Corrosion Management **ISSN: 1355-5243**
(https://corrosion-management.com/)
Volume 34, Issue 02, July– Dec 2024
SCOPUS

Study on factor responsible for operational risk in digital banking in public and private banks in Haryana

Ramender kour[1*], Dr Nayanpreet kaur[2]
[1*]Research Scholar, UCCM, Guru Kashi University
[2]Supervisor, UCCM, Guru Kashi University

ABSTRACT

Banking sector has gone through the rapid digitization, transforming financial services and delivering efficiency and convenience to the customer. While such aggregation has lowered operational costs, it has also stepped up their operational risk, particularly in the case of public and private banks. This paper studies the factors affecting operational risk associated with digital banking in the Indian State of Haryana, for both private and public sector banks. A mixed method research is used in the form of quantitative surveys, as well as qualitative interviews with banking professionals and customers. Operational risks found to be key include cyber threat, technological failure, regulatory compliance, human error, and fraud. Also, the study shows the difference in the adoption and means of managing digital banking operations between public and private sector banks. The technology integration level is high in Private Banks, but the system is overloaded and the data is prone to be breached. On the other hand, public banks face old technology, untrained workforce, and slower ability to thwart emerging threats. The findings further highlight that optimal risk management approaches and a well trained workforce, bolstered by stringent cybersecurity, play an instrumental role in fighting the operational risks. The study also strongly stresses the need for greater collaboration between public and private banks to share best practices and build a world class digital banking ecosystem. Results from this study can help policymakers as well as banking institutions to design effective risk mitigation strategies to promote the safe use of digital banking in Haryana.

1.Introduction

Over the past few years, digital banking has rapidly evolved banking process from the conventional banking ground and delivers improved convenience, efficiency, and affordability to customers. Digital banking means you can perform various financial functions on line, via mobile application, and other technological devices. But this digital transformation also brings with it a wide array of operational risks that could burden banking institutions. Cyber threats, fraud, technological failures, human errors, and failure to comply with regulatory requirements constitute these risks. Public and private sector banks are driving financial inclusion in Haryana, a state that has seen a growing economy and wide spread adoption of digital financial services. Although private sector banks typically enjoy advanced technological infrastructure and customer focused innovation, public sector banks provide critical services to rural and underserved populations. Although each sector has its own unique strengths, both sectors are susceptible to operational risks that can compromise the ability for banks to operate, data of customers, and ultimately the trust in the system.This study is conducted in order to understand the factors responsible for the operational risks in digital banking, except in the areas of public and private sector banks of Haryana. In an attempt to spot and contrast the critical risk factors influencing these banks, the research aims to find out whether it was possible for these banks to plan and control their operational risks in a highly digitizing atmosphere. In addition it examines the cross sectoral differences in technology adoption, risk management practices and customer experiences. The study analyzes these factors to provide banking professionals, policymakers, and regulators with important insights to improve the resilience and security of digital banking operations. Moreover, it highlights the need of collaboration between public and private banks to address common challenges, adopt best practices and create a secure and sustainable digital banking ecosystem in Haryana.

1.1Overview of Digital Banking

Digital banking, sometimes referred to as tech banking, means giving advanced technology to banking services so that customers can do financial transactions and access financial products on the web, mobile devices, and automated systems. What this transformation has done for the banking industry is that it has simplified, fastened, and generated accessibility services without the need for physical visits to bank branches. Fund transfers, bill payments, loan applications and investment tracking are just some of core features of digital banking you can

do anytime, anywhere. Rapidly growing technology, massive increase in the internet penetration and the wave of smartphones have driven the adoption of digital banking. Besides, the migration toward a cashless society and the rising demand for a user friendly financial solution have further sparked this trend. Digital banking industry carries its own perks but also comes with operational risks—cybersecurity threats, data breaches, technological failures in operation, etc., among which fraud is its common factor. The sophistication of cyber-attacks and reliance on interconnected systems heightens these risks, however, and exploitation of vulnerabilities could disrupt services to an extent that would slow economic activity. While public and private sector banks in regions such as Haryana have migrated to digital platforms, digital banking uptake has experienced a spike. Differences in infrastructure, training and customer reach limit adoption of the technology and risk management in various sectors, however, however, there are differences in how various sectors adopted the technology and risk management. With digital banking still in transition, it is essential for banking institutions to manage these operational risks, and build robust, secure, and inclusive systems that would sustain growth and maintain the trust of the customers.

1.2Importance of Digital Transformation in Banking

Digital transformation in banking is finally redefining how banks operate, how they engage and serve their customers. This is using resources like Artificial Intelligence, Blockchain, Cloud computing, and Data Analytics to improve efficiency and innovation as well as improve customer experience. It is not merely a technological upgrade but a fundamentally new strategy for responding to changing consumer needs, competitor pressures, and ever present regulatory environments.

Digital transformation is important because it simplifies banking processes and can lower operational costs, while increasing speed and reducing human error. In other words, real time data processing, fraud detection and predictive analytics made possible by automated processes and artificial intelligence help banks decide promptly. Additionally, digital platforms offer customers easy and convenient 24/7 access to banking services, which promotes financial inclusion, especially in remote and underserved areas.

Digital transformation lets banks equip themselves with the tools to provide personalized services, stronger customer engagement, and ultimately build customer loyalty in a competitive financial landscape. Mobile banking, digital wallets and chatbots are now share features of banking, which, along with other technological advancements, cater to tech savvy

customers and increase satisfaction. In an age of disruption – exemplified by the COVID-19 pandemic – digital transformation is vital for creating resilience. It allows banks to keep the continuity remotely and safely secure digital transactions. But for businesses to achieve a successful digital transformation, challenges like cybersecurity threats and ensuring legacy systems embrace technology, as well as upskilling employees need to be addressed. Digital transformation is integral to the backbone of modern financial systems, including banking; it is important for providing impetus for innovation, to remain competitive, and to ensure sustainable growth.

1.3Operational risk Operational risk is the possibility that a firm will lose money as a result of insufficient or faulty systems, workers, procedures, or external circumstances that make it difficult for the business to function efficiently. The Basel Committee on Banking Supervision defined operational risk as the chance of losing money due to external events or inadequate or defective internal procedures, people, or systems. **(Basel committee)**. Because of this increase, banks in the country are increasingly confronting varied forms of complicated hazards, and hence, banks play a key role in raising the need for risk management and mitigating risks connected with banking operations. operational risk is the "risk of loss resulting from inadequate or failed internal process, people, and systems, or external events." Human error, fraud, and information system failures, personnel management issues, commercial conflicts, accidents, fires, and floods are all included in this. Operational risk describes the risk and uncertainties that a bank faces when doing day to day activities. All organisational actions include some level of operational risk. Because of this, some of the first practitioners classified operational risk as every form of risk that does not fall under the purview of credit risk and market risk. This concept covers legal concerns, but ignores strategic and reputational issues. The definition of operational risk excludes risks that are not typically associated with market or credit risk. However, this definition of operational risk does not lend itself to the management of operational risk and instead encompasses a number of other risks that banks handle, such as interest rate, liquidity, and strategic risk . The Basel Committee categorises business-related risk occurrences into seven broad kinds. Internal fraud - External fraud - Employment practices and workplace safety - Clients and products - Physical asset damage - Business interruption and system failures - Execution and process management.

2.Literature Review

Anthala, H. R. (2018). Banking system of India performs an important role in the country's economy as it forms the core of financial transactions as well as the means of economic growth. The legal framework on fraud and forgery in public sector banks particularly, but not limited only to, Ambala City, Haryana, is covered in this doctoral dissertation. Specifically, it analyzes the provisions in the legislation, the regulatory initiative, and judicial responses concerning banking fraud and forgery as tools for dealing with banking related financial crimes. The research focuses on regional public sector banks and identifies their weaknesses including weaknesses in internal controls, a lack of awareness in employees and systemic weaknesses that are prone to fraud. It also discusses the responsibilities of law enforcement agencies, regulatory authorities like Reserve Bank of India (RBI) and legal procedures for dealing with these crimes. The research seeks to identify legal reforms and has recommended measures to enhance the accountability and security of public sector Banks so that Indian Banks can be strengthened in respect of integrity of the banking system.

SAGAR, K. D. (2023). This doctoral dissertation conducts a comparative study of e-banking services rendered by public sector banks and private sector banks in India, by specially taking into account technological development, service delivery, and customer satisfaction in both sectors. It studies on the adoption of digital banking technologies (Mobile banking, Internet banking and ATMs) and how they are incorporated into the operations of both public and private sector banks. The discussion compares private sector banks that are more agile, driven by innovativeness and are better equipped with the latest technology, with their lethargic counterparts who need to step out of the phase of old infrastructure, slower technology adoption and reluctance in the minds of staff to embrace the idea of change. The research evaluates customer experience of e banking service mainly through feasibility of use, security, reliability of services and comprehensive range of services. The dissertation assesses the regulatory environment and its underlying influence on the development of e banking in both sectors. Drawing comparisons, this study is able to identify best practices, as well as suggest ways to improve upon e banking services offered in Indian banks to ultimately increase customer satisfaction, create greater operational efficiency, and ultimately enhance the overall growth of e banking in the domain of Indian banks.

Masterson, A. (2016). Adaptability of internet banking in Haryana, India: Factors affecting its residents' and business adoption and usage are the issues investigated in this doctoral dissertation. This study seeks to address the barriers and enablers to integration and contribute to the better usage of internet banking services in urban and rural Haryana by studying the

level of awareness and access along with the technological readiness in Haryana. The assessment about the key aspects like role of internet infrastructure, digital literacy and government initiatives like Digital India, in influencing the acceptance rate of online banking platforms is being conducted. First, the dissertation examines security related consumer attitudes, internet banking trust, and customer support availability, all of which are critical components in shaping a positive consumer experience with internet banking. Furthermore, the research compares the rate of adoption in Haryana against other states in India so as to give a regional angle to the pace of digital banking adoption. Overall findings will help in providing ideas to extend internet banking accessibility in Haryana and its use by intending to help in the economic growth and financial inclusion in the State.

Singh, S. (2014). This work looks at the risks faced by service providers in India's e-banking sector and the challenges and vulnerabilities of banks that deliver secure and efficient digital banking services. However, as demand for electronic platforms grows, service providers must manage a gamut of risks including cybersecurity threats, data breaches, financial fraud, and system outages that have a potential to alienate and disengage customers and disrupt banking operations. The research looks at technology infrastructure, regulatory compliance and risk management strategies used by Indian banks to combat those risks. In addition, it brings out the threat posed by cybercrimes for example hacking, phishing and identity theft which is brought about by a faster digitization of financial services. The study also assesses the role of third party service providers such as payment gateways and fintech companies in enhancing or reducing these risks. Through an analysis of these challenges, the research seeks to provide insights on how risk management practices can be improved, security practices enhanced and a safer e-banking environment can be developed in India.

Chaudhry, S. (2017). The central thesis of this dissertation is that customer transactions in Indian banks carry the risk of repudiation and this dissertation examines the risk embedded in digital banking and electronic transactions. Repudiation happens when a customer protests that they did not authorize a particular transaction, resulting in frequent disputes between their bank and the customer, and instigates fears of fraud, security and the integrity of the banking systems. Factors that have resulted in repudiation of execution of transactions include inadequate transaction authentication processes, weak security protocols, and gaps in customer awareness. Moreover, it evaluates the role of regulatory frameworks particularly RBI guidelines in reducing repudiation risk. In addition, this study examines the efficiency of technological solutions, including multi factor authentication, biometric verification, and encryption in thwarting transactions dispute. Based on analysis of case studies and industry

practices over electronic banking in India, this research proposes ways in which banks can secure the legitimacy of the transactions by improving the transaction validation processes, educating their customers better and improving dispute resolution mechanisms to uphold the trust and reliability of electronic banking in India.

Lathigara, N. G. (2023). The assessment of customer satisfaction with online banking services of private sector banks in Gondal City, India is investigated. The factors considered for evaluation were: ease of use, speed, reliability, security and support provided through online banking platforms. The research learns key elements of offering a positive or negative online banking experience by analyzing customer feedback and service performance. The technological infrastructure of these private sector banks and the role of their mobile banking applications as well as availability of value added services such as online bill payments, fund transfers etc. are also studied in this thesis. In Gondal City, the research focuses on the influence of age factor, education, and income on adoption and satisfaction with online banking services. The findings highlight the strengths and weaknesses of the online banking services in the region and offer recommendations on how to enhance online banking service quality, improve user experience and customer loyalty in private sector banks.

BHATIA, H. (2021). Studying the data of e banking operations of Kotak Mahindra bank, one of the leading private banks in India is the focus of this doctoral dissertation. The study's methodology seeks to analyze the bank's e banking infrastructure (e.g mobile banking, internet banking and ATM services) to find the effectiveness of these channels meeting customer needs and business objectives. Key performance indicators (KPIs) like transaction volume, customer engagement, system uptime, and security measures are studied to quantitatively analyze the performance and reliability of digital services provided by the bank. Additionally, the research explores how Kotak Mahindra Bank plays a bridges role linking technology such as artificial intelligence, data analytics, and machine learning with its e-banking operations to improve user experience. In addition, the dissertation looks into customer feedback and their degree of satisfaction, and has also discovered where we need to improve our service delivery, accessibility and the user interface. Through an in depth analysis of the functioning of bank's digital operations, the study will also be looking into recommending on improvement of e-banking performance, strengthening security protocols and improving in the rates of customer satisfaction.

3.Factors Influencing Operational Risks in Digital Banking

Digital banking has revolutionized financial services, but it also brings significant operational risks that can impact the security, reliability, and efficiency of banking systems. Key factors influencing operational risks in digital banking include:

1. **Cybersecurity Threats**:
    - Cyberattacks, including phishing, malware, and ransomware, pose a significant risk to digital banking. These threats can lead to data breaches, financial fraud, and reputational damage.
    - Increasing sophistication in hacking methods, such as Distributed Denial of Service (DDoS) attacks, targets the availability of banking services.
2. **Technological Failures**:
    - Dependence on digital platforms means any technological malfunction, such as system outages or software glitches, can disrupt banking operations.
    - Legacy systems in many public sector banks struggle to integrate with modern technologies, increasing the risk of failure.
3. **Human Errors**:
    - Inadequate training and awareness among employees can result in mishandling of digital tools or lapses in maintaining security protocols.
    - Errors during data entry, system configurations, or customer interactions can amplify risks.
4. **Fraudulent Activities**:
    - Digital platforms are vulnerable to unauthorized access, fake accounts, and fraudulent transactions. Fraud detection systems may fail if not updated with the latest technologies.
    - Scams targeting customers, such as social engineering attacks, exacerbate operational risks.
5. **Regulatory and Compliance Challenges**:
    - Adhering to rapidly evolving regulations on data protection, anti-money laundering (AML), and cybersecurity can be challenging.

- Non-compliance may lead to penalties, operational disruptions, and loss of customer trust.

6. **Customer Behaviour and Expectations**:
    - Increasing customer demand for seamless, real-time services adds pressure on digital systems.
    - Lack of digital literacy among some customers can lead to misuse or mishandling of services, creating additional risks.
7. **Third-Party Dependencies**:
    - Reliance on third-party vendors for payment processing, cloud services, or cybersecurity solutions introduces risks related to vendor failures or breaches.

Understanding these factors is essential for developing robust operational risk management strategies and ensuring secure, efficient, and resilient digital banking systems.

4.Methodology

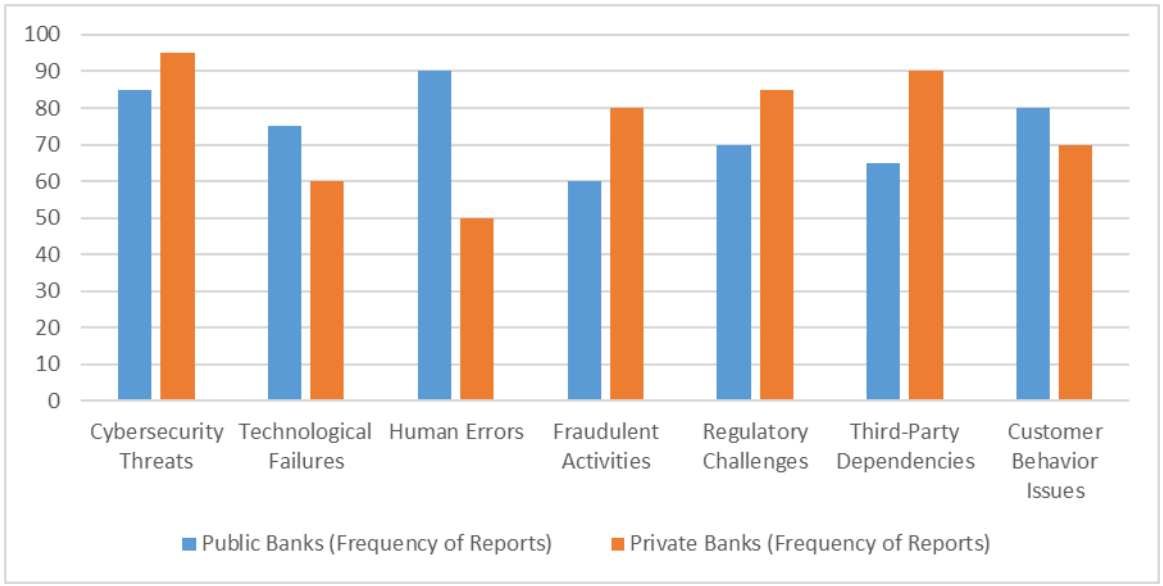
In order to understand operational risks in digital banking across public and private banks in Haryana, this study adopts a mixed methods approach. To identify the frequency and types of risks, including cybersecurity threats, technological failures, human errors, fraud and regulatory challenges, quantitative data is collected through structured surveys of 100 banking professionals (50 from each sector). Furthermore, semi structured interviews are conducted with 10–15 banking professionals to grasp the qualitative data to know more the perceptions and experiences of banking professionals with regard to risk management. Stratified random sampling provides even representation from both sectors. Descriptive and inferential statistics are used to analyze quantitative data and identify any patterns or differences between sectors, and qualitative data is analyzed via thematic analysis to discover any recurring themes and insights. Obtaining the informed consent, guaranteeing the confidentiality and seeking institutional ethical approval are ethical considerations. This methodology gives a thorough and balanced comprehension of the operational and the organization of the operations risks in the digital banking.

Corrosion Management ISSN: 1355-5243
(https://corrosion-management.com/)
Volume 34, Issue 02, July– Dec 2024
SCOPUS

Results and Discussion

Table 1 Frequency of Operational Risk Factors in Digital Banking for Public and Private Banks

Risk Factors	Public Banks (Frequency of Reports)	Private Banks (Frequency of Reports)
Cybersecurity Threats	85	95
Technological Failures	75	60
Human Errors	90	50
Fraudulent Activities	60	80
Regulatory Challenges	70	85
Third-Party Dependencies	65	90
Customer Behavior Issues	80	70



This table compares the frequency of operational risk reports presented in digital banking of public and private banks across the key variables of risk factors. Private Banks (95) report cybersecurity threats more frequently than Public Banks (85) on their higher exposure on the back of their advanced digital platforms. Public banks (75) have experienced more technological failures than private banks (60), probably because their systems are less up to date and they upgrade more slowly. Public banks (90) suffer from much higher levels of human errors as opposed to private banks (50), cases of failure training employee and digital adaptation. Private Banks are more vulnerable to fraudulent activities (80) owing to their

broad customer base and use of deep digital services. (85) The other challenge public banks face is slightly more that private banks (70), where stricter compliance requirements in a highly competitive environment applies. Private banks (90) are at higher risk of third-party dependencies than public banks (65), because they outsource services and solutions to the cloud. Concerning customer behavior, public banks (80) report more of these issues than do private banks (70). The distinct operational risks facing each sector imply that unique risk mitigation strategies are necessary, and this analysis illustrates this point.

Table 2 Effectiveness of Mitigation Strategies for Operational Risks in Digital Banking

Risk Factors	**Public Banks (Mitigation Effectiveness - %)**	**Private Banks (Mitigation Effectiveness - %)**
Cybersecurity Threats	65	75
Technological Failures	55	70
Human Errors	50	60
Fraudulent Activities	60	80
Regulatory Challenges	70	85
Third-Party Dependencies	60	75
Customer Behaviour Issues	50	65

The table shows how effective mitigation strategies are with regards to operational risks in digital banking, cross planning between public and private banks. It shows how each sector deals with most key risk factors, what percentage of its strategies are effective and how they compare to other sectors.

Compared to public banks, private banks have higher mitigation effectiveness across most risk factors owing to their more advanced technological infrastructure, proactive strategy, and more significant investment to risk management. Private banks are more effective in fighting against cybersecurity threat (75%) compared to public banks (65%) because of better cybersecurity systems and regular updates. Private banks also perform better in handling technological failures – 70 percent compared to 55 percent for public banks – owing to their use of modernized systems and shorter maintenance cycles. With respect to human errors, private banks (with 60%) are more effective especially in having structured training programs; whereas public banks (with 50%) face resource constraints. Private banks (60%) provides better addressments to fraud in compare to public banks (80%) with sophisticated fraud detection mechanisms. The ability to manage regulatory challenges is higher in private banks (85%) with automated compliance tools compared to public banks (70%). While both sectors experience difficulties managing third party dependencies, private banks (75%) are ahead of public banks (60%) in the adoption of strong vendor management protocols. Lastly, private (65%) banks are better at mitigating customer behavior issues, possibly attributed to better education of customers, than public (50%) banks.

5.Research Problem

Banking services are increasingly getting digitized, which has transformed the financial industry into offering much greater convenience and efficiency to customers. This transition to digital platforms, however, has triggered significant operational risks that may lead to disruption of services, privacy of customers' data and loss of trust. In an area where rapid adoption is occurring, all public and private banks in Haryana face differentiated challenges in managing these risks. On the other hand, public sector banks are painfully short of modern technology and resources, and their training and development capabilities are more limited than those of private sector banks, who are their own greatest enemy, coping with complicated cyber threats, system overload, and risk arising from depending on third parties. Cybersecurity threats, technological failures, human errors, fraudulent activities and an enterprise’s inability to adhere to the regulations under which it operates are all risks that occur in digital banking. In addition to posing risks for the operational stability of banks, these risks can impact customer confidence in the financial ecosystem at large. Whilst being fundamentally important to the continued presence of RRBs in the credit market, there is little research examining how both public and private Haryana banks identify, manage and mitigate

such risks. Moreover, the two sectors differ on technological adoption, risk management practices and engagement with customers. To bridge this gap, this study analyzes the factors causing operational risks in digital banking, and compares public and private banks in Haryana. The aim is to generate actionable insights regarding how to mitigate risks in effective, more secure and resilient ways that will safeguard the region's digital banking operations.

7.Conclusion

The paper studies the operational risks in digital banking in Haryana wherein the study brings out the multifaceted nature of operational risks faced by digital banking and the difference in the kind of challenges faced by public and private banks in Haryana. The problems affecting predominantly public banks include technological failures, human errors, and obsolete infrastructure that prevent them from keeping pace with the leapfrogging digital environment. On the flip side, private banks are more exposed to cybersecurity threats, fraud and dependence on third parties because the majority of their work is dependent on highly digitized systems and outsourced services. It argues that whereas public banks should pay more heed towards investments in technological enhancement and employee training to lower operational risks, private banks also have a duty to make improvements in the cybersecurity, fraud detection, and vendor management function. While both sectors struggle under regulatory pressure, the private banks have fared better due to taking on to the automated solutions proactively. Separately, issues of customer behavior that delay adoption and adoption rate in the public banks are credit to increased initiatives to develop digital literacy of the users to minimize the negative impact of such operational disruptions. The results underscore that tailored risk management approaches, collaboration between private and public banks and policy interventions are essential to address shared vulnerabilities, towards a secure and sustainable digital banking landscape. This study identifies key risk factors and sector specific strengths and drawbacks for banking professionals, policymakers and regulators to action on towards the growth of operational resilience and customer trust in the era of digital transformation.

8.Future Work

This paper also identifies major factors responsible for operational risks in digital banking of public and private banks located in Haryana as well as their challenges and ways of managing risks. Further research is warranted, though, to address the evolving nature of these risks and pursue more complete solutions. Future work could also be done in investigating the role of

new technologies, like blockchain, artificial intelligence and machine learning for alleviating operational risk in areas like fraud detection, cybersecurity and compliance.

The scope of the research is expanded to include banks from other states or areas to gain comparative insights and to develop understanding of how the regional disparity in digital banking risks could play out. Furthermore, the future work also involves a closer look at the customer perspective, to analyze the impact of customer satisfaction, trust, and engagement on operational risks and their mitigations. Another area to investigate is how fintech collaboration with third party vendors helps deal with operational risks, which are becoming increasingly important in the digital banking ecosystem. longitudinal studies could determine how mitigation strategies and operational risks change over time as digital transformation gains momentum and regulatory frameworks update their requirements to address emerging problems. Future work should also include an examination of the design and testing of advanced training programs and policy interventions to reinforce employee readiness for more resilient digital banking in different industry sectors.

Reference

1. Anthala, H. R. (2018). *Banking system in India: a legal study with special reference to fraud and forgery in public sector banks in Ambala city, Haryana* (Doctoral dissertation, PANJAB UNIVERSITY CHANDIGARH (INDIA).
2. SAGAR, K. D. (2023). *Comparative study of e-banking services by public and private sector banks of India* (Doctoral dissertation, GUJARAT TECHNOLOGICAL UNIVERSITY AHMEDABAD).
3. Masterson, A. (2016). *Adaptability of internet banking in Haryana State of India* (Doctoral dissertation, Dublin Business School).
4. Singh, S. (2014). Service providers' risk in E-banking in India. *International Journal of Management, IT and Engineering*, *4*(8), 289-301.
5. Chaudhry, S. (2017). RISK OF REPUDIATION OF CUSTOMERS'TRANSACTIONS IN INDIAN BANKS. *Asia Pacific Journal of Research in Business Management*, *8*(6).
6. Lathigara, N. G. (2023). *Measuring Customer Satisfaction With Online Banking Services: A Study Of Private Sector Banks In Gondal City* (Doctoral dissertation).
7. BHATIA, H. (2021). *TO STUDY DATA OF E-BANKING OPERATIONS AT KOTAK MAHINDRA BANK* (Doctoral dissertation, University of Mumbai).
8. Rautela, P., Sarkar, M. P., & Goel, R. (2024). Factors affecting the outsourcing activities in public and private sector banks in India. *FIIB Business Review*, *13*(4), 452-463.
9. Nayak, S., & Chandiramani, J. (2022). A crisis that changed the banking scenario in India: exploring the role of ethics in business. *Asian Journal of Business Ethics*, *11*(Suppl 1), 7-32.
10. Singh, S. (2014). Risk of counterfeiting of electronic money in e-banking. *ACADEMICIA: An International Multidisciplinary Research Journal*, *4*(9), 1-12.
11. Singh, S. (2017). Analysis of risk of fraud by employees in private sector banks. *International Journal of Research in Economics and Social Sciences (IJRESS)*, *7*(3).
12. Chaudhry, S. (2017). RISK OF OUTDATED STAFF AND LACK OF MANAGEMENT EXPERTISE IN INDIAN BANKS. *Journal on Banking Financial Services & Insurance Research*, *7*(5).

13. Chaudhry, S. (2017). Risk of frauds in Indian banks in e-banking scenario. *Asia Pacific Journal of Research in Business Management*, *8*(5).
14. Singh, D. S., & Sharma, D. K. (2014). Analysis of Problems Faced by Customers during Use of Internet Banking. *Singh, S. & Sharma, DK,(2014). Analysis of Problems faced by Customers during use of Internet banking. International Journal of*, *3600*.
15. Taneja, S., & Özen, E. (2023). To analyse the relationship between bank's green financing and environmental performance. *International Journal of Electronic Finance*, *12*(2), 163-175.
16. Shaikh, I., & Anwar, M. (2023). Digital bank transactions and performance of the Indian banking sector. *Applied Economics*, *55*(8), 839-852.
17. Bhasin, M. L. (2015). Menace of frauds in the Indian banking industry: an empirical study. *Australian Journal of Business and Management Research*, *4*(12).
18. Puri, N., & Garg, V. (2023). A sustainable banking services analysis and its effect on customer satisfaction. *Journal of Sustainable Finance & Investment*, *13*(1), 678-699.
19. Chawla, H., & Saluja, M. S. (2012). A Study on Adoption of Internet Banking Among Students in Indore. *INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT, VOLUME*, (2), 2231-1009.
20. Tondon, A. (2016). *Consumer Perception Towards Internet Banking: A Comparative study of public, Private and Foreign Banks* (Doctoral dissertation, JC Bose University).