IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

A Study on IT Audit Practices and Cybersecurity Measures in Banking Systems

Priyanshu Nikunj Dhanani, Sultan Asif Sayed, Prof. Chirag Deora
Students, MCA Semester IV
Guide, Department of Computer Applications
University of Mumbai, Mumbai

Abstract: *The banking industry has undergone massive digital transformation in recent years. With the rise of internet banking, mobile wallets, UPI based payments, and cloud infrastructure, financial institutions are more dependent on technology than ever, opening new doors for cyber criminals and threat actors.*

This internship report presents a detailed study on IT audit practices and cybersecurity measures in modern banking systems. The study was conducted during the internship at SecureNet InfoTech Solutions Pvt. Ltd., Mumbai, where the interns gained hands-on exposure to IT audit methodologies, vulnerability assessment procedures, compliance verification, and implementation of security controls in banking environments.

The report covers the cyber threat landscape facing banks globally and in India, reviews major frameworks (NIST CSF, ISO 27001, COBIT 2019, PCI DSS), examines RBI regulatory requirements, and discusses emerging threats such as AI-powered cyberattacks, quantum computing risks, and supply chain vulnerabilities. Based on findings from the internship, recommendations include transitioning to continuous audit models, adopting Zero Trust architectures, investing in cybersecurity talent, and planning for post-quantum cryptography...

Keywords: IT Audit, Cybersecurity, Banking Systems, NIST, ISO 27001, COBIT, RBI Guidelines, Threat Landscape, Vulnerability Assessment, Zero Trust

I. INTRODUCTION

1.1 Background and Motivation

The global banking industry has undergone tremendous change in the last two decades. From physical branch visits for basic transactions, we have reached a point where almost everything can be done from a mobile phone. Internet banking, mobile payments, UPI, cloud-based core banking platforms, and AI-driven chatbots have completely redefined how banking works today. However, this rapid digitisation has also made banks prime targets for cybercriminals and state-sponsored hackers. The IBM Cost of a Data Breach Report (2023) found that the financial services sector consistently has one of the highest average breach costs globally, with figures exceeding USD 5.9 million per incident (IBM Security, 2023). This demonstrates just how critical cybersecurity has become for the banking industry.

IT audit plays a critical role in this picture. Unlike regular financial audits, an IT audit examines technology infrastructure, security policies, access control mechanisms, data protection measures, and regulatory compliance. Our motivation for this topic came from a personal interest in cybersecurity developed during MCA coursework. The opportunity to intern at SecureNet InfoTech Solutions, a firm specialising in IT audit and cybersecurity consulting for financial institutions, provided the perfect opportunity to combine academic knowledge with practical experience. The RBI has been actively strengthening its cybersecurity guidelines through frameworks like the Cyber Security Framework for Banks (2016), the Master Direction on IT (2023), and Digital Payment Security Controls (2021).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, May 2026 Impact Factor: 8.2

1.2 Problem Statement

Despite growing awareness about cybersecurity risks, many banking institutions, especially smaller regional and cooperative banks in India, still lack mature IT audit processes and comprehensive cybersecurity frameworks. There is a considerable gap between regulatory requirements and actual practice. Attackers use increasingly sophisticated methods, from AI-powered phishing to advanced persistent threats that remain undetected for months. Annual IT audits are no longer sufficient for this dynamic threat environment.

1.3 Objectives of the Study

1. Understand the current cybersecurity threat landscape facing banking institutions globally and in India.
2. Study the role of IT audit in identifying, assessing, and mitigating cybersecurity risks in banks.
3. Evaluate major cybersecurity and IT governance frameworks (NIST CSF, ISO 27001, COBIT 2019, PCI DSS).
4. Examine the regulatory environment governing IT security in banking, focusing on RBI guidelines.
5. Gain practical experience in IT audit procedures and cybersecurity assessment methodologies.
6. Identify emerging threats and propose recommendations for strengthening IT audit and cybersecurity.

1.4 Scope and Limitations

This study covers IT audit practices and cybersecurity measures in commercial banking, drawing from published literature and practical observations at SecureNet InfoTech Solutions. The focus is primarily on the Indian banking context, with global frameworks and case studies included. Due to confidentiality agreements, specific client names and proprietary findings cannot be disclosed. The four-month internship limited the variety of engagements observed.

II. ABOUT THE ORGANISATION

2.1 Company Profile

SecureNet InfoTech Solutions Pvt. Ltd. is a Mumbai-based IT consulting and cybersecurity services company established in 2017, headquartered in Andheri East. The company works with financial institutions including banks, NBFCs, and insurance companies. It has a team of around 45 professionals including certified IT auditors (CISA), cybersecurity specialists (CISSP, CEH), and compliance consultants, with experience across over 30 banking clients in India.

2.2 Services Offered

The company offers: IT Audit and Assurance (covering infrastructure, applications, data security, and regulatory compliance); VAPT services for banking applications, networks, and APIs; Cybersecurity Consulting (policy development, security architecture review, incident response planning); Compliance Management (RBI guidelines, PCI DSS, ISO 27001); SOC Advisory (SIEM configuration, alert tuning, incident escalation); and Training and Awareness programmes for bank employees at all levels.

2.3 Role During Internship

We were assigned to the IT Audit and Compliance team as junior audit assistants under Mr. Rakesh Verma. Activities included assisting in IT audit fieldwork at banking client sites, reviewing IT security policies against RBI guidelines, participating in vulnerability assessment scans using Nessus and Qualys, preparing audit documentation, attending client meetings, studying publicly reported banking cyber incidents, and assisting in compliance gap analysis for PCI DSS and ISO 27001.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

III. LITERATURE REVIEW

3.1 Evolution of IT in Banking

The journey of IT in banking traces back to the 1960s with mainframe computers for back-office automation. The 1990s brought electronic banking and online portals, exposing bank systems to the public internet. Zavolokina et al. (2016) and Gomber et al. (2017) documented how FinTech innovations disrupted traditional banking. Arner et al. (2015) trace the emergence of "RegTech" as a response to growing compliance burdens post-2008. In India, digital transformation was accelerated by Jan Dhan Yojana, UPI, and demonetisation (2016). NPCI reported UPI transactions crossing 10 billion per month by 2023.

3.2 Cybersecurity Threats in Banking

Srinivasan (2019) categorises threats into external attacks (hacking, phishing, DDoS, ransomware) and internal threats (employee fraud, data leakage, social engineering). Bouveret (2018) in an IMF working paper estimated potential cyber losses in finance could amount to hundreds of billions annually. Connolly and Wall (2019) documented how crypto-ransomware and cryptocurrency payments have made attacks easier to monetise.

3.3 Role of IT Audit

ISACA's COBIT framework places IT audit at the centre of ensuring IT process alignment with business objectives (ISACA, 2018). Senft et al. (2012) describe IT auditing as comprising four core activities: evaluating IT plans, testing controls, assessing compliance, and verifying efficient resource usage. Hunton and Rose (2010) provide empirical evidence that banks with mature IT audit functions experience significantly fewer operational losses from IT failures and cyber incidents.

3.4 Prior Research and Gaps

Despite extensive literature on individual components of banking cybersecurity, there is a noticeable gap in holistic analyses integrating IT audit practice, cybersecurity frameworks, regulatory compliance, and practical implementation into a single study. Most research focuses on one aspect in isolation. Additionally, smaller regional and cooperative banks are underrepresented in academic literature despite facing comparable threats with far fewer resources. This report attempts to partially address these gaps.

IV. CYBER THREAT LANDSCAPE IN BANKING

4.1 Types of Cyber Threats

Phishing and Social Engineering: According to the Verizon 2023 DBIR, phishing accounted for over 36% of all data breaches, with financial services among the most targeted sectors. Spear phishing targeting specific employees, often impersonating senior executives, has become especially prevalent in banking.

Ransomware: These attacks encrypt critical data and demand cryptocurrency payments. "Double extortion" ransomware, where attackers also steal data and threaten publication, has worsened the situation significantly.

APTs: State-sponsored groups like the Lazarus Group and Carbanak represent the most sophisticated threats, capable of remaining hidden in networks for months or years. Carbanak reportedly stole over USD 1 billion from banks across 30 countries.

DDoS and Insider Threats: DDoS attacks target service availability and are sometimes used as distraction for deeper intrusions. Insider threats remain the most challenging category as attackers already have authorised access, rendering perimeter-based defenses ineffective.

Table 1: Common Cyber Threats Facing Banking Institutions

Threat Type	Impact Level	Primary Target	Detection Difficulty
Phishing	High	Employees	Medium
Ransomware	Critical	Data & Systems	Medium-High
APTs	Critical	Infrastructure	Very High

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

DDoS	Medium-High	Availability	Low
Insider Threats	High	Data & Financials	Very High
Supply Chain	High	Third-party links	High

4.2 Attack Vectors

The primary attack vectors in banking cyberattacks include email (phishing and malware delivery), web applications (exploiting vulnerabilities in online banking portals), network infrastructure (targeting misconfigured firewalls and unpatched systems), third-party connections (compromising vendor access points), and mobile applications. During the internship, we observed that many vulnerabilities found during audits were related to misconfigured systems and unpatched software rather than sophisticated zero-day exploits, suggesting that basic security hygiene remains a major challenge for many banks.

4.3 Notable Banking Cyber Incidents

Bangladesh Bank SWIFT Heist (2016): Attackers attributed to the Lazarus Group compromised SWIFT credentials and submitted fraudulent transfers totalling USD 951 million. USD 81 million was transferred before detection. The bank lacked a firewall between SWIFT and its internal network.

Capital One Data Breach (2019): A misconfigured WAF allowed access to AWS environments, exposing data of over 100 million customers, highlighting cloud security risks.

Cosmos Bank ATM Heist (2018): Hackers compromised the ATM switch server of Cosmos Cooperative Bank, Pune, authorising ~15,000 fraudulent transactions across 28 countries with losses of approximately INR 94 crore (~USD 13.5 million).

V. IT AUDIT IN BANKING SYSTEMS

5.1 Definition and Scope

IT audit is the process of systematically examining an organisation's IT infrastructure, policies, operations, and controls to determine whether they adequately protect assets, maintain data integrity, and operate effectively. Modern banking IT audits cover: core banking system integrity, network infrastructure security, cybersecurity controls, cloud governance, mobile/online banking security, data governance, third-party vendor risk, business continuity, regulatory compliance, and change management processes.

5.2 IT Audit Process

Table 2: IT Audit Process Phases

Phase	Key Activities	Deliverables
1. Planning & Risk Assessment	Define scope, review prior findings, assess IT risk profile	Audit plan, risk assessment report
2. Control Environment Assessment	Evaluate IT governance, review access controls, assess frameworks	Control assessment workpapers
3. Technical Testing	Vulnerability scanning, penetration testing, configuration reviews	VAPT reports, technical findings
4. Compliance Verification	Verify compliance with RBI, PCI DSS, internal policies	Compliance gap analysis report

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, May 2026 Impact Factor: 8.2

5. Reporting & Remediation	Document findings, assign risk ratings, provide recommendations	Final audit report, remediation tracker

During the planning phase, senior auditors emphasised understanding the bank's business context before technical work. They would spend time understanding the bank's product portfolio, customer base, and technology architecture before deciding what to focus on. This risk-based approach meant audit resources were concentrated on areas posing the greatest risk. The technical testing phase was the most exciting part for us personally, involving vulnerability scanning, configuration review, log analysis, and sometimes controlled penetration testing. We assisted with running Nessus scans on a client's internal network and it was fascinating to see the volume of vulnerabilities discovered even in well-managed banking environments.

5.3 Frameworks and Challenges

The most commonly used frameworks include COBIT 2019, ISO 27001, NIST CSF, and PCI DSS. Most banks use a combination for comprehensive coverage. COBIT 2019 is particularly popular for IT governance as it provides structured processes and control objectives directly mappable to audit procedures (ISACA, 2018).

Key challenges in banking IT audit include the rapid pace of technological change as banks constantly adopt cloud computing, AI-driven services, open banking APIs, and cryptocurrency integrations. Legacy system complexity is another major challenge as many banks still run COBOL-based core banking integrated with modern digital layers through complex middleware. During one engagement, the team spent nearly a week understanding data flows between the legacy core banking system and the newer internet banking platform. There is also a significant shortage of qualified IT audit professionals combining financial industry knowledge with deep technical cybersecurity competency.

VI. CYBERSECURITY FRAMEWORKS FOR BANKING

6.1 NIST Cybersecurity Framework

The NIST CSF, first published in 2014 and updated to version 2.0 in 2024, introduced a sixth core function "Govern" alongside the original five: Identify, Protect, Detect, Respond, and Recover. It is technology-agnostic and scalable for institutions of different sizes. The "Govern" function reflects recognition that cybersecurity is fundamentally a governance challenge requiring board-level strategy and oversight.

6.2 ISO/IEC 27001

ISO/IEC 27001 provides a systematic approach to managing sensitive information through risk management and security controls. The 2022 update introduced 11 new controls for threat intelligence, cloud security, data masking, and secure coding. Several banking clients we observed were either certified or preparing for certification.

6.3 COBIT and PCI DSS

COBIT 2019 organises IT governance into 40 processes under five domains, with strong business-IT linkage. The RBI has referenced COBIT principles in its guidelines. PCI DSS is mandatory for organisations handling payment cards. Version 4.0 (2022) introduced a "customised approach" allowing innovative controls rather than purely prescriptive requirements.

Table 3: Comparison of Cybersecurity Frameworks

Framework	Focus Area	Mandatory?	Key Strength
NIST CSF 2.0	Comprehensive cybersecurity	Voluntary	Scalable, technology agnostic
ISO 27001:2022	Information security management	Voluntary (certification)	International recognition
COBIT 2019	IT governance and management	Voluntary	Business-IT alignment

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

PCI DSS 4.0	Payment card data security	Mandatory for card processors	Specific, auditable requirements

VII. REGULATORY ENVIRONMENT

7.1 Global Regulatory Landscape

Banking cybersecurity is governed by complex regulatory frameworks spanning multiple jurisdictions. The Basel Committee incorporated cyber risk into its operational risk capital framework under Basel III and published cyber resilience guidelines in 2018. The EU's DORA (effective January 2025) establishes harmonised ICT risk management requirements. In the US, the Gramm-Leach-Bliley Act and NYDFS Cybersecurity Regulation (23 NYCRR 500) require specific controls including MFA, encryption, and regular penetration testing.

7.2 RBI Guidelines (India)

Table 4: RBI Cybersecurity Regulatory Timeline

Year	Guideline/Direction	Key Requirements
2016	Cyber Security Framework for Banks	Baseline cybersecurity, SOC establishment, incident reporting
2021	Digital Payment Security Controls	Controls for internet banking, mobile banking, card payments
2023	Master Direction on IT Governance	IT risk management, IS audit, business continuity
2023	Cyber Security Vision Document	Regulatory oversight, capacity building, international cooperation

The RBI's 2016 framework required all banks to implement baseline cybersecurity including SOC establishment and board-approved Information Security Policy. The 2023 Master Direction consolidated IT governance requirements. Non-compliance can result in monetary fines, business restrictions, and regulatory action against management. Globally, penalties are severe: GDPR allows fines up to EUR 20 million or 4% of global annual turnover; NYDFS 23 NYCRR 500 allows up to USD 250,000 per violation; and PCI DSS non-compliance can incur USD 5,000 to 100,000 per month.

VIII. WORK DONE DURING INTERNSHIP

8.1 Activities Performed

During the four-month internship (January–April 2026), we performed the following:

IT Audit Fieldwork: Assisted senior auditors at two banking client sites with data collection, reviewing access control lists, verifying user access rights against HR records, checking configurations against security baselines, and documenting observations. Every finding required proper evidence (screenshots, logs, configuration files).

Vulnerability Assessment: Participated in Nessus scans for a banking client's internal network. Findings included outdated SSL certificates, unpatched OS versions, default credentials on network devices, and misconfigured firewall rules.

Policy and Compliance Review: Reviewed information security policies against the RBI's Master Direction on IT (2023), mapping policy documents to regulatory requirements and identifying gaps.

Incident Case Study Research: Analysed five major banking cyber incidents, preparing summaries of attack methodology, vulnerabilities, impact, and lessons learnt.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

8.2 Tools and Technologies Used

Table 5: Tools Used During Internship

Tool	Category	Purpose
Nessus Professional	Vulnerability Scanner	Network vulnerability assessment
Qualys Cloud Platform	Vulnerability Scanner	Web application security scanning
Wireshark	Network Analyser	Network traffic analysis
Burp Suite Community	Web App Security	Web application penetration testing
Microsoft Excel	Data Analysis	Audit working papers and analysis
JIRA	Project Management	Tracking findings and remediation

8.3 Key Observations

• Access control weaknesses are widespread: Excessive privileges, shared accounts, dormant user IDs, and lack of regular access reviews found in almost every engagement.
• Patch management is a persistent challenge: Banks struggled to keep systems patched due to downtime fears and testing complexity.
• Security awareness varies significantly: Banks with regular training had fewer social engineering incidents.
• Smaller banks face disproportionate challenges: Same threats as larger banks but with significantly fewer resources.
• Documentation gaps: Good controls implemented but lacking proper documentation of policies and procedures.

IX. FINDINGS AND RECOMMENDATIONS

9.1 Key Findings

1. The threat landscape is dynamic, sophisticated, and increasingly enabled by advanced technologies. Traditional perimeter defenses are no longer sufficient.
2. IT audit provides critical independent assurance that security controls work as intended and identifies vulnerabilities before exploitation.
3. The most effective approach uses a combination of frameworks: NIST CSF for structure, ISO 27001 for management systems, COBIT for governance, PCI DSS for payment card security.
4. The regulatory environment is becoming increasingly stringent globally, with the RBI progressively strengthening requirements.
5. A significant gap exists between large banks and smaller institutions in cybersecurity maturity.
6. Human factors (security awareness, culture, skilled professionals) are as important as technical controls.
7. Emerging threats (AI-powered attacks, quantum computing, supply chain vulnerabilities) will require continuous evolution of security strategies.

9.2 Recommendations

9.2.1 Transition to Continuous IT Audit: The traditional model of conducting IT audits once or twice a year is no longer adequate for the dynamic threat environment. Banks should invest in automated data analytics, continuous control monitoring, and real-time dashboards for ongoing assurance rather than point-in-time assessments. This allows audit teams to detect anomalies and control failures more quickly, reducing the window of exposure.
9.2.2 Adopt Zero Trust Architecture: Banks should move towards a Zero Trust model operating on "never trust, always verify," where every user, device, and network flow is considered untrusted by default and must be authenticated and authorised before being granted access. This is particularly important in modern banking environments involving cloud computing, remote work, and extensive third-party integrations.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, May 2026 Impact Factor: 8.2

9.2.3 Invest in Cybersecurity Talent and Culture: Technical controls alone are not enough. Banks need regular security awareness training for all employees, specialised technical training for IT staff, competitive compensation to attract and retain skilled professionals, and a culture where employees feel comfortable reporting security concerns without fear of reprisal.

9.2.4 Strengthen Third-Party Risk Management: Given increasing reliance on third-party technology providers, banks must conduct rigorous vendor security assessments, include cybersecurity clauses in contracts, conduct periodic security reviews, and have contingency plans for compromised vendors.

9.2.5 Plan for Post-Quantum Cryptography: Banks should inventory all cryptographic dependencies, monitor NIST post-quantum standards (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+ finalised in 2024), and develop migration roadmaps for future adoption.

9.2.6 Engage with Threat Intelligence Sharing: Banks should actively participate in FS-ISAC and CERT-In, sharing threat information and defensive strategies with peer institutions to strengthen the collective defense of the entire banking sector.

9.2.7 Board-Level Cybersecurity Governance: Cybersecurity must be treated as a board-level strategic risk with regular briefings, board-approved budgets, and clearly defined accountability at the highest organisational levels. The RBI has explicitly required that banks have a board-approved Information Security Policy.

X. CONCLUSION AND FUTURE SCOPE

This report has presented a comprehensive study of IT audit practices and cybersecurity measures in banking systems, drawing from academic literature and practical experience during a four-month internship at SecureNet InfoTech Solutions Pvt. Ltd., Mumbai. The study covered the cyber threat landscape, IT audit role and methodology, major cybersecurity frameworks, the regulatory environment, and practical observations from real audit engagements.

The findings demonstrate that cybersecurity has become a fundamental pillar of sound banking governance. Threats are becoming more sophisticated and frequent, while regulatory expectations and penalties for non-compliance grow more severe. IT audit plays an indispensable role by evaluating cybersecurity controls, identifying vulnerabilities, and ensuring regulatory compliance.

The internship experience was immensely valuable, providing insights that classroom learning alone could not offer. Working alongside experienced IT auditors and cybersecurity professionals, observing real engagements, and gaining hands-on experience with industry tools gave us a much better understanding of what it takes to protect banking systems from cyber threats and how IT audit contributes to that goal.

Looking ahead, the banking cybersecurity landscape will continue to evolve rapidly. Emerging threats including AI-powered attacks, quantum computing risks, and growing supply chain vulnerabilities will require continuous innovation in cybersecurity practice and IT audit methodology. Banks that invest in building strong cybersecurity foundations today, through robust IT audit programmes, adoption of international security frameworks, compliance with regulatory requirements, and investment in cybersecurity talent and culture, will be better positioned to navigate the challenges of tomorrow.

Future Scope: This study can be extended through a quantitative survey of Indian banks, exploring blockchain-based security and AI-driven audit tools, and comparative studies of cybersecurity practices between Indian and international banks.

REFERENCES

[1]. Basel Committee on Banking Supervision. (2018). Cyber resilience: Range of practices. Bank for International Settlements.
[2]. Bouveret, A. (2018). Cyber risk for the financial sector. IMF Working Paper WP/18/143.
[3]. Connolly, L., & Wall, D. S. (2019). The rise of crypto-ransomware. Computers & Security, 87, 101568. Federal Bureau of Investigation. (2023). Internet Crime Report 2023. FBI IC3.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

[4]. Gomber, P., Koch, J. A., & Siering, M. (2017). Digital finance and FinTech. Journal of Business Economics, 87(5), 537-580.
[5]. IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation. ISACA. (2018). COBIT 2019 Framework: Introduction and Methodology. ISACA.
[6]. ISO/IEC 27001:2022. Information security management systems — Requirements. ISO. NIST. (2024). Cybersecurity Framework 2.0. US Department of Commerce.
[7]. PCI SSC. (2022). PCI DSS Version 4.0.
[8]. Reserve Bank of India. (2016). Cyber Security Framework in Banks. RBI/2015-16/418.
[9]. Reserve Bank of India. (2023). Master Direction on IT Governance, Risk, Controls and Assurance. Senft, S., Gallegos, F., & Davis, A. (2012). IT Control and Audit (4th ed.). CRC Press.
[10]. Srinivasan, R. (2019). Cybersecurity in Banking. Journal of Financial Crime, 26(2), 467-482. Verizon. (2023). 2023 Data Breach Investigations Report.
[11]. Zavolokina, L., Dolata, M., & Schwabe, G. (2016). The FinTech phenomenon. Financial Innovation, 2(1), 1-16.