African Multidisciplinary
Journal of Sciences and Artificial Intelligence

ISSN : 1595-7969

Index: Harvard, Boston, Sydney University, Dimensions, Lens, ResearchGet Scilit, Semantic, Google Scholar, Base etc

https://doi.org/10.58578/AMJSAI.v3i1.8322

Comparative Analysis of Theoretical Models for Digital Forensic Readiness (DFR) in Nigerian Banking

Chibuzor Akujobi[1], Francisa Ogwueleka[2], Gilbert Aimufua[3], Steven Bassey[4]
[1,3,4]Nasarawa State University Keffi, Nigeria; [2]University of Abuja-FCT, Nigeria
chibuzor.akujobi@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
Oct 21, 2025	Nov 26, 2025	Dec 9, 2025	Dec 14, 2025

Abstract

The increasing shift to digital banking in Nigeria has accelerated cyber fraud losses, prompting banks to adopt proactive forensic readiness measures. Recent industry reports show that Nigerian banks lost more than N300 billion ($833 million) in a single quarter of 2023, a 534% increase year-on-year. Digital Forensic Readiness (DFR) is a proactive cybersecurity strategy that ensures digital evidence is preserved and ready for analysis before a breach occurs. This paper reviews leading forensic readiness models, including Locard's Exchange Principle, the Diamond Intrusion Model, and the NIST Risk Management Framework, and compares their applicability to Nigerian banking. We integrate these theories into a proposed DFR framework tailored for Nigeria's banking sector, drawing on local and global studies. Key components of DFR (such as policies, technology, people, and legal compliance) are discussed with illustrations. Current challenges, notably reactive culture, evidentiary gaps, and regulatory compliance, are highlighted. Finally, best practices and a synthesis framework are presented to guide Nigerian banks toward a more resilient forensic posture.

Keywords: Digital Forensic Readiness; Digital Evidence Preservation; Cyber Fraud Losses; Forensic Readiness Models; Nigerian Banking Sector

Introduction

The Nigerian banking industry has witnessed a surge in digital financial services alongside escalating cybercrime. The Nigeria Inter-Bank Settlement System reports that financial losses in Nigeria's banking sector have been enormous as a result of fraudulent operations. The value of fraud in 2021 was put at N193.5 billion ($544 million), a significant increase from the N153.4 billion ($431 million) lost in 2020. This upward trend continued in 2022 when losses due to fraud topped N273 billion ($762 million). Even these troubling figures are expected to be exceeded by the end of 2023, with projections estimating potential losses of more than N300 billion ($833 million). Mobile and internet channels now account for nearly 72% of fraud cases in Nigeria's banks. These losses erode customer trust and can lead to regulatory penalties. Traditional security measures in Nigerian banks have tended to be reactive focusing on damage control after an incident leaving gaps in evidence preservation and legal compliance. Digital Forensic Readiness (DFR) addresses this gap by preparing systems to capture and manage evidence proactively.

Cyber fraud in Nigeria has grown rapidly with the expansion of internet banking. Data from Nigeria's regulators and police show widespread losses: during the COVID-19 lockdown alone, Nigerian banks lost ₦83.5 billion in one quarter. Most attacks occur via online/mobile channels – e-banking, USSD, social engineering rather than physical breaches. Fraud schemes take many forms: researchers have identified internal fraud (staff colluding with criminals), external fraud (outsiders phishing or hacking customers), and collusive fraud between insiders and outsiders. Historical cases such as multi-million dollar phishing fraud in 2019, demonstrate that cybercriminals exploit any vulnerability in bank systems or personnel.

Nigerian banks also face challenges unique to the local context. According to surveys, many banks lack comprehensive DFR policies and tend to prioritize fraud prevention over evidence preservation. For example, most banks focus on reducing attack impact after it happens, rather than on forensic readiness. Inadequate logging, insufficient staff training, and poor regulatory alignment further hamper investigations. This gap is exacerbated by evolving regulations like the Nigeria's Cybercrime Act (2015) and Data Protection Regulation (2019) which imposes stricter evidence-handling requirements, but many institutions remain unaware of how to comply proactively. Without forensic readiness, banks risk delayed incident response and weaker legal cases against fraudsters.

Despite these challenges, some strength exists: larger Nigerian banks have invested in security operations (e.g. SIEM systems, continuous monitoring, specialized fraud units). However, experts note that legal and procedural gaps persist evidence admissibility issues, outdated policies, and limited forensic skills are widespread. This evidence suggests a dual problem: cyber fraud is rising in Nigerian banking, and existing DFR practices are inconsistent or insufficient.

In this paper, we review core theoretical models underpinning forensic readiness (Locard's Principle, the Diamond model, and Risk Management frameworks) and analyze their relevance to Nigerian banks. We then outline the essential DFR components, compare the models, and propose a tailored DFR framework. This analysis is grounded in recent research and the challenges observed in Nigeria's banking sector.

Literature Review

Digital Forensic Readiness (DFR) is defined as the capacity of an organization to maximize its potential to use digital evidence for legal, investigative, or security purposes. (Rowlingson, 2004; Tan & Lee, 2019) Unlike traditional, reactive forensics, DFR is proactive it establishes policies, procedures, and systems to capture and preserve evidence before an incident (Keong & Choo, 2020; Reith et al., 2002). For example, every digital interaction (emails, transactions, and logins) leaves a trace; well-prepared systems log these artifacts so investigations can proceed swiftly (Elyas et al., 2014; Kent et al., 2006). In the Nigerian context, adequate DFR means banking systems are configured to retain logs, images, and transaction records in a legally compliant manner.

Locard's Exchange Principle (1920) asserted that every contact between a perpetrator and the environment leaves a trace. In cybersecurity, this implies that each malicious event will leave digital artifacts on servers or endpoints. Forensic readiness frameworks applies this principle by ensuring tools (e.g. log collectors, intrusion detectors) are always active so that "every contact" generates collectible evidence. The Diamond Model of Intrusion Analysis (Caltagirone et al., 2013) complemented Locard by focusing on adversary behavior. It breaks down an incident into four linked elements Adversary, Infrastructure, Capability, and Victim forming a "diamond" of relationships. By mapping these features, organizations can anticipate attacker tactics and ensure evidence (malware samples, network traffic, target assets) is gathered proactively. For example, knowing an "adversary" uses a particular tool motivates

deploying sensors to capture that tool's signatures. Meanwhile, the NIST Risk Management Framework (RMF**)** (SP 800-37) brought a structured, risk-based approach. By embedding risk assessment into system design, RMF ensures that critical assets are identified, controls are selected, and monitoring is continuous. In DFR terms, RMF drives organizations to implement security controls (e.g. audit logs, access controls) that protect evidence and support forensic processes.

Other models like the Cyber Kill Chain are also relevant, as they delineate attack stages from reconnaissance to execution (Hutchins et al., 2011). Such models imply that readiness efforts should cover each phase (e.g. capturing malicious payloads at "Delivery" stage, monitoring for "Exploit" events). Overall, these theoretical frameworks provide complementary views: Locard ensures evidence capture, the Diamond model guides threat context, and RMF ensures organizational preparedness. Integrating them yields a holistic forensic readiness strategy.

Digital forensic readiness depends on multiple organizational components. A broad literature survey identifies eight core categories of readiness: People, Process, Policy & Procedure, Technology, Monitoring & Reporting, Risk Assessment and Legal & Compliance. In practical terms, banks need clear policies and procedures to govern evidence collection and retention. For example, a bank should have documented retention policies, evidence-handling standard operating procedures (SOPs), and defined roles (who collect logs, who analyzes data). Technological components include log management systems, intrusion detection, firewalls, and endpoint forensics tools. These ensure that when an incident occurs, relevant data (logs, disk images, metadata) are captured and preserved. People and training are also crucial: staff must be aware of forensic policies and have skills (through training or certifications) to follow them. Furthermore, ongoing monitoring, incident reporting, and regular audits help detect potential breaches early and maintain evidence integrity.

These elements can be summarized as follows:

i. **Policies & Procedures:** Formal forensic policies, compliance frameworks, and SOPs to guide evidence handling.

ii. **Technology:** Systems configured for forensics e.g., SIEM platforms (Splunk, IBM QRadar), secure logging, intrusion detection, and forensic software (EnCase, Autopsy).

iii. **People & Training:** Skilled personnel (cybersecurity analysts, forensic investigators) and awareness programs (e.g., phishing simulations) to maintain readiness culture.

iv. **Legal & Compliance:** Alignment with laws (e.g. Nigeria's Cybercrime Act, NDPR) and admissibility standards – ensuring collected evidence is court-ready.

v. **Risk Assessment & Management:** Continuous risk analysis (using frameworks like ISO 31000 or NIST) to identify threats to digital assets and adjust controls accordingly.

vi. **Monitoring & Reporting:** Continuous monitoring (e.g., dashboards, network analyzers) and clear incident reporting protocols, so suspicious events trigger forensic workflows.

Table 1. illustrates how various tools and techniques support these DFR components. In practice, Nigerian banks leverage platforms (Metric Stream, KnowBe4, SIEM, etc.) and processes (policy development, incident escalation, evidence imaging) that map to each component. Implementing all components cohesively is key; missing elements (for example, having SIEM tools but no documented chain-of-custody) undermines readiness.

Table 1. Illustration of tools and techniques by Digital Forensic Readiness (DFR) components

DFR Component	Example Tools/Platforms	Techniques/Practices
Policy & Procedure	Compliance platforms (MetricStream), document repositories (SharePoint)	Policy development, formal SOPs, retention policies
Technology	SIEM (e.g. Splunk, QRadar), firewalls, IDS/IPS, endpoint security (CrowdStrike) Forensic suites (EnCase, FTK, Autopsy), data recovery tools	Log aggregation/correlation, alert triage, threat-intel integration. Disk imaging, file carving, timeline & metadata analysis
People (Awareness)	E-learning (KnowBe4), forensic training (CHFI, GCFA)	Security awareness training, phishing simulations, skill development
Legal & Compliance	e-Discovery tools, legal audit platforms	Regulatory gap analysis, evidence admissibility reviews, alignment with NDPR/NPDC requirements
Risk Assessment	Risk Mgmt tools (e.g. RSA Archer), vulnerability scanners (Nessus)	Threat modeling, impact analysis, digital risk scoring
Monitoring & Reporting	Dashboards (SIEM), packet analyzers (Wireshark), logging agents	Continuous monitoring, anomaly detection, automated incident reporting
Process	Workflow systems (Jira, ServiceNow), chain-of-custody platforms	Incident escalation procedures, evidence documentation, optimized forensic workflows

Comparative Analysis of Theoretical Models

We compared three prominent models relevant to forensic readiness:

i. **Locard's Exchange Principle:** Emphasized that *"every contact leaves a trace"*. In DFR terms, this means every digital action (login, transaction, and email) will deposit artifacts. Models based on Locard's principle focuses on evidence collection ensuring systems are configured to capture logs, memory dumps and other traces before they are overwritten. Its strength is a firm evidentiary foundation: by assuming traces exist, an organization remains vigilant in data capture. However, Locard's model is conceptual rather than prescriptive; it does not specify processes or controls, so banks need complementary frameworks to operationalise it.

ii. **Diamond Intrusion Model (Caltagirone et al., 2013):** Breaks down an intrusion into four linked elements (Adversary, Infrastructure, Capability, Victim) forming a "diamond". This model excels at threat context as it helps analysts map attacker tools to targets. In practice, a bank using the Diamond model will proactively hunt for evidence of known adversary infrastructure (e.g., command-and-control servers) and capabilities (malware signatures) against its systems. Its advantage is structured threat analysis and attribution support; it encourages linking incidents into broader campaigns. Limitations include complexity (requires detailed intelligence about adversaries) and focus on networked attacks it may be less directly helpful for purely insider fraud without external infrastructure. Still, it guides collecting evidence about who is attacking and how, enriching DFR.

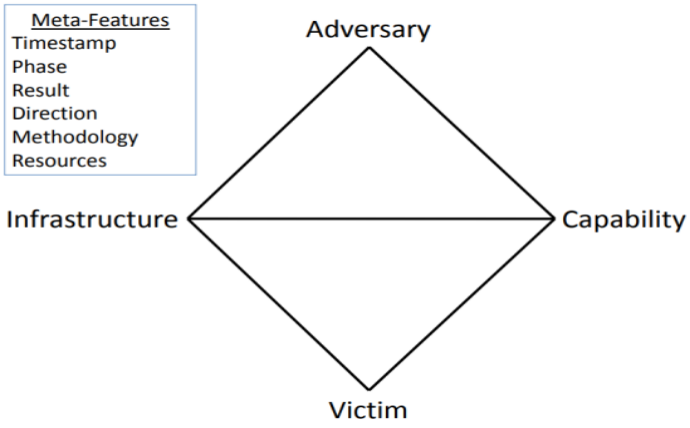

Figure 1. The Diamond Model of intrusion analysis (Caltagirone et al, 2013)

iii. **Risk Management Framework (NIST RMF):** A process-oriented model (Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor) for managing cybersecurity risk. In

a DFR context, RMF ensures that forensic readiness is institutionalized through policies and controls. For example, during the "Select" phase, a bank would choose specific forensic controls (e.g. write-once logs); the "Monitor" phase enforces their continuous operation. RMF's strength lies in its comprehensive, formal approach – aligning forensic controls with business objectives and compliance requirements. It also emphasizes continuous oversight, which supports forensic readiness over time. However, RMF is resource-intensive and bureaucratic; smaller banks may find its processes heavy. Moreover, RMF is broad (covering all security), so forensic-specific needs could be overlooked unless explicitly addressed.

These models overlap but emphasize different facets as shown in Table 2.0. Locard's principle underpins evidence focus, the Diamond model underpins adversary-centric analysis, and RMF underpins governance and process controls. In Nigerian banking, a hybrid approach is advisable: apply Locard by enhancing logging and data preservation; use Diamond concepts in threat intelligence and incident analysis; and adopt RMF practices for policy and risk governance. Each model contributes: for instance, logs collected per Locard become inputs into a diamond-style analysis of an attack, and RMF ensures both activities are documented and compliant. The comparative advantages and limitations of each are summarized below.

Table 2. Comparative summary of key DFR-related models/frameworks, with their focus and trade-offs.

Model/Framework	Focus	Strengths	Limitations
Locard's Principle	Evidence collection ("every contact leaves trace")	Ensures all system interactions are considered as potential evidence; simple forensic rationale	Conceptual only needs policies/tools to implement; limited guidance on processes
Diamond Model	Adversary-centric threat analysis (Adversary, Capability, Infrastructure, Victim)	Structured view of attacker behavior; aids threat hunting and attribution	Requires detailed threat intel; may not cover insider-only scenarios
Risk Management Framework (NIST)	Risk-based security lifecycle (Prepare→Monitor)	Aligns forensic controls with business objectives; mandates continuous oversight	Complex and process-heavy; forensic elements may be overlooked without focus; requires mature governance

Proposed DFR Framework for Nigerian Banks

Drawing on these models and Nigeria-specific needs, A tailored Digital Forensic Readiness Framework (DFRF) for the Nigerian banking sector was proposed. This framework integrates technical, organizational, and legal dimensions. Seven key components form its core: Policy & Procedure, People, Process, Technology, Risk Assessment, Legal & Compliance, and Monitoring & Reporting. For example, the "Policy & Procedure" component mandates formal forensic policies aligned with NDPR and CBN rules, while "Technology" covers forensic-capable IT systems (SIEMs, endpoint agents). The "Legal & Compliance" component ensures evidence handling complies with Nigeria's Cybercrime Act (2015) and admissibility standards.

This DFRF is proactive rather than reactive. Its goal is to enable evidence collection before an incident: for instance, real-time logging of transactions and automated alerts for anomalies. As an expert review of this framework found, it "ensures banks can collect, preserve, and utilize digital evidence efficiently before a cyber incident occurs". To ground the framework in practice, we leverage existing strengths of Nigerian banks: many already use SIEM and monitoring tools. The DFRF layers on these by adding clear roles (People component) and legal checks. Conversely, it directly addresses known gaps: e.g. reinforcing Risk Assessment (via threat modeling) and strengthening legal compliance (via internal audit).

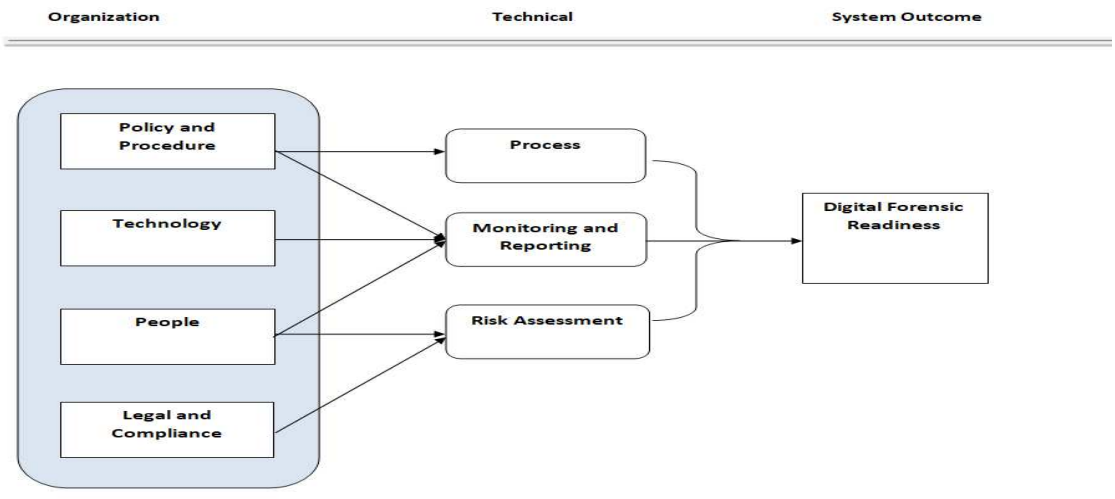

Figure 2. Proposed Visual Representation of the components for DFRF

Figure 2 conceptually illustrates the proposed framework. In essence, all components interact dynamically so that whenever suspicious activity is detected (through Monitoring &

Reporting), the Process and People components spring into action (incident protocols and forensic response), supported by Technology and guided by Policies. This cycle ensures Nigerian banks are "strategically positioned to prevent and manage [cyber attacks] through continuous monitoring and reporting", fulfilling both security and regulatory objectives.

Discussion

This analysis highlights that effective DFR in Nigerian banking requires a synthesis of models and practice**s**. Locard's principle drives evidence-centric preparedness: e.g. expecting that a fraudster's laptop will retain traces of transactions. The Diamond model encourages Nigerian banks to build threat intelligence, connecting adversaries to their tools and targets. The RMF brings the necessary governance rigor (setting policies, authorizations, and monitoring loops) to make readiness systematic.

Local challenges underscore where gaps remain. Many Nigerian banks have reactive cultures; experts note that digital forensics capabilities are often fire-fighting rather than planned. In practice, this means logs may not be retained long enough, and evidence chains might be broken. There is also a shortage of skilled forensic personnel, as well as low awareness of legal requirements (e.g., preserving electronic records per NDPR). Best practices emerging from industry studies include: defining clear incident response roles, conducting regular readiness drills (simulations), and aligning forensic processes with compliance audits.

Our proposed framework embodies these lessons. By integrating continuous risk assessment, legal audits, and technical controls, it addresses the implementation gaps identified. For instance, incorporating the RMF's "Authorize/Monitor" steps ensures banks periodically review forensic controls. Embedding the Diamond model means correlating cross-incident data (e.g. linking multiple phishing attempts to a single actor). And anchoring in Locard's idea, the framework assumes every transaction leaves traces, so systems must preserve them.

In summary, Nigerian banks can leverage a multi-model approach: use Locard's evidence focus to justify logging, the Diamond model to enrich threat context, and RMF to create a culture of proactive readiness. Regulatory and technological developments (like Nigeria's NDPR and new anti-fraud tools) can further support this. The key is institutionalizing forensic readiness as an ongoing process, not just an afterthought.

Conclusion

Cyber fraud poses a severe threat to Nigerian banks' profitability and reputation. This paper surveyed major forensic readiness models Locard's Exchange Principle, the Diamond Intrusion Model, and the Risk Management Framework and analyzed their applicability to the banking sector. Each model contributes useful perspectives: evidence capture, threat analysis, and structured governance, respectively. We synthesized these insights into a comprehensive DFR framework tailored for Nigeria, emphasizing seven core components (policy, people, process, technology, risk, legal, and monitoring). This framework is designed to leverage existing strengths (security tools, monitoring) while filling gaps in policy and compliance.

For researchers and practitioners, this work highlights that proactivity is essential. Banks should shift from reactive forensics to readiness: routinely preserve logs, train staff in evidence handling, and align forensic processes with law. Future work could empirically test the proposed framework's effectiveness across Nigerian banks or refine it as new threats emerge. Overall, a robust DFR posture will help Nigerian banks detect fraud earlier, conduct swifter investigations, and support legal action when needed, thereby strengthening trust in the financial system.

References

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis*. Center for Cyber Intelligence Analysis and Threat Research. https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains* [White paper]. Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Locard, E. (1930). *The crime scene investigation: A comprehensive guide*. Flammarion.

National Information Technology Development Agency. (2019). *Nigeria Data Protection Regulation 2019*. https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf

Nigeria. (2015). *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015*. https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf

Nigeria Deposit Insurance Corporation. (n.d.). *Annual reports*.

Nigeria Inter-Bank Settlement System. (2020–2021). *NIBSS industry reports*.

Reilly, T., Wren, C. J., & Berry, T. (2010). Cloud computing: Forensic challenges for law enforcement. In *Proceedings of the 5th International Conference for Internet Technology and Secured Transactions (ICITST 2010)*.

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence, 2*(3).

Sachowski, K. (2019). Proactive vs. reactive security strategies in banking. *International Journal of Cyber-Security, 5*(2), 120–130.

Tan, J. (2001). Digital forensic readiness: Data preservation, security, and forensic preparedness. In *Proceedings of the Digital Forensic Research Workshop (DFRWS)*.