

A Study on Evaluation of Risk Management and Security Protocols in Digital Banking Operations

P. Rekha

Assistant Professor,
Valliammal College for Women,
E-9 Anna nagar East, Chennai.

Sankara Rajeswari

III B. Com,
Valliammal College for Women,
E-9 Anna nagar East, Chennai.

T. Gnana Priya

III B. Com,
Valliammal College for Women,
E-9 Anna nagar East, Chennai.

Abstract

Banks had attracted several customers to their digital platforms in the last half of the century, even before the pandemic. However, concerns and hesitation from customers regarding risks in digital banking were obstructing this transformational journey. Digital banking products and services are now flourishing both in payment and lending domain. On one hand, we see openness to adoption, on the other hand, with increasing growth, increase in various systems and technology risk comes into play. Keeping these concerns in view, we will discuss common risk in bank's digital domain and actions taken by banks to mitigate these risks underpinning customers' confidence. Let us take you through the risk and its management practices followed by banks in digital banking procedures.

I.INTRODUCTION

Banks have been responsible for the smooth functioning of economies for decades. However, the credit crisis, global recessions, the Covid-19 pandemic, and the more recent collapse of banks in the US and Singapore in 2023 have been major setbacks for the banking sector. The pressure on risk management continues to intensify. A 2025 global survey of banking risk leaders found that 75% of banks plan to increase investment in risk technology infrastructure, reflecting rising volatility, regulatory complexity, and credit and liquidity pressures across the sector. Unless banks act immediately and prepare for these longer-term structural shifts, they may struggle to keep pace with new constraints and supervisory expectations. Banking risks in the digital space can be classified into two categories, data security risk and cyber security risk. Cyber security and data security are closely linked as both protect against information breaches. For a better understanding we can say that cyber security protects data from outside invasion. Safe banking cyberspace is protected from cyber-attacks that encompass cybercrimes and fraud. Professionals monitor the digital space to take immediate action against active threats and Advanced Persistent Threats (APT). Data security involves protecting the information provided by the customer, such as the date of birth or KYC details, from being accessed, modified or removed by unauthorized users. Security measures strengthen confidentiality and integrity through digital risk management. To understand let us see the major types of risks that banks are likely to encounter. Digital banking has made financial transactions faster and more convenient. However, increased online activity has also led to higher risks of cyber fraud. Many account holders are unaware of basic safety practices that can protect them from financial loss. This guide explains digital banking safety measures that help individuals protect their bank accounts in 2026. These steps focus on awareness, discipline, and responsible usage-essential for secure online banking.

Objectives of the study

1. To study the risk management of banking operations.
2. To know the Security Protocols in Digital Banking Operations

Research Methodology

This is a descriptive research paper based on secondary data. Data have been found out from different websites, journals, books and research papers.

Major Types of Banking Risks

Banking risks in the digital space can be classified into two categories, data security risk and cyber security risk. Cyber security and data security are closely linked as

both protect against information breaches. For a better understanding we can say that cyber security protects data from outside invasion. Safe banking cyberspace is protected from cyber-attacks that encompass cybercrimes and fraud. Professionals monitor the digital space to take immediate action against active threats and Advanced Persistent Threats (APT). Data security involves protecting the information provided by the customer, such as the date of birth or KYC details, from being accessed, modified or removed by unauthorized users. Security measures strengthen confidentiality and integrity through digital risk management. To understand let us see the major types of risks that banks are likely to encounter.

Payment Risk

Digital space payment methods like NEFT, RTGS, UPI, and Wallet payments are the popular modes of payment. The booming success of payment service providers (PSPs) has increased the risk of digital payment crimes. Weaknesses in regulations from many electronic payment platforms are a continuous concern for regulators. We take you through various digital payment modes and the risks and concerns involved with them.

- **NEFT:** National Electronic Funds Transfer (NEFT) is a centralised Reserve Bank of India (RBI) owned and operated nationwide digital payment system. This allows round-the-clock payment securely to the beneficiary. The system operates on layers of verification. Banks urge NEFT transactions through banking websites or use sites with https. Avoid banking on free networks.
- **RTGS:** Real-Time Gross Settlement is Reserve Bank of India (RBI) owned. This is a low-risk settlement of instant payment transfer dealing with high-value minimal-risk transactions.
- **UPI:** Unified Payments Interface enables peer-to-peer and person-to-merchant transactions. UPI handles, fake calls, money mule, sim cloning, and malware.
- **E-Wallets:** These are safe payment modes, but they are vulnerable to cyber theft if you lose your phone, or your phone gets stolen and does not have lock protection. These wallets do not offer insurance to users. If you are using unsecured public networks to initiate payment you invite hackers to steal your data. Download reliable digital wallets only.

Technologies that Strengthen the Risk Function

Banks need to follow innovative measures in financial analysis and forecasting to meet the demands of customer experience. Risk management in banking is closely associated with regulatory compliance that involves countless resource-intensive, error-prone document verifications. Machine learning (ML) and

Artificial Intelligence (AI) automate and largely take care of this change management system. But risk management in banking needs a central regulatory system which is why banks can use Model Risk Management (MRM) structures to bring risk factors down.

- **Uniform definition of AI/ML:** While banking needs are being gauged better with business analytics, these efficient computer systems rely on self-learning to perform tasks replacing human intelligence. Banks should work on established models defining the exact inclusions of these models for confirmed banking practices.
- **More transparency in the model:** Both AI/ML models come with risks that can emerge from materiality, uncertainty etc. By addressing and improving these grey areas, banks can take inherent risk factors better.
- **Working out new risk appetite guidelines:** ML models do not follow the traditional statements for risk appetite. They need different regulations, so peer networks combined with industry intelligence can draft fresh statements dealing with risk appetite.
- **Introducing accountability platforms:** With the increase of risk management independent platforms like compliance, Operational Risk Management (ORM), MRM, Data Management and Controls, banks need to rely on governance structures that can clearly define the roles of each for risk management in banking.
- **Internal skill enhancement:** Skill set boosting internally through external Subject Matter Experts (SME) will help banks meet and edge the approved standards of banking.
- **Testing products at all stages:** Testing products based on the technology models during their design stage, implementation stage, operational stage, and validation process and throughout their life cycle should be an essential part of digital risk management.
- **Blockchain technologies:** Banks can benefit from Blockchain technology for data management that decentralizes ledger technology. Allowing suitable coordination, it establishes better regulations in data sharing. Customer information can be stored in decentralised blocks ensuring safety from third party intrusion.

Risk Management Protocols

Banking risk management protocols are structured security measures, technical controls, and operational workflows designed to protect a financial institution's capital, customer data, and digital infrastructure from financial and

cyber threats. Modern risk management moves beyond traditional financial underwriting to address cyber, fraud, and system vulnerabilities.

Multi-Factor Authentication (MFA): Mandatory for both customer-facing applications and internal staff accessing bank infrastructure. This includes combinations of biometrics, hardware tokens, and one-time passwords (OTPs).

Data Encryption: Banks use advanced encryption standards (like AES-256) to protect data at rest (stored in servers) and data in transit (moving between bank systems, ATMs, or mobile apps).

Network Segmentation: Critical banking systems (like the core banking ledger) are isolated from general internet-facing applications to prevent a breach in one department from compromising the entire bank.

Security Operations Centres (SOC): Banks operate 24/7 monitoring centers that use AI and machine learning to analyze network traffic and instantly detect anomalies, unauthorized access attempts, or malware.

Behavioural Biometrics & AI Profiling: Systems continuously monitor how a user typically interacts with their account (e.g., standard login locations, typical transfer amounts, and device fingerprints) to flag suspicious deviations.

Sanction & AML Screening: Automated matching of account creators and transaction recipients against global anti-money laundering (AML) and counter-terrorism financing (CTF) watchlists.

Operational & Governance Protocols

A significant portion of banking risk stems from internal human error, vendor failure, or system crashes.

Third-Party Risk Management (TPRM): Before onboarding cloud service providers or software vendors, banks run exhaustive security audits, ensuring third parties match the bank's strict encryption and compliance guidelines.

VAPT (Vulnerability Assessment & Penetration Testing): Regularly hiring ethical hackers to find weaknesses in bank applications and patching those security flaws before malicious entities exploit them.

II.CONCLUSION

Digital banking comes with a wealth of facilities that are undeniably more attractive to the common consumer. When banks are focusing on customer experience, concentrating on risk management in digital banking is equally important. Banking with a dependable financial institute will help customers participate in safer banking while exploring and investing in wider opportunities. Digital banking offers speed and convenience, but it also requires consistent vigilance. By following these digital banking safety practices, individuals can better protect their accounts, personal information, and financial well-being in 2026.

Staying alert, using only authorised platforms, and reporting suspicious activity promptly are essential habits for secure online banking. Referring to official digital banking security guidelines and updates shared by Utkarsh Small Finance Bank further helps customers stay informed and adopt safe banking practices with confidence.

III. REFERENCES

1. **Pandey & Rathore (2018).** In this study the authors explored the impact of the digital payment system.
2. **Dr.Kamal Mohan Bansal-2020.** Cyber Security Issues Affecting Online Banking Transaction: A Thematic Analysis” The study shows the challenges faced by online financial platforms and any potential risks associated with them.
3. **Alghazo,J. M., Kazmi, Z., & Latif, G. (2025).** An integrated cyber security risk management framework for online banking systems. *International Journal of Information Security*. Springer. [link.springer.com]
4. **Sharma, A. (2026).** Cybersecurity risks in digital banking systems: A framework for fraud detection and prevention. *International Journal of Computer Applications*, 187(123), 42-54. h
5. **Balachandran, R., & Thomas, C. (2025).** Evaluating cybersecurity risks and measures in the banking sector. *International Journal of Research Publication and Reviews*, 6(3), 9379-9384.
6. **Murthy, K. S. V. G. K., & Kumar, G. P. (2025).** Operational risk in the digital banking era: New threats and mitigation strategies.
7. **Gulhane, P. N. (2026).** The evolution of cybersecurity: A new operational risk in the banking sector. *International Journal of Research in Finance and Management*, 9(8), 110-113.
8. **Reserve Bank of India. (2023),** Master direction on information technology governance, risk, controls and assurance practices.