.

When it comes to managing risks in online banking, regulatory compliance is just as important. To ensure the safety of customers and the stability of the financial system,

the financial sector is governed by a tangled web of rules. A financial institution risks fines and public disapproval if it does not adhere to anti-money-laundering (AML) and know-your-customer (KYC) regulations. In order to keep their online banking operations in line with legal and ethical requirements, financial institutions must monitor the ever-changing regulatory environment. A culture of openness and responsibility must be nurtured, as must stringent compliance standards, and audits must be performed on a regular basis.

The risk environment of online banking is already complex, and operational weaknesses like human mistake and internal fraud only make things worse. Serious financial and reputational harm may result from insider threats, whether they are deliberate or not. To lessen the impact of these dangers, it is necessary to set up robust systems of internal controls and to implement training and awareness initiatives for staff members. Organizations need to lay out specific rules for dealing with confidential data and make sure their staff follow them.

A comprehensive strategy for risk management is required due to the ever-changing nature of the online banking landscape, in addition to the aforementioned particular dangers. It is imperative that banks and other financial organizations have a comprehensive risk management strategy that addresses cybercrime, technological vulnerabilities, regulatory noncompliance, and operational controls. This method requires constant vigilance in order to detect and respond to new vulnerabilities and threats. To improve their risk assessment skills and foresee any problems before they happen, institutions should use data analytics and artificial intelligence.

The effectiveness of risk management initiatives may be amplified by cooperation with other businesses and regulatory agencies. The best way to protect ourselves from cyber dangers and operational difficulties is to share knowledge about new risks and best practices. Contributing to industry forums and working groups may help shed light on important topics and pave the way for standardized risk management practices.

The larger financial ecosystem is impacted by the implications of e-banking risk assessments, which go beyond specific institutions. Because of how interdependent the financial sector is, a single risk incident at one institution might trigger a domino

effect that affects other institutions. Encouraging a robust and safe online banking environment requires a collective effort from all sectors of the business. The overall stability and dependability of the financial system may be enhanced if financial institutions take a proactive approach to risk management and prioritize it.

In order to effectively manage risks in the digital banking environment, it is crucial to conduct a thorough and ever-changing risk analysis of e-banking activities. The ever-changing landscape of cyber threats, technical obstacles, regulatory mandates, and operational weaknesses need constant watchfulness and adjustment. To keep their operations and clients secure, financial institutions should invest in cutting-edge innovation, put in place stringent security measures, and keep their internal control environment strong. The intricacies of e-banking may be overcome and digital banking operations can be made resilient and sustainable if institutions adopt a comprehensive risk management framework and encourage industry cooperation.

5.2 FINDINGS OF THE STUDY

1. Findings on the Various Types of Operational Risks in E-Banking

The study finds that operational risks in e-banking are multidimensional and technology-driven. The major types of risks identified in the selected banks include system failure risk, cybersecurity risk, data breach risk, transaction processing errors, internal fraud, external fraud, and legal and compliance risks. System downtime due to server failure, software malfunction, or network disruption emerges as one of the most frequent operational issues affecting uninterrupted service delivery. Cybersecurity threats such as phishing, malware attacks, hacking, and ransomware incidents are observed to be increasing with the expansion of digital banking platforms.

The study also finds that human error plays a significant role in operational risks. Mistakes in transaction processing, incorrect data entry, and improper handling of customer information contribute to operational inefficiencies. Additionally, risks related to third-party service providers, including payment gateways and cloud service vendors, are identified as emerging concerns in the digital banking ecosystem. Therefore, operational risks in e-banking are found to be both internal and external in nature, influenced by technological, human, and procedural vulnerabilities.

2. Findings on the Factors Responsible for Operational Risks in E-Banking

The study identifies several factors responsible for operational risks in e-banking in the selected banks. One of the primary factors is inadequate technological infrastructure, including outdated software systems and insufficient cybersecurity frameworks. Weak encryption standards, lack of multi-factor authentication, and poor network security increase vulnerability to cyber threats.

Another significant factor is insufficient employee training and lack of awareness regarding digital risk management practices. Employees who are not adequately trained in handling digital platforms and cybersecurity protocols contribute to internal operational failures. The study also finds that rapid digitalization without parallel strengthening of risk management systems creates operational gaps.

Customer behavior is also identified as a contributing factor. Limited awareness among customers about safe digital practices, such as secure password management and phishing identification, increases the likelihood of fraud and unauthorized transactions. Furthermore, inadequate internal controls, weak audit mechanisms, and ineffective monitoring systems are found to intensify operational risks. Regulatory compliance challenges and frequent changes in digital banking guidelines also add complexity to operational risk management.

3. Findings on the Impacts of Operational Risks in E-Banking on Bank Functioning

The study finds that operational risks significantly affect the functioning and performance of the selected banks. Financial losses due to fraud, compensation to customers, and recovery costs are observed as direct impacts. System failures and cyber incidents disrupt normal banking operations, leading to transaction delays and reduced service efficiency.

Operational risks also negatively influence customer trust and satisfaction. Data breaches and security lapses damage the reputation of banks and result in loss of customer confidence. The study notes that reputational damage often has long-term consequences, including reduced customer retention and slower growth in digital adoption.

Additionally, operational risks increase compliance costs and regulatory scrutiny. Banks facing repeated digital failures or fraud cases are subject to stricter oversight, penalties, and mandatory corrective actions. This diverts managerial focus and financial resources from strategic development to risk mitigation activities. Overall, operational risks are found to affect financial stability, operational continuity, customer relationships, and institutional credibility.

4. Findings on Parameters for Identification, Monitoring, and Control of Operational Risk in E-Banking

The study finds that effective identification and monitoring of operational risk require clearly defined risk assessment frameworks. The selected banks use key risk indicators (KRIs), internal audit reports, and incident reporting systems as primary tools for risk identification. Real-time transaction monitoring systems and automated fraud detection mechanisms are identified as crucial parameters in minimizing digital risks.

Periodic system audits, vulnerability assessments, and penetration testing are found to be essential monitoring mechanisms. The study highlights that segregation of duties, strong authentication protocols, and access control measures strengthen internal control systems. Business continuity planning and disaster recovery frameworks are also identified as critical parameters for ensuring operational resilience.

The study further finds that regular compliance reviews, adherence to regulatory guidelines, and establishment of dedicated risk management committees enhance the overall risk governance structure. Continuous monitoring supported by advanced analytics and artificial intelligence tools improves early detection of anomalies and suspicious activities in e-banking operations.

5. Findings on Measures for Overcoming Operational Risks in E-Banking

The study finds that strengthening cybersecurity infrastructure is the most effective measure for overcoming operational risks in e-banking. Implementation of multi-factor authentication, end-to-end encryption, biometric verification, and secure coding practices significantly reduces vulnerability to cyber threats. Regular system upgrades and investment in modern IT infrastructure are also identified as essential measures.

Employee training and awareness programs are found to play a vital role in minimizing human errors and internal fraud. Continuous skill development in cybersecurity and digital risk management enhances operational efficiency. The study also finds that customer awareness campaigns regarding safe digital banking practices reduce external fraud incidents.

Establishment of strong internal control systems, periodic audits, and independent risk assessment mechanisms strengthen operational risk management. Collaboration with regulatory authorities and adherence to digital banking standards improve compliance and risk mitigation. Furthermore, adoption of advanced technologies such as artificial intelligence, machine learning, and blockchain enhances fraud detection and operational transparency.

Overall, the study concludes that a comprehensive, technology-driven, and proactive risk management approach is essential for effectively managing and overcoming operational risks in e-banking in the selected banks.

5.3 SUGGESTION OF THE STUDY

Because it is so much easier and faster to manage and complete banking transactions online, e-banking has completely changed the banking industry. To guarantee the safety and soundness of digital financial activities, however, a variety of dangers have emerged as a result of this shift, and they must be thoroughly investigated. An in-depth risk analysis of online banking activities is the primary goal of this research, which seeks to identify potential dangers, assess current weaknesses, and provide solutions.

There has been a rise in cyber dangers with the fast adoption of online banking services. Hacking, phishing, malware, and ransomware are all forms of cybercrime that financial institutions and their clients are vulnerable to. It is critical for banks to remain ahead of cybercriminals since their strategies are always evolving. This research dives into the specifics of cyber-attacks, looking at how they target weak spots in online banking systems and what that may mean for customers and banks. To protect against these ever-changing cyber threats, the study stresses the need for strong cybersecurity solutions including intrusion detection systems, firewalls, and encryption.

Assessing operational risks is another important part of e-banking risk analysis. Technical problems and interruptions may halt or severely impact online banking operations because of how reliant on intricate IT systems they are. A bank's reputation and bottom line might take a serious hit in the event of a system failure, software error, or hardware malfunction. The difficulties of guaranteeing data integrity and keeping systems online are just two of the many operational concerns that this research explores in relation to electronic banking. Regular system maintenance, backup processes, and disaster recovery planning are some of the measures that are explored as ways to improve operational resilience.

Identity theft, account takeovers, and illegal transactions are just a few ways that fraud may emerge in online banking. The many forms of online banking fraud and the safeguards that banks may put in place to stop them are the subjects of this research. Artificial intelligence (AI) and machine learning (ML) are some of the cutting-edge technologies that are used to spot potentially fraudulent patterns and behaviors. Customers should be educated about safe online activities and the hazards of e-banking, according to the report.

An additional essential part of e-banking risk assessment is compliance with regulations. In order to safeguard client information and the integrity of financial transactions, financial institutions must follow a number of rules and guidelines. Data protection legislation, anti-money laundering rules, and cybersecurity requirements are all part of the regulatory environment for online banking that this paper investigates. It draws attention to the difficulties banks have in becoming compliant and the consequences that may result from failing to do so, including fines and legal penalties.

Beyond these considerations, the research also delves into the potential harm to reputation that may arise from security breaches or e-banking failures. Incidents like data breaches or service outages may greatly impact how the public views a financial organization. Loss of trust from customers, reduced sales, and lasting harm to a bank's brand are all consequences of reputational risk. Effective communication tactics, openness, and proactive customer interaction are some of the reputational risk management and mitigation tactics examined in this report.

The research delves further into the function of external suppliers in the context of online banking. Payment processing, information technology support, and cloud services are just a few of the many services that many banks outsource to third parties. Despite the fact that these collaborations have the potential to increase operational efficiency, they also bring forth new dangers. Data breaches and service interruptions are only two of the many hazards that third-party providers are considered in this research. It covers topics including doing comprehensive due diligence, creating explicit contractual agreements, and evaluating vendor performance as best practices for controlling third-party risk.

5.4 RECOMMENDATIONS OF THE STUDY

Several important suggestions for strengthening the safety, effectiveness, and robustness of online banking services arise from the thorough risk assessment of e-banking activities. These suggestions include a wide range of topics related to risk management, such as technological safeguards, operational controls, regulatory conformity, and cyber safety. Financial institutions may enhance their e-banking framework and reduce risks by implementing these guidelines.

1. **Enhance Cyber security Measures:** Improving their cyber defenses need to be a top priority for banks and other financial organizations. Putting money into state-of-the-art security measures like encryption, intrusion detection systems (IDS), and firewalls is a part of this strategy. Institutions should take a multi-pronged approach to security by conducting penetration tests, vulnerability assessments, and exchanging threat information on a regular basis. To keep up with ever-changing cyber dangers, it is vital to continuously evaluate and update security systems. Further, the likelihood of unwanted access may be drastically reduced by establishing robust authentication procedures like multi-factor authentication (MFA).
2. **Strengthen Technological Resilience:** Investing in dependable and scalable technology solutions may help financial organizations reduce the risk of technical disasters. Part of this process is making sure the system is well-designed, testing it extensively before release, and having a strategy in place for when things go wrong. In order to fix any software errors and hardware malfunctions, regular

maintenance and upgrades are essential. You may improve system dependability and decrease downtime by using cloud-based solutions that have failover and redundancy built in.

3. **Ensure Regulatory Compliance:** Minimizing legal and reputational risks requires being compliance with regulatory regulations. A thorough compliance structure, including audits, risk assessments, and industry standards adherence, should be established by financial institutions. To further guarantee that employees comprehend and adhere to regulatory standards, institutions should engage in compliance training programs. To prevent fines and keep operations running smoothly, it is essential to monitor regulatory developments and adjust policies as needed.
4. **Implement Strong Internal Controls:** Management of operational vulnerabilities and prevention of fraud are two areas where internal controls are crucial. The development and enforcement of transparent rules and processes for the management of sensitive information and the performance of important duties is a responsibility of financial institutions. You may help find and avoid problems by reviewing and revising these rules regularly, doing internal audits, and establishing division of roles. To encourage responsibility and watchfulness, it is also important to provide staff with continuing training on security best practices and ethical behavior.
5. **Adopt a Risk Management Framework:** One all-encompassing method for handling e-banking concerns is a holistic risk management framework that incorporates many risk areas. The four Ps of risk management—identification, assessment, mitigation, and monitoring—should be implemented by institutions. Data analytics and AI may improve risk assessment and open the door to proactive risk management. The key to resilience is keeping the risk management framework reviewed and updated on a regular basis to deal with new vulnerabilities and threats.
6. **Foster Industry Collaboration:** When financial institutions work together, they can better control the risks associated with online banking. The best way for institutions to share knowledge is to join industry organizations and forums and

take part in information-sharing efforts. There may be a more secure and resilient environment for online banking if people share their thoughts on new security risks, best practices, and safeguards. In addition to strengthening the industry as a whole, working together may speed up the process of creating standardized methods for risk management.

7. **Promote Customer Education:** Reducing the risk of cyber attacks and fraud requires educating clients about e-banking security and best practices. Customers can better safeguard their accounts, identify phishing attempts, and use secure authentication mechanisms if financial institutions make this information easily available. Customers may be empowered to take proactive actions in preserving their financial information by participating in consumer awareness programs and receiving frequent updates on security concerns.
8. **Enhance Incident Response Planning:** The key to efficiently handling and reducing the effects of security events is to have a solid incident response strategy. A well-defined process for identifying, mitigating, and recovering from security incidents should be put in place by financial institutions. As part of this process, it is important to establish clear duties and obligations, organize frequent exercises and simulations, and keep stakeholders informed at all times. Damage can be minimized, operations can be restored, and customer confidence can be maintained with a well-defined incident response strategy in place.
9. **Evaluate Emerging Technologies:** An important part of risk management is keeping up with new technology and how they could affect online banking. It is important for banks to weigh the pros and cons of emerging technology like biometric identification, block chain, and artificial intelligence. The efficacy of these technologies in improving operational efficiency and security may be evaluated via the execution of pilot projects and feasibility studies.
10. **Monitor and Adapt to Evolving Threats:** New risks and vulnerabilities appear often, altering the ever-changing risk environment of e-banking. A dynamic risk management strategy should be put in place by financial institutions. This strategy should include ongoing monitoring, evaluation, and adaptation to evolving threat landscapes. To be resilient and proactive in tackling new risks, institutions should

regularly update their risk management policies, incorporate lessons gained from accidents, and keep updated about industry trends.

In order for financial institutions to keep their digital banking services safe, efficient, and in compliance, these suggestions are meant to provide a thorough method for handling the risks connected with e-banking activities.

5.5 FUTURE SCOPE OF THE STUDY

Due to the ever-increasing complexity of digital financial systems and the ever-changing nature of technology, the future of research into e-banking risk analysis looks bright and exciting. Numerous new avenues of inquiry have great potential for advancing the state of the art in risk management, especially in light of the growing importance of online banking to the global financial system. An important step toward better risk prediction and mitigation is the use of state-of-the-art AI and ML methods. Taking a preventative stance against cybercrime, these technologies may shed light on transaction patterns more thoroughly and pinpoint possible dangers with more precision. Further research into the uses and consequences of block chain technology is necessary because of the new opportunities it presents for improving the openness and safety of online financial transactions.

A further critical factor influencing the direction of future studies will be the maturation of regulatory frameworks. It is essential to regularly evaluate compliance methods and the effects of new legislation on risk management procedures since the regulatory environment is expected to change in tandem with the evolution of e-banking. How institutions adjust to new regulations and how successful new compliance technologies are might be the subjects of future research.

More and more banks are moving toward digital-only and mobile banking models, therefore studying the specific dangers of these platforms is crucial. In order to keep services safe and dependable, it is critical to understand the vulnerabilities that affect mobile banking apps and how to fix them.

Lastly, it will always be important to study how consumer knowledge and behavior affect the security of online banking. To better educate users, future studies should look at how consumer knowledge and participation affect security measures' efficacy.

With a wide-ranging focus on technical, regulatory, and behavioral aspects, this research has a lot of room to grow and will undoubtedly contribute to the advancement of e-banking risk management.

REFERENCES

CHAPTER -1

- Ahmad, R., Noraini, R., Abu Talib, & Mohd Khan, N. A. (2013). Remodeling of Risk Management in Banking: Evidence from the Sub-Continent and Gulf. *The Journal of Risk Finance*, 14(5), 468–489.
- Akbari, P. (2012). A Study on Factors Affecting Operational Electronic Banking Risks in Iran Banking Industry. *International Journal Management Business Research: Spring*, 2(2), 123–135.
- Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology*, 4, 643–656.
- Cavusoglu, H., Cavusoglu, H., & Ragunathan, S. (2005). Economics of IT Security Management: Four Improvements to Current Security Practices. *Communications for the Association for Information Systems*, 14(4), 65–75.
- Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2018). Hacking, protection and the consequences of hacking. *Communications - Scientific Letters of the University of Zilina*, 20(2), 83–87. doi:10.26552/com.C.2018.2.83-87.
- Chapelle, A., Crama, Y., Hübner, G., & Peters, J. P. (2008). Practical methods for measuring and managing operational risk in the financial sector: A clinical study. *Journal of Banking & Finance*, 32(6), 1049–1061. doi:10.1016/j.jbankfin.2007.09.017
- Chaudhry, Sahila & Singh, S. (2012). Impact of Reforms on Asset Quality in Indian Banking. *ZENITH: International Journal of Multidisciplinary Research*, 2(1), 13-31.
- Chaudhry, Sahila (2014). Risk of Careless Attitude of Service Providers in E-banking. *KAIM Journal of Management and Research*, 7(2), 53-58.

- Chaudhry, Sahila (2015). Risk of Hacking in E-Banking: A Group-wise Study of Indian Banks. *Galaxy International Interdisciplinary Research Journal*, 3(11), 61-71.
- Ebnother, Silvan; Vanini, Paolo; Mcneil, Alexander & Antolinez-Fehr, Pierre (2003). *Modeling Operational Risk. Journal of Risk*, 5(3), 1-16. <http://ssrn.com/abstract=293179>
- Embrechts, Paul & Hofert, Marius (2011). Practices and Issues in Operational Risk Modeling under Basel II. *Lithuanian Mathematical Journal*, 51 (2), 180-193.
- Savic, A. (2008). Managing IT Related Operational Risks. *Economic Annals*, 53(176) 88–109.
- Sharifi, S., Haldar, A., & Rao, S. V. D. (2016). Relationship between Operational Risk Management, Size, and Ownership of Indian Banks. *Managerial Finance*, 42(10), 1–14. doi:10.1108/MF-05-2015-0145

CHAPTER- 2

- Barkha, Jadwani & Parkhi, Shilpa & Kiran, Karande & Barge, Prashant & Bhimavarapu, Venkata Mrudula & Rastogi, Shailesh. (2022). Rebuilding Operational Risk Management Capabilities: Lessons Learned from COVID-19. *The Journal of Asian Finance, Economics and Business*, 9(9), 249-261. 10.13106/jafeb.2022.
- Bezawada, Brahmaiah. (2022). Market Risk Management Practices of the Indian Banking Sector: An Empirical Study. *International Journal of Economics and Financial Issues*, 12(3), 68-72. 10.32479/ijefi.13160.
- Chaturvedi, Ankita & Joshi, Sakshi. (2019). E-Business and Banking Industry: -An Analysis (A Study of ICICI Bank in Rajasthan). *RESEARCH REVIEW International Journal of Multidisciplinary*, 4 (6), 666-668. DOI: 10.13140/RG.2.2.29173.81122
- Chaudhary, Mahima. (2024). Security for Online Banking and Transaction. *International Journal of Scientific Research in Engineering and Management*, 08(04), 1-5. 10.55041/IJSREM31332.
- Daryakin, A.A. & Andriashina, S.G.. (2015). Problems of Evaluation and Management of Operational Risks in Banks. *Procedia Economics and Finance*, 24 (15), 156-165. DOI: 10.1016/S2212-5671(15)00637-1.
- Eknath, Shankarrao & Mundhe, Eknath. (2007). A Critical Study of E-Banking: Their Risks and Mechanisms of Risk Management. *International Journal of Innovative Research in Science, Engineering and Technology*, 5(11), 18869-18875. DOI: 10.15680/IJRSET. 0511009.
- Frolov, Serhiy & Ivasenko, Maksym & Dykha, Mariia & Shalyhina, Iryna & Hrabar, Vladyslav & Fenyves, Veronika. (2024). Interaction between decentralized financial services and the traditional banking system: A comparative analysis. *Journal "Banks and Bank Systems"*, 19(2), 53-74. 10.21511/bbs.19(2).2024.05.

- Goyal, Sahil. (2024). E-Banking, Its Growth & Future in India. *International Journal of Scientific Research in Engineering and Management*, 8(4), 1-5. 10.55041/IJSREM32541.
- Habib, Sitwat & Masood, Haris & Mubeen, Muhammad & Baig, Umair. (2014). Operational Risk Management in Corporate and Banking Sector of Pakistan. *Information and Knowledge Management*, 4(5), 58-66. DOI: 10.2139/ssrn.2663415.
- Jankiraman, Usha (2008). Operational Risk Management in Indian Banks in the context of Basel II: A Survey of the State of Preparedness and Challenges in Developing the Framework. *Asia Pacific Journal of Finance and Banking Research*, 2 (2), 26-44.
- Krishnan, K.Santhosh & Subarayan, Ulaganathan. (2024). Non-Performing Assets of the Banking Sector During the Unprecedented Periods in India. *Royal Book Publishing*, 2, 324-329.
- Kujur, Teju & Shah, Mushtaq & Shah, Mushtaq. (2015). Electronic Banking: Impact, Risk and Security Issues. *International Journal of Engineering and Management Research*, 5(5), 207-212.
- Kumar, Abhishek. (2024). A Study on Customer Awareness on E- Banking Services At Union Bank of India, Mangalore. *International Journal of Scientific Research in Engineering and Management*, 08(04), 1-5. 10.55041/IJSREM32932.
- Laksana, Rio Dhani & Shaferi, Intan & Naznii, Humaira. (2023). The Effect of Operational Risks for Digital Banking Services at Banks. *Jurnal Manajemen Bisnis*, 14(2), 451-468. 10.18196/mb.v14i2.19302.
- M., Aravind & Nair, Vinith. (2020). Customer's operational risk towards electronic banking products and its mitigation: a covariance-based structural equation modelling approach. *International Journal of Electronic Banking*, 2(1), 38-54. 10.1504/IJEBANK.2020.105416.

- Malhotra, Pooja & Singh, Balwinder. (2010). An analysis of Internet banking offerings and its determinants in India. *Internet Research*, 20(1), 87-106. DOI: 10.1108/10662241011020851.
- Malusare, Lalita. (2024). Paperless Banking Technology: Impact and Application in India. *JAC: A Journal of Composition Theory*, 17(4), 93-111.
- Mogos, Gabriela & Jamail, Nor. (2020). Study on security risks of e-banking system. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, 21(2), 1065-1072. DOI: 10.11591/ijeecs.v21.i2.pp1065-1072
- More, Ujjval & Mancharkar, Dr. (2023). Digitization of Banking Industry in India: Review of Literature. *Journal of Indian School of Political Economy*, 35(9), 85-97.
- Odedra, Jayshree. (2024). Survey on the Usage of E-Banking Facilities Among Generation Y and Generation Z in Ahmedabad. *Journal of Advanced Research in Operational and Marketing Management*, 07(01), 11-17. 10.24321/2582.5399.202403.
- Petare, Purushottam & Mohite, Dr. Pratapsinh. (2014). AN ANALYTICAL STUDY ON INTERNET BANKING. *International Journal of Research in Management & Social Science*, 2(4), 88-93. DOI: <https://www.researchgate.net/publication/303585430>
- Rao, D. & Ghosh, Prodipta. (2008). Preparedness of Indian Banks in Managing Operational Risk. *Economic and Political Weekly*, 43(18), 47-51. DOI: 10.2307/40277665.
- S.Jayalakshmi, & R.Thangavel, Dr. (2024). Impact of Internet Banking System on Banking Environment in India. *South India Journal of Social Sciences*, 21(17), 63-72.
- Salim, Archana. (2022). E-Banking Need and Benefits in Indian Economy and Current Financial Innovations in E-banking in India. *East Asian Journal of Multidisciplinary Research*, 1(9), 1757-1770. 10.55927/eajmr.

- Shakyawar, Mragank & Shakya, Kanchan. (2024). Using Artificial Intelligence to Improve Banking Services in India: A Review and Prospects for the Future. *International Journal for Research in Applied Science and Engineering Technology*, 12(4), 728-738. 10.22214/ijraset.2024.59549.
- Sharifi, Sirus & Haldar, Arunima & Rao, S.V.D.. (2016). Relationship between Operational Risk Management, Size, and Ownership of Indian Banks. *Managerial Finance*, 42(10), 1-14. DOI 10.1108/MF-05-2015-0145.
- Shirley & Hsu, Carol & Sarker, Suprateek & Lee, Allen. (2017). Enabling Effective Operational Risk Management in a Financial Institution: An Action Research Study. *Journal of Management Information Systems*, 34(3), 727-753. DOI: <https://doi.org/10.1080/07421222.2017.1373006>
- Singh, Govind & Singh, Mr. (2023). A STUDY ON ADOPTION OF E-BANKING SERVICES IN INDIA. *Sambodhi Indological Research Journal of L.D.I.I*, 45(5), 140-148.
- Siyabi, Amira & Araithi, Sarah & Pandey, Jitendra. (2020). An investigation of risk management practices in electronic banking in Sultanate of Oman. *Journal of Student Research*, 13(3), 1-8, 10.47611/jsr.vi.914.
- Tandon, Deepak & Mehra, Yogieta & Bansal, Mansi. (2015). Risk Management Practices of Indian Banks: A Survey based Study. *Asian Journal of Research in Social Sciences and Humanities*, 5(4), 118-133. DOI: 10.5958/2249-7315.2015.00085.4
- Tiwari, Rishabh. (2024). the Implication of Electronic Banking on Indian Banking Sector. *Interantional Journal of Scientific Research in Engineering and Management*, 8(4), 1-5. 10.55041/IJSREM32707.
- Varadai, Suvarna & Navi, Bhimappa. (2024). Trends and Performance of Digital payments in India. *Manas Publisher and distributors*, 1(1), 71-85.

- Wu, Dexiang & Wu, Desheng. (2010). Performance evaluation and risk analysis of online banking service. *Kybernetes*, 39(5), 723-734. DOI: 10.1108/03684921011043215.
- Yadav, Parmeshwar & Talmale, Pallavi. (2024). e-Banking Adoption in India of the Creative Commons Attribution License (CC BY 4.0). *International Journal of Trend in Scientific Research and Development (IJTSRD)*, 7(2), 861-866.
- Yadav, Pooja & Prakash, Anshika & Kampani, Shivani. (2023). Digital Banking in India: A Literature Review. *Journal of Survey in Fisheries Sciences*, 10(01), 1368-1372. 10.53555/sfs.v10i1.2219.

BIBLIOGRAPHY

ARTICLES

- Abul Hassan. (2009). Risk management practices of Islamic banks of Brunei Darussalam. *The Journal of Risk Finance*, 10(1), 23-37.
- Acharya, V. V., & Schnabl, P. (2010). Do global banks spread global imbalances? Asset-backed commercial paper during the financial crisis of 2007–2009. *IMF Economic Review*, 58(1), 37-73.
- Ahmad Raza Bilal, Noraini Bt. Abu Talib, & Mohd Noor Azli Ali Khan. (2013). Remodeling of risk management in banking: Evidence from the sub-continent and Gulf. *The Journal of Risk Finance*, 14(5), 468-489.
- Akbari, P. (2012). A study of factors affecting operational electronic banking risks in the Iran banking industry: A case study of Kermanshah Melli Bank. *International Journal of Management and Business Research*, 2(2), 123-135.
- Al. I. cuza” Iasi. (2004). Some issues about risk management for E banking. *Electronic Journal of Information Systems Evaluation*, 9(2), 73-82.
- AlHaliq, H. A., & AlMuhirat, A. A. (2016). Customer satisfaction with electronic banking services in the Saudi banking sector. *Asian Social Science*, 12(5), 139-146.
- Almagtome, A., Shaker, A., Al-Fatlawi, Q., & Bekheet, H. (2019). The integration between financial sustainability and accountability in higher education institutions: An exploratory case study. *International Journal of Innovation, Creativity and Change*, 8(2), 202-221.
- Alsudairi, M. A. T. (2012). E-service quality strategy: Achieving customer satisfaction in online banking. *Journal of Theoretical and Applied Information Technology*, 38(1), 6-24.
- Alter, S. (2002). The work system method for understanding information systems and information systems research. *Communications of the Association for Information Systems*, 9(1), 6-10.

- Al-Wattar, Y. M. A., Almagtome, A. H., & ALShafeay, K. M. (2019). The role of integrating hotel sustainability reporting practices into an accounting information system to enhance hotel financial performance: Evidence from Iraq. *African Journal of Hospitality, Tourism and Leisure*, 8(5), 1-16.
- Amato-McCoy, D. (2005). Creating virtual value. *Bank Systems and Technology*, 1(22), 9-15.
- Anghelache, C., Anghelache, G. V., Anghel, M. G., & Nita, G. (2016). General notions on banking risks. *Romanian Statistical Review Supplement*, 64(5), 7-10.
- Anghelache, G.-V., Cozmanca, B.-O., Handoreanu, C.-A., Obreja, C., Olteanu, A.-C., & Radu, A. N. (2011). Operational risk – An assessment at international level. *International Journal of Mathematical Models and Methods in Applied Sciences*, 1(5), 184-192.
- Angur, M. G., Rajan, N., & Jahera, J. S., Jr. (1999). Service quality in the banking industry: An assessment in a developing economy. *International Journal of Bank Marketing*, 17(3), 116-125.
- Anthony, R. (2004). User friendly e-banking: A survey of online e-banking retail initiatives. *Communications of the ACM*, 47(10), 99-102.
- Bamoriya Singh, P. S. (2012). Study on adoption of e-banking in India. *Integral Review - A Journal of Management*, 5(1), 1-7.
- Bauer, H. H., Hammerschmidt, M., & Falk, T. (2005). Measuring the quality of e-banking portals. *International Journal of Bank Marketing*, 23(2), 153-175.
- Bitner, M. J. (1990). Evaluating service encounters: The effects of physical surroundings and employee responses. *The Journal of Marketing*, 54(2), 69-82.
- Bolton, R. N., & Drew, J. H. (1991). A multistage model of customers' assessments of service quality and value. *Journal of Consumer Research*, 17(4), 375-384.
- Brown, S. W., & Swartz, T. A. (1989). A gap analysis of professional service quality. *The Journal of Marketing*, 53(4), 92-98.

- Calisir, F., & Gumussoy, C. A. (2008). Internet banking versus other banking channels: Young consumers' view. *International Journal of Information Management*, 28(3), 215-221.
- Chen, Y. K., Shen, C. H., Kao, L., & Yeh, C. Y. (2018). Bank liquidity risk and performance. *Review of Pacific Basin Financial Markets and Policies (RPBFMP)*, 21(01), 1-40.
- Chou, D. C., & Chou, A. Y. (2000). A guide to the Internet revolution in banking. *Information Systems Management*, 17(2), 51-57.
- Choudhary, V., & Chauhan, V. (2015). Internet banking: Challenges and opportunities in the Indian context. *Apeejay-Journal of Management Sciences and Technology*, 2(3), 29-40.
- Culp, C. L., & Neves, A. M. (2017). Shadow banking, risk transfer, and financial stability. *Journal of Applied Corporate Finance*, 29(4), 45-64.
- Daniel, E. (1999). Provision of electronic banking in the UK and the Republic of Ireland. *International Journal of Bank Marketing*, 17(2), 72-83.
- DeYoung, R. (2005). The performance of Internet-based business models: Evidence from the banking industry. *Journal of Business*, 78(3), 893-947.
- Eknath, S. (2016). Critical study of e-banking: Their risks and mechanisms of risk management. *International Journal of Innovative Research in Science, Engineering and Technology*, 5(11), 38-49. ISSN Online: 2319-8753.
- El Arif, F. Z., & Hinti, S. (2014). Methods of quantifying operational risk in banks: Theoretical approaches. *American Journal of Engineering Research (AJER)*, 3(3), 238-244. e-ISSN: 2320-0847, p-ISSN: 2320-0936
- González, M. E., Quesada, G., Picado, F., & Eckelman, C. A. (2004). Customer satisfaction using QFD: An e-banking case. *Managing Service Quality: An International Journal*, 14(4), 317-330.
- Goyal, A. K., & Agrawal, S. (2010). Risk management in Indian banks: Some emerging issues. *International Economic Journal Research*, 1(1), 102-109.

- Goyal, V. M., & Gania, G. (2012). Customer perception towards Internet banking with reference to private and foreign banks in India. *International Journal of Computing & Business Research*, 6(5), 631-637, ISSN 2229-6166.
- Grabner-Kräuter, S., & Faullant, R. (2008). Consumer acceptance of internet banking: The influence of internet trust. *International Journal of Bank Marketing*, 26(7), 483-504.
- Gupta, K. K., & Bansal, I. (2012). Development of an instrument to measure internet banking service quality in India. *Researchers World*, 20(1), 185-207.
- Guriting, P., & Ndubisi, N. O. (2006). Borneo online banking: Evaluating customer perceptions and behavioral intention. *Management Research News*, 29(1/2), 6-15.
- Hair, J. F., Sarstedt, M., Matthews, L. M., & Ringle, C. M. (2016). Identifying and treating unobserved heterogeneity with FIMIX-PLS: Part I–method. *European Business Review*, 28(1), 63-76.
- Hamlet, C. (2000). Community banks go online. *ABA Banking Journal*, 92(3), 61-67.
- Ho, S. H., & Ko, Y. Y. (2008). Effects of self-service technology on customer value and customer readiness: The case of Internet banking. *Internet Research: Electronic Networking Applications and Policy*, 18(4), 427-446.
- Hughes, T. (2001). Market orientation and the response of UK financial services companies to changes in market conditions as a result of e-commerce. *International Journal of Bank Marketing*, 19(6), 222-232.
- Hussein, A. (2014). An investigation of risk management practices in electronic banking: The case of the UK banks. *International Journal of Mathematical Models and Methods in Applied Sciences: Banks and Bank Systems*, 9(3), 184-192.
- Keramati, A., Ghaneei, H., & Mirmohammadi, S. M. (2016). Developing a prediction model for customer churn from electronic banking services using data mining. *Financial Innovation*, 2(1), 1-13.

- Khaghaany, M., Kbelah, S., & Almagtome, A. (2019). Value relevance of sustainability reporting under an accounting information system: Evidence from the tourism industry. *African Journal of Hospitality, Tourism and Leisure*, 8, 1-12.
- Khan, M. S., Scheule, H., & Wu, E. (2017). Funding liquidity and bank risk taking. *Journal of Banking & Finance*, 82(9), 203-216.
- Klomp, J., & De Haan, J. (2012). Banking risk and regulation: Does one size fit all? *Journal of Banking & Finance*, 36(12), 3197-3212.
- Kolodinsky, J. M., Hogarth, J. M., & Hilgert, M. A. (2004). The adoption of electronic banking technologies by U.S. consumers. *The International Journal of Bank Marketing*, 22(4), 238-259.
- Kumar, M., Sareen, M., & Barquissau, E. (2012). Relationship between types of trust and level of adoption of Internet banking. *Problems and Perspectives in Management*, 10(1), 82-92.
- Laforet, S., & Li, X. (2005). Consumers' attitudes towards online and mobile banking in China. *International Journal of Bank Marketing*, 23(5), 362-380.
- Laukkanen, P., Sinkkonen, S., & Laukkanen, T. (2008). Consumer resistance to internet banking: Postponers, opponents, and rejectors. *International Journal of Bank Marketing*, 26(6), 440-455.
- Liao, Z., & Wong, W.-K. (2008). the determinants of customer interactions with internet-enabled e-banking services. *Journal of the Operational Research Society*, 59(9), 1201-1210.
- Lichtenstein, S., & Williamson, K. (2006). Understanding consumer adoption of internet banking: An interpretive study in the Australian banking context. *Journal of Electronic Commerce Research*, 7(2), 50-66.
- Lochab, N., & Dalal, J. S. (2012). Customer perception about e-banking system in the hotel industry. *International Journal of Business and Management Research*, 2(11), 1-10.

- Mahfooz, Y., Al-Motairi, M., Ahmad, F., & Khan, A. (2013). A study of the service quality issues of internet banking in non-metro cities of India. *Journal of Advanced Management Science*, 1(1), 75-79.
- Mihalcescu, C., Ciolacu, B., Pavel, F., & Titrade, C. (2008). Risk and innovation in e-banking. *Romanian Economic and Business Review*, 3(2), 86-91.
- Miranda, F. J., Cortés, R., & Barriuso, C. (2006). Quantitative evaluation of e-banking websites: An empirical study of Spanish banks. *The Electronic Journal of Information Systems Evaluation*, 9(2), 73-82.
- Ndlovu, I. (2013). Benefits and risks of e-banking: Case of commercial banking in Zimbabwe. *International Journal of Computing and Business Research*, 2(4), 34-40.
- Pandya, H. (2014). Identifying major determinants of profitability for selected nationalized banks in India. *International Journal of Business and Administration Research Review*, 2(4), 1-8. ISSN 2347-856X.
- Prasad, K. V. N., & Ravinder, G. (2012). A Camel model analysis of nationalised banks in India. *International Journal of Trade & Commerce*, 1(1), 23-33. ISSN: 2277-5811.
- Rawashdeh, M. (2012). Information technology role in reducing e-banking services risk in Jordanian banking sector. *Journal of Computer Science*, 8(3), 374-381. ISSN 1549-3636.
- Salihu, A., & Metin, H. (2017). The impact of services, assurance, and efficiency in customer satisfaction on electronic banking services offered by the banking sector. *Journal of Internet Banking and Commerce*, 22(3), 1-12.
- Scannella, E., & Polizzi, S. (2018). Market risk disclosure in banking: An empirical analysis on four global systemically important European banks. *Journal of Banking Regulation*, 19(2), 87-100.
- Sood, R. K. (2004). Operational risk under the new Basel Accord. *IBA Bulletin*, 26(6), 21-29.

- Tanase, R. D., & Serbu, R. (2010). Operational risk and e-banking. *Bulletin of the Transilvania University of Brasov, Series V: Economic Sciences*, 3(1), 327-334.
- Trenca, I., & Neag, I. (2010). Considerations regarding operational risk management in the context of the Basel II Agreement. *The Romanian Economic Journal*, 13(36), 171-186.
- Tsintsadze, A., Glonti, V., Oniani, L., & Ghoghoberidze, T. (2019). Empirical analysis of financial and non-financial risks of the commercial bank. *European Journal of Sustainable Development*, 8(2), 101-101.
- Witowski, I. R. B., & Luca, F. A. (2016). Bank capital, risk, and performance in European banking: A case study on seven banking sectors. *Prague Economic Papers*, 25(2), 127-142.
- Zahoor, H. (2017). E-banking challenges in Pakistan: An empirical study. *Journal of Computer and Communications*, 5(2), 11-19. ISSN Online: 2327-5227, ISSN Print: 2327-5219

BOOKS

- Barberis, N., & Thaler, R. (2003). *A Survey of Behavioral Finance*. National Bureau of Economic Research.
- Cox, J. C., & Rubinstein, M. (2005). *Options Markets*. Princeton University Press.
- Crouhy, M., Galai, D., & Mark, R. (2006). *Risk Management: Concepts and Guidance*. McGraw-Hill Education.
- Crouhy, M., Galai, D., & Mark, R. (2014). *The Essentials of Risk Management*. McGraw-Hill Education.
- Gorton, G., & Winton, A. (2019). *The Risk of Financial Institutions*. University of Chicago Press.
- Graham, J. R., & Harvey, C. R. (2001). *The Theory and Practice of Corporate Finance: Evidence from the Field*. Journal of Financial Economics.

- Green, R. K., & Goh, R. (2014). *Risk Management in Financial Institutions*. Routledge.
- Khan, M. Y., & Jain, P. K. (2016). *Financial Services*. Tata McGraw-Hill Education.
- Kirkpatrick, G., & McCarthy, R. (2010). *Regulation and Risk Management in E-Banking*. Routledge.
- Mayo, H. B. (2016). *Financial Institutions Management: A Risk Management Approach*. Cengage Learning.
- Saunders, A., & Allen, L. (2010). *Credit Risk Management In and Out of the Financial Crisis: New Approaches to Value at Risk and Other Paradigms*. Wiley.

QUESTIONNAIRE

The following questionnaire is designed to gather detailed insights into the risk analysis of e-banking operations, focusing on the various types of operational risks and their impact on banking institutions. This instrument aims to assess the prevalence and severity of risks associated with e-banking, identify contributing factors, and evaluate the effectiveness of current risk management strategies. Your responses will provide valuable information for understanding the complexities of operational risks in e-banking and help in developing more robust risk mitigation strategies. The questionnaire covers a range of topics, including risk identification, monitoring practices, and the impact of these risks on overall banking performance. Your participation is crucial for a comprehensive analysis and will contribute to enhancing the security and efficiency of e-banking operations.

1. Gender

- Male
- Female

2. Experience (years)

- Less than 4
- 5-8
- More than 8

3. Qualification

- Graduate
- Postgraduate
- Professional qualification

4. Please give your opinion with regards to factors responsible for following operational risks, their impacts on the functioning of the banks and measures to

overcome these risks (please tick in the relevant box). (1=Strongly Disagree, 2=Disagree, 3=Indifferent, 4=Agree, 5=Strongly Agree)

Particulars					
(1.1) Risk of Repudiation of Customers' Transactions	1	2	3	4	5
(A) Factors					
(a) No system of customer's authentication					
(b) Use of outdated hardware and software system					
(c) Cyber threats and vulnerabilities					
(d) Non-availability of sufficient balance in customer's account					
(e) Failure of the system to provide online services					
(B) Impacts					
(a) Costs incurred in proving that no transaction took place					
(b) Loss of present and potential customers					
(c) Increase in costs associated with regeneration of customers' transactions					
(d) Potential adverse publicity in media					
(e) Significant deterioration in the quality of services					
(C) Measures					
(a) Implement security measures for customers' authentication					
(b) Introducing audit trails for transactions					
(c) Introducing more options for informing the customers about the transactions					

(d) Use of active and updated response procedures and plans					
(e) Use of most current version of content management system or publicly accessible software					
(f) Use of most current version of anti-virus and anti-malware system					
(g) Consider cyber threats and vulnerabilities as a part of operational risk					
Cronbach's Alpha Coefficient = 0.766					
(1.2) Risk of Inadequate Customers Security Practices	1	2	3	4	5
(A) Factors					
(a) Lack of reliability of information system					
(b) Lack of awareness about the compliance of security mechanism					
(c) Customers use of personal information (credit card numbers, bank account numbers) in non-secure e-transmission					
(d) Access of confidential information of customers' accounts by criminals					
(B) Impacts					
(a) Financial loss through unauthorized transactions					
(b) Potential adverse publicity about the bank					
(c) Loss of existing and potential customers					
(C) Measures					
(a) Informing the customers on the importance of safeguarding information in non-secure transactions					

(b) Incorporating security measures into products and services					
(c) Enforcing the necessary level of secrecy at each stage of data processing and prevents unauthorized disclosure					
(d) Provide direction for all future security activities within the organization					
(e) Address specific security issues that management need more detailed explanation					
(f) Building a comprehensive structure and ensuring how employees comply with the security issues					
(g) Present the management's decisions that are specific to the computing network, applications and data					
Cronbach's Alpha Coefficient = 0.771					
(1.3) Risk of Outdated Staff and Lack of Management Expertise	1	2	3	4	5
(A) Factors					
(a) Outdated recruitment, selection, placement and promotion policies					
(b) Lack of proper and timely training and development facilities					
(c) Absence of challenging opportunities to the staff for growth					
(d) Lack of abilities to implement the new technology					
(e) Lack of abilities to understand the impact of technological upgradation					
(B) Impacts					
(a) Poor implementation of new technology					

(b) Inability to provide ongoing support					
(c) Deficiencies in the system					
(d) Lack of reliability of the staff and system					
(e) Delay in customer service					
(f) Poor quality of customer service					
(g) High cost of providing service					
(C) Measures					
(a) Use of modern techniques of recruitment, selection, placement and promotion of staff and management					
(b) Developing corporate view of training and development as an ongoing process					
(c) Providing training to staff and management at planning stage					
(d) Providing training to staff and management at implementation stage					
(e) Providing training to staff and management at monitoring and control stage					
Cronbach's Alpha Coefficient = 0.800					
(1.4) Risk of Hacking	1	2	3	4	5
(A) Factors					
(a) Easy entry of hackers into the system					
(b) Breach with confidentiality of customers					
(c) Illegal obstruction of unauthorized person(s)					

(d) Introducing virus into the system					
(e) Bank's system deliberately crashed					
(f) Bank's data corrupted intentionally					
(B) Impacts					
(a) Loss of data of accountholders					
(b) Tempering with customers' information					
(c) Infringing customers' privacy and its legal implications					
(d) Disability of significant portion of internal computer system					
(e) Costs associated with repairing the system					
(f) Perceived insecurity of bank's system					
(C) Measures					
(a) Regular review of market place developments					
(b) Sufficient staff with information security expertise					
(c) Penetration testing for vulnerabilities					
(d) Active use of system based security management and monitoring tools					
(e) Surveillance to detect anomalies in usage					
(f) Strong business information security controls					
(g) Strategic approach to data security					
(h) Proper authorization of end users					
(i) Building security control best practices into the system					

(j) Development of Communication Security Measures:					
Firewalls					
Password Management					
Encryption Techniques					
Collaborating Websites					
Authentication					
Personal Identification Number					
Hardware Basket Tokens					
Virus Control					
Biometrics					
Employees Screening					
Cronbach's Alpha Coefficient = 0.885					

REPRINT OF THE CONFERENCE
CERTIFICATES & RESEARCH
PAPER



IAIR CONFERENCES

National Conference on Latest Innovations in Engineering, Science, Management and Humanities (NCLIESMH- 2024)

NCLIESMH/2024/C0524555

CERTIFICATE

This is to certify that Zehra Fatima, Research Scholar, Ph.D. in Commerce,
P.K. University, Shivpuri, M.P., India.

**presented a paper in the National Conference on Latest Innovations in Engineering, Science
Management and Humanities (NCLIESMH- 2024)**

at The Downton Hotel, Raipur, Chhattisgarh, India on 26th May 2024

Title of the Paper A study of Monitoring and control of operational

Risk in E-Banking.

K. Jaya Kumar.
Dr. K. Jaya Kumar
Session Chair



A. Usha Ruby
Dr. A. Usha Ruby
Session Chair



**National Conference on Latest Innovations in Engineering,
Science, Management and Humanities (NCLIESMH – 2024)**

26th May, 2024, Raipur, Chhattisgarh, India.

CERTIFICATE NO : NCLIESMH /2024/C0524555

A Study of Monitoring and Control of Operational Risk In E-Banking

Zehra Fatima

Research Scholar, Ph. D. in Commerce, P.K University, Shivpuri, M.P., India.

ABSTRACT

Monitoring and control of operational risk in e-banking are essential to ensure secure, reliable, and uninterrupted financial services. Since e-banking heavily depends on technology and online platforms, banks must adopt a multi-layered risk management strategy. The first step is establishing a strong internal control framework that includes regular monitoring of transactions, system audits, and fraud detection mechanisms. Real-time monitoring tools and advanced analytics help identify unusual activities, such as unauthorized logins or abnormal fund transfers, which can be flagged for immediate investigation. Cybersecurity measures like firewalls, multi-factor authentication, and encryption are also critical in controlling risks. Moreover, banks should conduct periodic stress testing and vulnerability assessments to detect system weaknesses and prepare for cyber threats. Employee training and awareness programs further reduce risks associated with human errors or insider fraud. Compliance with regulatory guidelines issued by central banks and international bodies ensures that institutions maintain industry-wide standards for operational security. Additionally, a well-structured incident response plan allows quick recovery from system failures or cyberattacks, minimizing customer inconvenience and financial loss. Continuous monitoring, combined with preventive and corrective control measures, not only reduces the likelihood of operational risks but also builds customer confidence in e-banking services.



IJAMSR CONFERENCES

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH – 2025)

ICLTSEMH / 2025 / C0125253

Certificate

This is to certify that Zehra Fatima Research scholar,

Ph.D. in Commerce, P.R. University, Shivpurri, M.P., India.

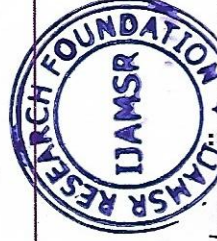
presented a paper in the International Conference on Latest Trends in Science, Engineering,
Management and Humanities (ICLTSEMH – 2025)
at Hotel Krishna Residency & Banquet, Noida, India on 19th January, 2025.

Title of the Paper Impacts of operational Risks in E-Banking.

SK Choudhary.

Dr. Sravanthi Roy Chaudhary

Session Chair



Kishan Singh Rawat

Dr. Kishan Singh Rawat

Session Chair

<https://www.ijamsr.com/conference/>



**International Conference on Latest Trends in Science, Engineering,
Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.**

CERTIFICATE NO : ICLTSEMH /2025/C0125253

Impacts of Operational Risks in E-Banking

Zehra Fatima

Research Scholar, Ph. D. in Commerce, P.K University, Shivpuri, M.P., India.

ABSTRACT

Operational risks in e-banking have significant impacts on both financial institutions and customers. These risks arise from system failures, cyber-attacks, fraud, human errors, and inadequate internal controls. One major impact is financial loss, as cybercriminals exploit weak security systems to steal money or customer data, causing huge monetary damage to banks and their clients. Another concern is reputational damage—when customers experience fraud or service disruptions, their trust in digital banking decreases, leading to customer dissatisfaction and loss of market share for the bank. Furthermore, frequent operational risks can trigger regulatory penalties if banks fail to comply with security and risk management standards. On the customer side, operational risks often result in unauthorized transactions, data breaches, or denial of service, causing stress and inconvenience. Additionally, system breakdowns or technical glitches can delay payments, disrupt business transactions, and affect the smooth flow of the economy. For banks, operational risks also increase the cost of investing in advanced security technologies and employee training. Ultimately, these risks undermine the efficiency and reliability of e-banking services, which are otherwise designed to enhance speed, convenience, and accessibility. Therefore, managing operational risks is crucial for ensuring security, customer trust, and long-term sustainability in e-banking.

**ENHANCED RESEARCH PUBLICATIONS**

RUNNING UNDER THE AEGIS OF ER EDUCATIONAL & RESEARCH SOCIETY
REGISTERED UNDER SOCIETIES REGULATION ACT, 2012

Enhancing The Impact Of Research

Thomson Researcherid Journals | UGC Approved Journals | Online & Print Journals | Refereed Journals | Peer Reviewed Journals

UGC Approved Journals. Publish Research Papers & Books with

Home / Our Journals / International Journal of Enhanc... / Volume 14, Issue 3 (March 2025)

Volume 14, Issue 3 (March 2025)

Call For Papers, IJERMCA, Vol. 14, Issue 3, March 2025, UGC Approved, International Peer Reviewed/Refereed Journal. Published papers will be indexed in Google Scholar, Thomson Reuters researcherid, Endnotes, Orcid and Various search engines worldwide like Google, Yahoo, UK Index, Europeana Libraries, Open Research, Get-cited Entire Web and many more. Fast Publications Services within 1-2 days.

Downloads :-



ASSESSING OPERATIONAL RISKS IN E-BANKING: A COMPARATIVE STUDY OF SELECTED BANKS

Zehra Fatima, Dr. Aiman Fatma

Download Now

DOI : <https://doi.org/10.55948/IJERMCA.2025.0311>



INVESTIGATING RELATIONSHIP BETWEEN COMPANY LAW AND CORPORATE GOVERNANCE IN INDIAN SCENARIO

B. Raju, Dr. Surendra Singh Baghel

Download Now

DOI : <https://doi.org/10.55948/IJERMCA.2025.0312>



INTEGRATING THEORETICAL FRAMEWORKS AND JUDICIAL APPROACHES IN CORPORATE CRIMINAL LIABILITY

Eduka Lakshmi Narasimha Reddy, Dr. Surendra Singh Baghel

Download Now

DOI : <https://doi.org/10.55948/IJERMCA.2025.0313>



EXAMINING THE AWARENESS AND IMPLEMENTATION OF HUMAN RIGHTS EDUCATION IN INDIA

Challa Suneetha, Dr. Gali Vinod Kumar

Download Now

DOI : <https://doi.org/10.55948/IJERMCA.2025.0314>



ROLE OF CYBERCRIME IN SHAPING E-COMMERCE ACCEPTANCE AND USAGE PATTERNS AMONG CONSUMERS

Amshala Shankar, Dr. Gali Vinod Kumar

Download Now

DOI : <https://doi.org/10.55948/IJERMCA.2025.0315>



KṢĀRASŪTRA IN THE MANAGEMENT OF ARŚA (HEMORRHOIDS) AND BHAGANDĀRA (FISTULA-IN-ANO)

Dr. Namrata Sharma

Download Now

DOI : <https://doi.org/10.55948/IJERMCA.2025.0316>



ER Publications

ISSN: 2319-7471, New Delhi, India

**International Journal of Enhanced Research in
Management & Computer Applications**

UGC Certified International Peer-Reviewed & Refereed Journal

UGC Journal no. 7618

Certificate of Publication

Zehra Fatima

Research Scholar, Department of Commerce, P. K. University, Shivpuri, M.P.

TITLE OF PAPER

**Assessing Operational Risks in E-Banking:
A Comparative Study of Selected Banks**

has been published in

IJERMCA, Impact Factor: 8.285, Volume 14, Issue 3, March 2025

Paper Id: MCA-3103250229

Date: 31-03-2025

Website: www.erpublishations.com

Email: erpublishations@gmail.com



Authorized Signatory



ER Publications

ISSN: 2319-7471, New Delhi, India

**International Journal of Enhanced Research in
Management & Computer Applications**

UGC Certified International Peer-Reviewed & Refereed Journal

UGC Journal no. 7618

Certificate of Publication

Dr. Aiman Fatma

Associate Professor, Department of Commerce, P. K. University, Shivpuri, M.P.

TITLE OF PAPER

**Assessing Operational Risks in E-Banking:
A Comparative Study of Selected Banks**

has been published in

IJERMCA, Impact Factor: 8.285, Volume 14, Issue 3, March 2025

Paper Id: MCA-3103250230

Date: 31-03-2025

Website: www.erpublishations.com

Email: erpublishations@gmail.com



Authorized Signatory

Assessing Operational Risks in E-Banking: A Comparative Study of Selected Banks

Zehra Fatima¹, Dr. Aiman Fatma²

¹Research Scholar, Department of Commerce, P. K. University, Shivpuri, M.P.

²Associate Professor, Department of Commerce, P. K. University, Shivpuri, M.P.

ABSTRACT

This research compares and contrasts a few banks in Hyderabad, Telangana, to look at the operational hazards of online banking. In order to gauge the perceived operational hazards of online banking services, 125 bank officials from different participating institutions were randomly selected. The study mainly aimed at banking clients who often use online banking systems and used a quantitative research approach. In order to gather information on the participants' perspectives and experiences with operational hazards, surveys and questionnaires were used. Using state-of-the-art software tools, the study included descriptive statistics, inferential statistics, and comparison methodologies to guarantee that the results were robust. The findings should help us better understand the operational risk picture in online banking, which will help banks reduce risk and provide better service. This study adds to what is already known about operational hazards in online banking and provides useful suggestions for how the digital banking industry may improve its risk management practices.

Keywords: E-Banking, People, Banks, Risk, Management.

INTRODUCTION

There has been a dramatic transition from conventional banking practices to online banking in recent years, brought about by the lightning-fast development of technology. Customers may conduct financial transactions whenever and wherever they choose using e-banking since it is convenient, efficient, and accessible. But along with technological advancements have come a plethora of operational concerns that pose a danger to the security and reliability of financial institutions. The concept of operational risk, which refers to the potential for financial loss due to insufficient or malfunctioning internal processes, people, systems, or external factors, is gaining significance in the realm of online banking. Cybersecurity breaches, system outages, fraud, and compliance problems are just some of the operational hazards that banks face due to their growing dependence on digital platforms. This research aims to compare and contrast the management and mitigation strategies used by various financial institutions in order to draw conclusions about operational risks in electronic banking. This research intends to provide light on the difficulties faced by financial institutions in today's increasingly digital world by analyzing a selection of banks in order to draw conclusions about best practices. Notably, the research's comparative nature enables an analysis of the various frameworks and tactics used by other banks, shedding light on the efficacy of their risk management approaches.

Cybersecurity is a major concern for online banking operations. Cybercriminals are increasingly focusing on financial institutions, thus it is imperative that these institutions take strong security precautions to safeguard their customers' personal information and keep their confidence. Because of the catastrophic financial losses, reputational harm, and regulatory fines that may result from such catastrophes, the significance of robust cybersecurity practices has been highlighted by recent high-profile data breaches. Through an analysis of the technology and methods used by chosen financial institutions, this research will seek to understand how these institutions have dealt with the ever-changing nature of cybersecurity threats. There are a lot of threats to e-banking operations, including cybersecurity and the possibility of system malfunctions. Service disruptions caused by technical difficulties, software errors, or infrastructure failures may result in unhappy customers and even financial losses. The study's goal is to learn how financial institutions handle their information technology (IT) infrastructure and how they prepare for the possibility of system failures affecting their online banking services. Since banks run the danger of incurring extra expenses due to their dependence on external service providers, this study will also evaluate the function of third-party vendors in online banking operations.

Another important operational risk in e-banking is fraud, since thieves are becoming smarter at finding ways to get into online banking systems. This research will examine the various methods used by participating banks to combat fraud, including as consumer education campaigns, sophisticated analytics, and machine learning. The study intends to

provide light on how banks may fortify their defenses against digital fraud by analyzing the efficacy of these measures. An further critical component of operational risk management in e-banking is compliance with regulatory standards. There is a labyrinth of rules that banks and other financial organizations must follow to safeguard customers and the economy. In order to preserve regulatory adherence and encourage innovation in their e-banking products, the research will evaluate the measures used by chosen banks in relation to compliance risk. The investigation will shed light on the fine line that banks have to walk between keeping up with regulatory requirements and adopting new technologies.

Because it is comparative, this research sheds light on the many ways that e-banking takes operational risk management. The study seeks to discover industry-wide applicable lessons and suggestions by examining the activities of chosen institutions. Further, by adding to what is already known about operational hazards in e-banking, this study hopes to pave the way for further investigation into this important area.

It is crucial to adequately manage operational risks while the e-banking industry undergoes continuous evolution. Banks need to take risk management seriously, using technology, educating employees, and strong regulations to protect their operations from possible major financial and reputational consequences. By comparing and contrasting the methods used by different banks, this research will provide light on the operational risks associated with online banking and the extent to which these risks have been adequately addressed. With this research, the study hopes to help shed light on the possibilities and threats that the banking sector faces in the digital era, with the end goal of creating a safer and more resilient online banking environment for everyone involved.

REVIEW OF LITERATURE

Iwedi, Marshal. (2024). Examining how commercial banks in Nigeria have improved their operational efficiency via the use of digital banking technologies is the focus of this article. Theories such as the Customer Experience and Efficiency Enhancement Theory, the Regulatory Compliance and Risk Management Theory, and the Technological Adoption and Operational Efficiency Theory are developed via the synthesis of current literature. Financial time series analysis is used in a quasi-experimental research strategy to provide empirical data. There is a strong correlation between commercial banks' efficiency and their use of digital banking technologies, according to the results. At the level values of all variables, panel unit root tests prove non-stationarity; differencing achieves stationarity. The adoption of digital banking technology and banking efficiency show a long-run equilibrium connection, according to cointegration tests. There seems to be a unidirectional causal relationship between operational efficiency and electronic money transfer, according to pairwise Granger causality tests. The research shows that if Nigerian authorities and stakeholders want to see commercial banks become more efficient and successful, they should focus on initiatives that encourage the use of digital banking technologies.

Mamadiyarov, Zokir. (2022). The COVID-19 epidemic is hastening the FinTech revolution because to the quick flow of information. In such a competitive market, banks can't afford to lose customers' trust unless they take steps to meet their needs, such as researching their wants and needs, developing online platforms that are easy to understand and use, and managing risks associated with providing banking services remotely. After all, banks can attract clients, boost future revenues, and save expenses by integrating current FinTech products into their systems. Along with discussing how banks are undergoing digital transformation, this article delves into the author's methods for managing risk and how they affect the current ecosystem. It also covers the various types of risks that have emerged in the electronic banking system and their traits, as well as risk management in relation to remote banking services.

Mohammed et al., (2021) The purpose of this article is to investigate how banking risk affected the Rafidain Bank's and the Baghdad Bank's online banking services. Data collection and analysis for the research were carried out using the field survey technique. Of the 43 persons selected for the sample, 25 were employees of the Rafidain Bank and 18 were employees of the Bank of Baghdad; the sample also included department leaders, aides to managers, and other individuals present at the decision-making site. The study's variables were measured using a questionnaire. Usability, advantages, and cost reduction are significantly affected by liquidity risk and credit risk, according to the findings. Since risks are the root cause of many financial crises, it is imperative that the relevant institutions implement measures to mitigate them.

Rashid, Orooba et al., (2018) The current research aims to center on the basics of bolstering electronic payment systems' internal control systems and creating specialized programs to handle operational risks, all of which contribute to the safety and security of the bank, which in turn helps the national economy grow and achieve its goals while remaining stable. The article helps illuminate the positive aspects of banking management's success as well. On a more practical level, the research paper's findings can be put to use by assisting financial institutions in implementing new control systems that enhance the efficacy and efficiency of banking supervision. This, in turn, can bolster the capacity of banking management to adapt to the ever-changing E-banking landscape, and account balance management is a boon for customers. Achieving the legal nature of electronic banking operations is the primary goal of this paper. We also aim to stay up-to-date on upcoming events and potential risks, measure and assess the risks associated with using electronic banking services, and manage these risks to a level that the bank can handle. Next, we will identify the

challenges related to the electronic banking environment by sticking to the nature of banking supervision systems, which focuses on electronic payment methods and their suitability for technological developments. Lastly, we will develop a concept for monitoring electronic banking operations within the framework of developing the performance of banking supervision units.

Santika, Ery et al., (2022) The COVID-19 outbreak has altered the routines of several Indonesian financial institutions. Virus COVID-19 has the potential to disrupt the established order of banking in Indonesia. One way to evaluate a business's financial health is to look at its profit or loss for a certain time frame. Problems with interest rate, operational, and currency rate risk management are all possible in the banking industry. Reducing the likelihood of bankruptcy and increasing banking stability may be achieved by bringing attention to the ways in which risk impacts financial performance. The purpose of this research is to identify the relationship between the dependent variable—financial success as defined by ROA and ROE—and the independent variables—investment over years, exchange rate, total operational expenditure, average asset turnover, net interest income. The goal of this research is to find out how operational risk affects the bottom line for IDX-listed banks.

RESEARCH METHODOLOGY

Sample Size

From all the participating banks in Hyderabad, Telangana, 125 bank employee are chosen at random.

Research Design

Quantitative methods were used in this study's design. People who used online banking services were the subjects of this research.

Data Collection

Quantitative methods were used in this study's design. People who used online banking services were the subjects of this research.

Data Analysis Techniques

Statistics (both descriptive and inferential), as well as comparative analysis utilizing computer programs.

DATA ANALYSIS AND INTERPRETATION

Table 1: Gender of the Respondents

Particular	Frequency	Percentage%
Male	89	71.2
Female	36	28.8
Total	125	100

Table 1 illustrates the gender distribution of the research participants. Among 125 responders, 89 were male, constituting 71.2% of the sample, whilst 36 were female, comprising 28.8%. This suggests that men constituted a markedly greater percentage of the respondents than females. The total number of responders is 125, constituting 100% of the sample population.

Table 2: Age of the Respondents

Particular	Frequency	Percentage%
18-25	30	24%
26-35	45	36%
36-45	25	20%
46 and above	25	20%
Total	125	100

Table 2 presents the age distribution of the participants. Of the 125 persons polled, the predominant age group is 26-35 years, consisting of 45 responses, or to 36% of the overall population. The second biggest demographic, aged 18-25, comprises 30 responses, accounting for 24%. The age categories 36-45 and 46 and above each include 25 respondents, representing 20% of the sample correspondingly. The table illustrates a varied age distribution, mostly including responders aged 26-35.

Table 3: Awareness of E-Banking Among Respondents

Awareness Level	Frequency	Percentage (%)
Very Aware	50	40%
Somewhat Aware	40	32%
Neutral (Neither aware nor unaware)	15	12%
Somewhat Unaware	10	8%
Very Unaware	10	8%
Total	125	100%

Table 3 depicts the awareness levels of e-banking among the participants. Among 125 persons, the predominant group, including 50 respondents (40%), indicated being "Very Aware" of e-banking services. Subsequently, 40 respondents (32%) reported being "Somewhat Aware." A minority, including 15 respondents (12%), indicated neutrality, showing neither awareness nor unawareness of e-banking. Furthermore, 10 respondents (8%) were classified as "Somewhat Unaware," while another 10 respondents (8%) were categorized as "Very Unaware." The research indicates that a majority of respondents had a certain amount of knowledge about e-banking, with 72% acknowledging awareness to some extent.

Table 4: Comparative Analysis of Operational Risks

Risk Category	Mean Score
Cybersecurity Threats	4.25
Technology Failures	4.00
Regulatory Compliance	4.05
Service Availability	4.15
Customer Data Privacy	4.25

Table 4 provides a comparative study of operational hazards according to the mean ratings supplied by the respondents. Cybersecurity Threats and Customer Data Privacy both had the highest mean score of 4.25, indicating that both risks are seen as the most critical. Service Availability gets a mean score of 4.15, whilst Regulatory Compliance scores 4.05, indicating its significance as well. Finally, Technology Failures is assessed somewhat lower, with a mean score of 4.00, however it continues to pose a considerable operational risk. The analysis indicates that all risk categories are deemed extremely significant, with cybersecurity and data privacy issues garnering the greatest focus.

Table 5: Correlation Analysis

Risk Factor	Correlation Coefficient (r)
Cybersecurity & Technology Failures	0.78
Service Availability & Customer Data Privacy	0.65

Table 5 displays the correlation analysis among several risk variables. The correlation coefficient between Cybersecurity Threats and Technology Failures is 0.78, indicating a robust positive association. This implies that an escalation in cybersecurity risks is likely to correlate with a rise in technological failures, and vice versa.

The correlation between Service Availability and Customer Data Privacy is 0.65, indicating a relatively significant positive relationship. This suggests that improved service availability is often linked to increased consumer data privacy, or that difficulties in one domain may adversely affect the other. Both correlations indicate substantial links between these operational hazards.

CONCLUSION

Operational risks in e-banking, including cybersecurity threats, system failures, fraud, and regulatory compliance issues, provide substantial hurdles for financial organizations. This research emphasizes the varied tactics used by selected institutions to manage risks via comparative analysis.

Efficient risk management is crucial for preserving the security, confidence, and stability of e-banking systems. As the digital banking ecosystem evolves, banks must stay watchful by embracing new technology and comprehensive risk management frameworks to protect their operations and assure ongoing success against rising threats.

REFERENCES

- [1]. Acharya, V. V., & Schnabl, P. (2010). Do global banks spread global imbalances? Asset-backed commercial paper during the financial crisis of 2007–09. *IMF Economic Review*, 58(1), 37-73.
- [2]. Ali, M. N., Almagtome, A. H., & Hameedi, K. S. (2019). Impact of accounting earnings quality on the going-concern in the Iraqi tourism firms. *African Journal of Hospitality, Tourism and Leisure*, 8(5), 1-12.
- [3]. Ali, M., Hameedi, K., & Almagtome, A. (2019). Does sustainability reporting via accounting information system influence the investment decisions in Iraq? *International Journal of Innovation, Creativity and Change*, 9(9), 294-312.
- [4]. Almagtome, A., & Abbas, Z. (2020). Value relevance of financial performance measures: An empirical study. *International Journal of Psychological Rehabilitation*, 24(7), 6777-6791.
- [5]. Błach, J. (2011). Financial innovations and their role in the modern financial system: Identification and systematization of the problem. *Financial Internet Quarterly - e-Finance*, 7(3), 13-26.
- [6]. Bruhn, M., & Love, I. (2014). The real impact of improved access to finance: Evidence from Mexico. *The Journal of Finance*, 69(3), 1347-1376.
- [7]. Ho, S. H., & Ko, Y. Y. (2008). Effects of self-service technology on customer value and customer readiness: The case of Internet banking. *Internet Research: Electronic Networking Applications and Policy*, 18(4), 427-446.
- [8]. Iwedi, M. (2024). Digital banking technology and the operational efficiency of banks in Nigeria. *African Banking and Finance Review Journal (ABFRJ) International Open Access Journal*, 14(14), 1-13.
- [9]. Mamadiyarov, Z. (2022). Risk management in the remote provision of banking services in the conditions of digital transformation of banks. *Journal of Computer and Communications*, 1(1), 311-317. <https://doi.org/10.1145/3508072.3508119>
- [10]. Mohammed, A.-H., Mohammed, M., & Ahmed, A. (2021). Impact of banking risks on the electronic banking services: A comparative study. *TEM Journal*, 10(2), 663-672. <https://doi.org/10.18421/TEM102-22>
- [11]. Rashid, O., Al-Badran, A., & Albadran, O. (2018). The effect of banking risks on banking financial performance: Banking modern technologies as mediating variable. *Journal of Advanced Research in Dynamical and Control Systems*, 10(10), 382-389.
- [12]. Raza, S. A., Jawaid, S. T., Hassan, A., & Burton, B. (2015). Internet banking and customer satisfaction in Pakistan. *Qualitative Research in Financial Markets*, 7(1), 24-36.
- [13]. Santika, E., Fakhruhozy, M., Nur, W., & Lestari, H. (2022). Effect of operational risk on financial performance in the banking industry IDX. *Jurnal Ekonomi*, 27(1), 123-137. <https://doi.org/10.24912/je.v27i1.915>
- [14]. Yiu, C. S., Grant, K., & Edgar, D. (2007). Factors affecting the adoption of Internet banking in Hong Kong: Implications for the banking sector. *International Journal of Information Management*, 27(5), 336-351.
- [15]. Yousafzai, S. (2012). A literature review of theoretical models of internet banking adoption at the individual level. *Journal of Financial Services Marketing*, 17, 215-226. <https://doi.org/10.1057/fsm.2012.19>

[Link to Read/Download](#) : [Click Here](#)**S. No:34**

Section : Research Paper
 Title : JUDICIARY'S ROLE IN RECONCILING SECURITY MEASURES AND HUMAN RIGHTS IN INDIA
 DOI : doi.org/10.39124/ijesrr.12.2/247886
 Author : Challa Suneetha and Dr. Gali Vinod Kumar
 Country : India
[Link to Read/Download](#) : [Click Here](#)

S. No:35

Section : Research Paper
 Title : EVALUATING THE IMPACT OF THE NATIONAL COMPANY LAW TRIBUNAL ON CORPORATE GOVERNANCE
 DOI : doi.org/10.39124/ijesrr.12.2/247887
 Author : B. Raju and Dr.Surendra Singh Baghel
 Country : India
[Link to Read/Download](#) : [Click Here](#)

S. No:36

Section : Research Paper
 Title : IMPACT OF INTELLECTUAL PROPERTY RIGHTS POLICIES ON DEVELOPING SEPS STANDARDS STANDARD ESSENTIAL PATENTS
 DOI : doi.org/10.39124/ijesrr.12.2/247888
 Author : M. Varalakshmi and Dr. Gali Vinod Kumar
 Country : India
[Link to Read/Download](#) : [Click Here](#)

**S. No:37**

Section : Research Paper
 Title : A STUDY EXPLORING THE PROBLEMS AND CONSEQUENCES OF CORPORATE CRIMES
 DOI : doi.org/10.39124/ijesrr.12.2/247889
 Author : Edula Lakshmi Narasimha Reddy and Dr. Surendra Singh Baghel
 Country : India
[Link to Read/Download](#) : [Click Here](#)

**S. No:38**

Section : Research Paper
 Title : INVESTIGATE PARAMETERS FOR IDENTIFICATION, MONITORING AND CONTROL OF OPERATIONAL RISK IN E-BANKING
 DOI : doi.org/10.39124/ijesrr.12.2/247890
 Author : Zehra Fatima and Dr. Aiman Fatma
 Country : India
[Link to Read/Download](#) : [Click Here](#)

**S. No:39**

Section : Research Paper
 Title : Meerut jile ke madhyamik Star ke vidyalayon mein adhyapan Rath shikshakon ka prasanta suchnak ek adhyayan
 DOI : doi.org/10.39124/ijesrr.12.2/247891
 Author : Dr Neeraj Kumar
 Country : India
[Link to Read/Download](#) : [Click Here](#)

S. No:40

Section : Research Paper
 Title : A REVIEW STUDY OF MICROFINANCE IN WOMEN'S EMPOWERMENT
 DOI : doi.org/10.39124/ijesrr.12.2/247892
 Author : Avijit Pal, Dr. Purnima Tiwari and Dr. Archana Mishra



E: ISSN 2348-6457
P:ISSN 2349-1817
Impact Factor -7.02

INTERNATIONAL JOURNAL OF EDUCATION AND SCIENCE RESEARCH REVIEW

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Published by: Advance Research Educational Society (ARES)

PAPER PUBLICATION CERTIFICATE

April-2025 Volume-12, Issue-2

Prof./Mr./Ms./Dr. Zehra Fatima for the research paper entitled:

**Investigate Parameters For Identification, Monitoring
And Control of Operational Risk In E-Banking**

IJESRR



www.ijesrr.org

Publication in IJESRR

Editor-in-Chief

E: ISSN 2348-6457
P:ISSN 2349-1817
Impact Factor -7.02

INTERNATIONAL JOURNAL OF EDUCATION AND SCIENCE RESEARCH REVIEW

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Published by: Advance Research Educational Society (ARES)

PAPER PUBLICATION CERTIFICATE

April-2025 Volume-12, Issue-2

Prof./Mr./Ms./ Dr. Aiman Fatma for the research paper entitled:

**Investigate Parameters For Identification, Monitoring
And Control of Operational Risk In E-Banking**

IJESRR



www.ijesrr.org

Publication in IJESRR

Editor-in-Chief

INVESTIGATE PARAMETERS FOR IDENTIFICATION, MONITORING AND CONTROL OF OPERATIONAL RISK IN E-BANKING

¹Zehra Fatima

¹Research Scholar, Department of Commerce, P. K. University, Shivpuri, M.P.

²Dr. Aiman Fatma

²Associate Professor, Department of Commerce, P. K. University, Shivpuri, M.P.

ABSTRACT

This study analyzes the criteria for recognizing, overseeing, and managing operational risk in e-banking, using a sample of 120 participants from the banking sector. The process involves gathering primary data via surveys and use statistical analysis to evaluate the findings. Critical operational risks are identified, and the efficacy of control methods is assessed. Recommendations for enhancing risk management in e-banking are provided based on the data analysis.

Keywords: E-Banking, Banks, Customer, Risk, Control.

I. INTRODUCTION

The rapid progression of technology has revolutionized the banking industry, resulting in the widespread use of electronic banking (e-banking) services. E-banking includes various financial services provided via electronic platforms, such as internet banking, mobile banking, and automated teller machines (ATMs). Although these advances have improved ease and accessibility for clients, they have also brought several operational concerns that may jeopardize the stability and integrity of financial institutions. Operational risk, characterized as the potential for loss due to insufficient or malfunctioning internal procedures, personnel, systems, or external occurrences, has become a significant issue for banks as they manage the intricacies of digital banking. In this environment, recognizing, overseeing, and managing operational risk in e-banking is crucial to maintain the stability of financial systems and safeguard consumer assets.

The importance of operational risk management in e-banking is highlighted by the rising incidence of cyberattacks, system failures, and compliance violations that may result in substantial financial losses and reputational harm. As banks increasingly implement digital solutions to satisfy client needs, they must also address the problems presented by rising dangers, including phishing attempts, data breaches, and technology obsolescence. A thorough framework for examining the factors that regulate the identification, monitoring, and management of operational risk in e-banking is important. This framework must adopt a comprehensive approach, including both quantitative and qualitative indicators to evaluate possible risks and execute successful mitigation actions.

The identification of operational risk parameters necessitates a comprehensive investigation of the internal and external elements that contribute to risk exposure in e-banking. This process often involves doing risk assessments, which may include evaluating technological infrastructure, third-party suppliers, staff skills,

and regulatory compliance. By thoroughly identifying possible risk factors, banks may get a greater understanding of their weaknesses and customize their risk management methods appropriately. Furthermore, the significance of technical breakthroughs, such artificial intelligence and machine learning, in improving risk detection is undeniable, since these technologies provide banks real-time insights into unusual activity that may indicate operational risk.

Upon identification of operational hazards, the subsequent stage is the continuous monitoring of these risks. Effective monitoring necessitates the formulation of key risk indicators (KRIs) that provide quantifiable standards for evaluating risk levels. These indicators may include measures pertaining to transaction volumes, system downtimes, user access patterns, and incident reports. By consistently monitoring these indicators, banks may get prompt insights into the changing risk environment and make educated choices about resource allocation and risk mitigation methods. The use of sophisticated analytics and dashboard reporting may improve the visibility of operational hazards, allowing institutions to react proactively to emerging threats.

Control measures are the last element in the operational risk management system. Banks must establish stringent controls to alleviate recognized risks and guarantee adherence to regulatory mandates. This may include formulating extensive rules and procedures, augmenting staff training initiatives, and allocating resources towards sophisticated cybersecurity safeguards. Moreover, cultivating a robust risk culture inside the firm is essential, as it promotes workers' prioritization of risk awareness and responsibility in their everyday activities. The creation of a robust governance framework, including monitoring from senior management and the board of directors, is essential for maintaining operational risk management as a strategic priority for the business.

The examination of factors for the identification, monitoring, and management of operational risk in e-banking is crucial for protecting the interests of financial institutions and their clients. As the digital banking sector evolves, banks must stay attentive to the many hazards linked to their operations. By implementing a proactive and comprehensive strategy for operational risk management, financial institutions may safeguard against possible risks while simultaneously bolstering their overall resilience in a competitive market. In examining the criteria and tactics for managing operational risk in e-banking, it is essential to acknowledge the evolving nature of the risk landscape and the need for ongoing adaptation and enhancement of risk management procedures.

II. REVIEW OF LITERATURE

Eknath, Shankarrao & Mundhe, Eknath. (2016). Thanks to recent developments in ICT, banks may now provide electronic services to customers in faraway places. Internet banking, online bill payment, electronic financial transactions, and automated teller machines (ATMs) are all parts of the evolution of electronic banking (e-Banking). Financial institutions have a lot to gain from the expansion of online banking and e-commerce, which includes the introduction of electronic money. Online banking has the potential to become the principal source for a wide range of financial services and products in the near future. By extending traditional banking operations to the digital realm over the internet, electronic banking provides customers with a wider range of financial products and services. The use of IT has rethought and re-engineered the banking industry, guaranteeing that customers will get ever-improving services in the future as a result of

innovations in both products and processes. There are great potential for organizational and economic growth with the use of IT in banking, but there are also ways for new kinds of risk to emerge. There are benefits and drawbacks to the fast growth of e-banking. The purpose of this research paper is to define e-banking and to explain its many types, as well as its advantages, disadvantages, risks, and management.

English, John et al., (2014) This research takes a look at how well-known UK banks handle online banking risk according to the guidelines set forth by the Basel Committee on Banking Supervision (BCBS). The pilot study's first four interviews focused on risk management in online banking and were conducted with employees of a well-known UK bank. Board management and oversight, security measures, and legal and reputational risk management are the three main areas that the research instrument focuses on. The instrument is a questionnaire. Ten well-known UK banks utilize the survey to see whether they follow these risk management guidelines. According to the respondents, security concerns are the main worry of customers using online banking, and the bank is working hard to address this issue. Based on our survey findings, UK banks have robust risk management systems in place to lessen the impact of potential electronic hazards and e-banking-related losses. Our research provides further evidence that the 14 BCBS risk guidelines are being followed by UK banks and that their e-banking security procedures are well-managed. We caution UK banks against falling into the same trap of complacency with online payments, corporate governance issues, and the ever-increasing number of complaints, many of which end up with the financial ombudsman, in light of the continued remarkable growth and investment in e-banking. Additionally, they need to make sure that staff members are knowledgeable about legal and reputational risk management standards and that present security systems are maintained to reduce security risks for different stakeholders.

Kostjunina, T. (2018). The research delves into the basics of developing a database to track operational banking risks. The proposed design approach lays the groundwork for an all-encompassing operational risk management system by automating the gathering of data about information security incidents inside the banking network. The system's remote functionality allows for the tracking and forecasting of various operational events inside the banking network. An outline of a CMS's structure is provided.

Mishchenko, Volodymyr et al., (2022) Efficient payment systems and the smooth functioning of electronic money issuers (EMIs) are both made more difficult by the proliferation of digital and mobile currencies, which in turn poses new risks. This research aims to investigate operational risk management as it pertains to digital and mobile money. The paper classified operational risk types and outlined how these types appear in electronic and mobile money payment systems. There is a breakdown of the losses (costs) caused by operational risk incidents into direct and indirect costs, and a set of key risk indicators has been developed to assess the operational risk components linked to electronic and mobile payment systems. Both the National Bank of Ukraine and the International Monetary Fund study how different countries employ digital and mobile currencies. The results about the seriousness of using electronic money are given, and the value of the electronic money multiplier in Ukraine is calculated. In order to make EMIs more operationally sustainable, we provide a thorough framework for organizing operational risk management in payment systems that use electronic and mobile money. Regulatory and supervisory processes that aim to make EMIs and the payment systems they manage more operationally sustainable are given a lot of attention. This article discusses issues that are relevant to the ongoing discussion about developing and emerging countries' usage of electronic and mobile money, namely how to apply balanced methods for operational risk management.

III. RESEARCH METHODOLOGY

Research Design

A descriptive study strategy is used, using both qualitative and quantitative methodologies. The research examines the operational hazards encountered by banks in their electronic banking services. Data is gathered from experts in the banking sector who are directly engaged in e-banking activities.

Sample Size and Sampling Technique

The sample comprises 120 individuals, chosen using purposive sampling. The participants include risk managers, IT experts, compliance officials, and other stakeholders engaged in e-banking operations across diverse financial organizations.

Data Collection Methods

Primary Data: A structured questionnaire was designed, focusing on key operational risks, their identification, monitoring, and control mechanisms.

Secondary Data: Literature from journals, reports, and regulatory guidelines related to e-banking operational risks were reviewed.

Data Analysis

The acquired data were examined using descriptive statistics and correlation analysis. The descriptive statistics provide a comprehensive summary of risk perceptions, while correlation and regression models facilitated the identification of correlations between risk variables and management measures.

IV. DATA ANALYSIS AND INTERPRETATION

Table 1: Gender of the respondents

Particular	Frequency	Percentage%
Male	49	39.2
Female	76	60.8
Total	125	100

Table 1 presents the gender distribution of the respondents in the study. Out of a total of 125 participants, 49 (39.2%) identified as male, while 76 (60.8%) identified as female. This indicates a higher representation of female respondents compared to male respondents in the sample.

Table 2: Types of E-Banking Operational Risk faced by Customers

Operational Risk Factor	Frequency	Percentage (%)
System Failures	85	68%
Fraud (Internal/External)	76	61%
Data Breaches	72	58%
Regulatory Non-Compliance	45	36%
Transaction Errors	58	46%
Weak Customer Authentication	69	55%
Technological Complexity	53	42%
Lack of Customer Support	61	49%
System Security Vulnerabilities	74	59%

Table 2 delineates the several categories of operational hazards associated with e-banking that clients face, along with their corresponding frequencies and percentages. The most stated risk is system breakdowns, impacting 85 respondents, or 68% of the total. Subsequently, 76 respondents (61%) identified fraud, whether internal or foreign, as a major problem. Seventy-two participants reported data breaches, constituting 58% of the total.

Additional significant hazards include inadequate consumer identification, identified by 69 respondents (55%), and transaction mistakes, impacting 58 respondents (46%). Furthermore, 61 consumers (49%) voiced apprehensions about inadequate customer service, whilst 45 participants (36%) identified issues of regulatory non-compliance. Finally, technical complexity and system security risks were identified by 53 respondents (42%) and 74 respondents (59%), respectively. These results underscore the diverse operational risks encountered by clients in e-banking, with system breakdowns and fraud being the predominant concerns.

Table 3: Descriptive Statistics of Operational Risk Factors

Risk Factor	Mean Score	Standard Deviation	Risk Level (High/Low)
System Failures	4.2	0.65	High
Fraud (Internal/External)	4.4	0.56	High
Data Breaches	4.0	0.72	High
Regulatory Non-compliance	3.6	0.88	Medium
Customer Authentication	3.9	0.67	High

Transaction Errors	3.5	0.74	Medium
--------------------	-----	------	--------

Table 3 displays the descriptive data for many operational risk indicators in e-banking, including mean scores, standard deviations, and evaluated risk levels. The risk variables are evaluated on a scale, with greater scores signifying more perceived risk.

The highest mean score, 4.4 with a standard deviation of 0.56, is assigned to fraud (internal/external), classifying it as a high-risk category. System failures constitute a considerable issue, shown by a mean score of 4.2 and a standard deviation of 0.65, indicating a substantial degree of risk. Data breaches exhibit a mean score of 4.0 and a standard deviation of 0.72, categorizing them as high risk.

Conversely, regulatory non-compliance and transaction mistakes are classified as medium risk, with average ratings of 3.6 and 3.5, respectively. The standard deviation for regulatory non-compliance is 0.88, while transaction mistakes have a standard deviation of 0.74. Customer authentication attained a mean score of 3.9 and a standard deviation of 0.67, categorizing it as high-risk. The table indicates that several operational risk categories are seen as high risks by respondents, including fraud and system breakdowns, whilst others are considered medium risk.

Table 4: Correlation Between Risk Monitoring and Control Effectiveness of Operational Risk in E-Banking.

Risk Factor	Monitoring	Control Mechanisms	Correlation Coefficient
System Failures	3.8	4.0	0.72
Fraud (Internal/External)	4.1	4.2	0.78
Data Breaches	3.7	4.1	0.69
Regulatory Non-compliance	3.5	3.6	0.64
Customer Authentication	3.6	4.0	0.71
Transaction Errors	3.4	3.8	0.65

Table 4 depicts the relationship between risk monitoring and control efficacy across several operational risk variables in e-banking, showcasing mean scores for both monitoring and control methods, as well as the correlation coefficients.

Fraud (internal/external) has the highest mean scores for both monitoring (4.1) and control methods (4.2), yielding a robust correlation value of 0.78, which indicates a substantial association between effective monitoring and control in alleviating this risk. System failures exhibit a significant association, with a monitoring score of 3.8 and a control score of 4.0, resulting in a correlation value of 0.72.

Data breaches are well monitored and regulated, with scores of 3.7 and 4.1, yielding a correlation value of 0.69. Customer authentication has an average monitoring score of 3.6 and a control score of 4.0, indicating a correlation value of 0.71.

Conversely, regulatory non-compliance has the lowest mean scores for both monitoring (3.5) and control methods (3.6), yielding a correlation value of 0.64, indicating a moderate association between monitoring and control. Transaction mistakes, with monitoring and control ratings of 3.4 and 3.8 respectively, provide a correlation value of 0.65, indicating a moderate link.

The table demonstrates a mostly positive association between risk monitoring and control efficacy across several operational risk variables in e-banking, with fraud being the most successfully monitored and managed.

V. CONCLUSION

The precise identification, monitoring, and management of operational risk in e-banking are essential for maintaining the stability and integrity of financial institutions in a progressively digital environment. As banks manage the intricacies of electronic services, they must establish strong frameworks that include risk assessment, important risk indicators, and thorough control procedures. By using new technology and cultivating a robust risk culture, financial institutions may proactively identify possible vulnerabilities and alleviate the effects of emerging risks. A comprehensive approach to operational risk management safeguards client assets and bolsters the resilience and competitiveness of banks within the growing financial ecosystem.

REFERENCES

- Ako, R. E., & Okpako, A. E. (2018). A causality learning of e-banking operational risk using tree augmented naïve Bayes classifier. *International Journal of Soft Computing and Engineering*, 8(4), 22-37.
- Barakat, A., Chernobai, A., & Wahrenburg, M. (2014). Information asymmetry around operational risk announcements. *Journal of Banking & Finance*, 48, 152-179.
- Chernobai, A., Ozdagli, A., & Wang, J. (2021). Business complexity and risk management: Evidence from operational risk events in U.S. bank holding companies. *Journal of Monetary Economics*, 117, 418-440.
- Del Gaudio, B. L., Porzio, G., Sampagnaro, G., & Verdoliva, V. (2021). How do mobile, internet and ICT discussions affect the banking industry? An empirical analysis. *European Management Journal*, 39(3), 327-332.
- Eknath, S., & Mundhe, E. (2016). A critical study of e-banking: Their risks and mechanisms of risk management. *International Journal of Innovative Research in Science, Engineering and Technology*, 5(11), 18869-18875.
- Greenacre, J., & Buckley, R. P. (2015). Using trusts to protect mobile money customers. *Singapore Journal of Legal Studies*, 4(1), 59-78.

- Haberly, D., MacDonald-Korth, D., Urban, M., & Wójcik, D. (2019). Asset management as a digital platform industry: A global financial network perspective. *Geoforum*, 106, 167-181.
- J., Abdou, H., & Adewunmi, P. (2014). An investigation of risk management practices in electronic banking: The case of the UK banks. *Banks and Bank Systems*, 9(3), 1-24.
- Kostjunina, T. (2018). Methodology for designing operational banking risks monitoring system. *Journal of Physics: Conference Series*, 1015(4), 1-10.
- Mishchenko, V., Naumenkova, S., Grytsenko, A., & Mishchenko, S. (2022). Operational risk management of using electronic and mobile money. *Banks and Bank Systems*, 17, 142-157.
- Mokhtari, K., Ren, J., Roberts, C., & Wang, J. (2011). Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals. *Journal of Hazardous Materials*, 192(2), 465-475.
- Shah, M., Pandya, A., Yadav, A., Chitalia, Y., & Row, D. T. (2014). A fuzzy logic-based food security risk level assessment. *International Journal of Emerging Technology and Advanced Engineering*, 4(12), 547-551.