

“Enhancing Fraud Detection in Core Banking Systems Through Risk-Based Internal Controls and Forensic Auditing”

Dr. Shailendrasingh Dikit

Assistant Professor-Chhatrapati Shahu Institute of Business Education and Research,
Kolhapur(Maharashtra) India.

DOI: <https://doi.org/10.51583/IJLTEMAS.2026.150600295>

Received: 16 July 2026; Accepted: 21 July 2026; Published: 04 August 2026

ABSTRACT

The proliferation of Core Banking Systems (CBS), digital banking, cloud computing and real-time payment platforms has made financial fraud more sophisticated. Current fraud detection techniques are not effective anymore against new cyber assaults and complex financial crimes. This paper discusses the role of forensic auditing, risk-based internal controls and emerging technologies in enhancing fraud prevention in commercial banks. It discusses the application of forensic auditing with a combination of digital forensics, artificial intelligence (AI), machine learning, behavioural analytics, blockchain, and continuous auditing to improve fraud detection, fraud investigation, and regulatory compliance. The study also discusses contemporary issues in banking fraud such as insider threats, data privacy, legacy system integration, and regulatory requirements and suggests strategic measures to enhance fraud resilience. The findings indicate that the implementation of intelligent technologies with strong governance and forensic auditing mechanisms enable proactive fraud management, strengthen operational resilience, protect customer assets, and build trust in digital banking ecosystems.

Keywords : Core Banking Systems (CBS), Forensic Auditing, Financial Fraud Detection, Artificial Intelligence (AI), Blockchain Technology, Continuous Auditing, Risk-Based Internal Controls, Digital Banking

Part 1: Introduction and Development of Fraud in Core Banking Systems

The Digital revolution of banking has transformed the financial services with Core Banking Systems (CBS), cloud computing, artificial intelligence (AI), mobile banking and real-time payment platforms. Although these technologies have enhanced operational efficiency and customer convenience, they have also heightened banks' exposure to sophisticated cyber fraud.

Modern CBS converges the deposits, loans, payments, customer management and regulatory reporting on one central platform enabling real time banking on multiple digital channels. But this combination is a lucrative target for cybercriminals who use phishing, malware, ransomware, identity theft, insider fraud and social engineering attacks. The growing volume of digital transactions is beyond the capability of traditional manual audits or rule-based fraud detection systems.

In the face of these challenges, banks are turning to AI, machine learning, predictive analytics and behavioural monitoring to fight fraud in real-time. But technology alone cannot eliminate fraud. Strong governance, risk-based internal controls, ethical organisational culture, regulatory compliance and forensic auditing are key to effective fraud prevention. As banking moves online, banks can enhance operational resilience, safeguard customer assets, comply with regulations and maintain public trust by combining intelligent fraud detection, risk-based controls and forensic auditing.

Part 2: Risk Based Internal Controls and Fraud Prevention

The growing sophistication of financial fraud in Core Banking Systems (CBS) has made banks to move to proactive risk-based internal control frameworks instead of traditional compliance-based approaches. Risk-based

frameworks are unlike traditional controls as monitoring, authorisation and audit resources are assigned based on the likelihood and consequences of fraud. This allows banks to focus on high risk transactions, critical operations and vulnerable systems.

Modern CBS platforms handle millions of transactions every day via branches, ATMs, mobile banking, internet banking, UPI and Fintech platforms. These create new opportunities for cyber fraud. “Effective fraud prevention, therefore, requires continuous risk assessment, behaviour monitoring, cybersecurity governance and predictive analytics.” Strong Know Your Customer (KYC) procedures, biometric verification, transaction monitoring, role-based access control (RBAC), multi-factor authentication and segregation of duties minimise the risk of both external and insider fraud.

Artificial intelligence and machine learning improve fraud prevention by analysing transaction patterns, customer behaviour and anomalies in real-time, increasing detection accuracy and reducing false alerts. But technology alone is not sufficient. Good governance, ethical leadership, employee awareness, internal audit and regulatory compliance are also critical in effective fraud prevention. By embedding intelligent technologies, risk-based internal controls, cybersecurity and forensic auditing, banks can improve their operational resilience, protect their customers’ assets, meet regulatory requirements and maintain public trust in the changing digital banking environment.

Part 3: Forensic Auditing Techniques and Integration with Core Banking

The digital transformation of banking has increased the complexity of financial fraud, making traditional financial audits insufficient for detecting sophisticated cyber-enabled crimes. Therefore, forensic auditing has been developed as a specialised discipline by combining accounting, auditing, digital forensics, data analytics, information technology and legal investigation to detect, investigate and prevent fraud in Core Banking Systems (CBS).

Unlike conventional audits that focus on financial statement accuracy, forensic auditing seeks to identify fraudulent activities, determine responsible individuals, quantify losses, preserve digital evidence, and support legal proceedings. Modern Core Banking Systems produce huge amounts of digital data such as transaction histories, audit logs, user credentials, IP addresses, device data, and authorisation trails. Such digital footprints enable forensic auditors to rebuild fraudulent events and present evidence that can be used in a court of law.

Forensic auditing uses a risk-based investigation approach that focuses on high-risk areas such as unauthorised fund transfers, loan fraud, privileged user activities, dormant accounts, procurement, and digital payment systems. Advanced data analytics and artificial intelligence allow auditors to analyse millions of transactions, identify anomalies, detect hidden fraud patterns, and monitor customer and employee behaviour in real time. Behavioural analytics, network analysis, machine learning and graph analytics techniques greatly enhance fraud detection and cut down the time spent on investigations.

Forensic auditing combined with Core Banking Systems allows for continuous instead of periodic monitoring. Automated alerts, real-time transaction analysis and centralised digital evidence provide investigators with the tools to identify suspicious activities before major financial losses occur. Technologies like cloud computing, blockchain and Explainable Artificial Intelligence (XAI) further enhance the evidence integrity, transparency and regulatory compliance.

In conclusion, forensic auditing along with risk-based internal controls and intelligent technologies can offer a comprehensive framework for fraud management in commercial banks. In a growing digital banking environment, it enhances fraud prevention, enables timely investigations, provides better governance, supports regulatory compliance, and sustains customer trust.

Part 4: Emerging Technologies Revolutionising Fraud Detection in Core Banking Systems

Higher operational efficiency and increased complexity in financial fraud, due to the fast pace of digitisation in banking, has made traditional fraud detection methods insufficient. Commercial banks are adopting emerging

technologies such as Artificial Intelligence (AI), advanced analytics, blockchain, cloud computing, and continuous auditing to develop proactive fraud management systems to counter the evolving cyber risks.

Machine learning and artificial intelligence analyse large volumes of banking data to detect trends of fraud, behavioural irregularities and suspicious transactions in real time, helping to improve detection accuracy and reduce false positives. The sophisticated analytics and graph based network analysis reveal hidden relations between customers, accounts and transactions, aiding the detection of organised financial crimes like money laundering and insider fraud.

Blockchain provides immutable and transparent transaction records that enhance fraud prevention and help strengthen audit trails and data integrity. With cloud computing, you can perform scalable analytics in real time. Continuous auditing automates the monitoring of transactions and controls as opposed to periodic reviews.

The convergence of AI, blockchain, advanced analytics and continuous auditing creates an intelligent fraud detection ecosystem that enhances operational resilience, regulatory compliance, customer trust and the capacity of financial institutions to prevent increasingly sophisticated financial crimes.

Part 5: Challenges, Recommendations and Conclusion

Despite the significant technological advancements, Fraud detection in Core Banking Systems (CBS) still face several challenges including rapidly evolving cyber risks, insider fraud, high false-positive rates, data privacy concerns, integration of legacy systems, regulatory compliance and scarcity of skilled cybersecurity professionals. The increasing presence of digital banking, cloud platforms and fintech partnerships increases the attack surface, demanding ongoing improvements in fraud mitigation.

To tackle these issues, banks need to implement integrated fraud management frameworks that bring together Artificial Intelligence (AI), machine learning, behavioural analytics, blockchain, risk-based internal controls and continuous auditing. Equally important are regular employee training, strong cybersecurity governance, enhanced Know Your Customer (KYC) procedures, multi-factor authentication and periodic forensic audits. Regulators, banks and technology providers should be encouraged to collaborate to share threat intelligence and enhance industry-wide resilience.

To put it simply, modern banking fraud prevention requires a proactive and technology-driven approach rather than relying on traditional controls alone. Intelligent fraud detection, forensic auditing, advanced analytics and sound governance help financial institutions spot emerging threats, improve regulatory compliance, protect customer assets and boost operational resilience. Future research should focus on explainable AI, quantum-resistant security, blockchain-based auditing, and collaborative fraud intelligence to address new financial crime.

REFERENCES

1. Abdullahi, R., Mansor, N., & Nuhu, M. S. (2020). Fraud prevention initiatives in the banking sector: A systematic review. *Journal of Financial Crime*, 27(4), 1255–1272.
2. ACFE. (2020). Report to the Nations: Global Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners.
3. ACFE. (2022). Occupational Fraud 2022: A Report to the Nations. Association of Certified Fraud Examiners.
4. ACFE. (2024). Occupational Fraud 2024: A Report to the Nations. Association of Certified Fraud Examiners.
5. Adesina, K., Erin, O. A., Ajetunmobi, O., Ilogho, S., & Asiriwa, O. (2020). Does forensic audit influence fraud control? Evidence from Nigerian deposit money banks. *Banks and Bank Systems*, 15(2), 214–229. [https://doi.org/10.21511/bbs.15\(2\).2020.19](https://doi.org/10.21511/bbs.15(2).2020.19)
6. Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2023). The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry. *Cogent Business & Management*, 10(1), 2163560. <https://doi.org/10.1080/23311975.2022.2163560>

7. Al Naqvi, A. (2020). *Artificial Intelligence for Audit, Forensic Accounting, and Valuation*. Wiley.
8. Alles, M. G. (2021). Continuous auditing and continuous monitoring: The evolving role of internal audit. *Journal of Emerging Technologies in Accounting*, 18(2), 1–18.
9. Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2021). Artificial intelligence and analytics in auditing: Current trends and future opportunities. *Accounting Horizons*, 35(4), 1–23.
10. Basel Committee on Banking Supervision. (2021). *Principles for Operational Resilience*. Bank for International Settlements.
11. Basel Committee on Banking Supervision. (2023). *Principles for the Sound Management of Operational Risk*. Bank for International Settlements.
12. Brazel, J. F., Carpenter, T., Gimbar, C., Jenkins, J. G., & Jones, K. L. (2024). Recent research on the identification, assessment, and response to fraud risks: Implications for audit practice and future research. *Accounting Horizons*, 38(3), 1–27.
13. COSO. (2020). *Fraud Risk Management Guide*. Committee of Sponsoring Organizations of the Treadway Commission.
14. Deloitte. (2022). *Global Financial Crime Survey*. Deloitte Insights.
15. Deloitte. (2023). *Banking and Capital Markets Outlook*. Deloitte Insights.
16. EY. (2022). *Global Integrity Report*. Ernst & Young.
17. EY. (2024). *Global Forensic Data Analytics Survey*. Ernst & Young.
18. Gotelaere, S., & Paoli, L. (2025). Prevention and control of financial fraud: A scoping review. *European Journal on Criminal Policy and Research*, 31, 1–21. <https://doi.org/10.1007/s10610-022-09532-8>
19. Huamán, C. B., De la Cruz-Montoya, D., Gutierrez-Cuadros, J., Pilco Labajos, S., & Lopez-Almeida, M. (2025). Financial auditing as an effective tool for fraud detection: A systematic review. *Journal of Risk and Financial Management*, 18(9), 523.
20. IIA. (2020). *The Three Lines Model*. Institute of Internal Auditors.
21. Institute of Internal Auditors. (2024). *Global Internal Audit Standards*. Institute of Internal Auditors.
22. ISACA. (2022). *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution*. ISACA.
23. KPMG. (2021). *Global Banking Fraud Survey*. KPMG International.
24. KPMG. (2023). *Global Banking Risk Outlook*. KPMG International.
25. Liu, Q., Singh, S., & Terzi, E. (2022). Machine learning approaches for financial fraud detection: A comprehensive review. *Expert Systems with Applications*, 202, 117–135.
26. Moffitt, K. C., Rozario, A. M., & Vasarhelyi, M. A. (2021). Robotic process automation for auditing and fraud detection. *Journal of Information Systems*, 35(2), 123–145.
27. PwC. (2020). *Global Economic Crime and Fraud Survey 2020*. PricewaterhouseCoopers.
28. PwC. (2022). *Global Economic Crime and Fraud Survey 2022*. PricewaterhouseCoopers.
29. PwC. (2024). *Global Economic Crime and Fraud Survey 2024*. PricewaterhouseCoopers.
30. Richins, G., Stapleton, A., Stratopoulos, T., & Wong, C. (2021). Big data analytics in auditing and fraud detection. *Journal of Information Systems*, 35(1), 63–87.
31. Rittenberg, L. E., & Johnstone, K. M. (2021). *Auditing: A Business Risk Approach* (11th ed.). Cengage Learning.
32. Soni, L., & Mangala, D. (2025). Preventing and detecting internal fraud risk: A critical analysis of the anti-fraud tools used by the Indian banking industry. *Journal of Money Laundering Control*, 28(2), 424–441.
33. Vasarhelyi, M. A., Kogan, A., & Tuttle, B. (2021). Big data analytics in accounting and auditing. *Accounting Horizons*, 35(3), 1–21.
34. World Economic Forum. (2023). *Global Cybersecurity Outlook 2023*. World Economic Forum.
35. World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. World Economic Forum.
36. Zhang, Y., Xie, L., & Wang, H. (2021). Deep learning techniques for financial fraud detection: A survey. *IEEE Access*, 9, 152248–152269.
37. Zhou, Y., Kapoor, G., & Piramuthu, S. (2022). Explainable artificial intelligence for fraud detection in financial institutions. *Decision Support Systems*, 158, 113790.