

**A Forensic-Centric Security Framework for
Financial Database Systems Addressing
Advanced Threats and Regulatory Demands.**

Introduction.....	3
Context and Background.....	3
Research Problem Statement.....	3
Research Aim and Objectives.....	4
Research Significance.....	5
Literature Review.....	6
Evolution of Database Forensics Investigation Models.....	6
Database Security in Financial Institutions.....	6
Forensic Readiness Frameworks.....	7
International Standards and Regulatory Compliance.....	7
Critical Gaps and Research Positioning.....	8
Literature Summary.....	8
Research Methods and Materials.....	9
Research Methods.....	9
Overview of Research Approach.....	9
Research Strategy: Design Science Research Methodology.....	9
Systematic Literature Review Protocol.....	10
DFRF Architecture and System Design.....	11
Data Analysis and Evaluation Methods.....	11
Materials.....	12
Research Data Sources.....	12
Data Collection Methods and Tools.....	12
Justification of Data Collection Approach.....	12
Ethical Considerations.....	13
Hardware & Software Requirements.....	13
Software and Tools.....	13
Hardware Requirements.....	14
Expected Outcomes & Impact.....	15
Anticipated Results.....	15
Implications.....	15
Limitations.....	15
Project Timeline.....	16
Conclusion.....	17
References.....	18

Introduction

Context and Background

Cores database systems serve as a core component in the banking and financial industry, being the backbone of all of the most important functions, such as the processing of real-time transactions and client portfolio management, as well as regulatory reporting requirements. This complete reliance on databases in managing highly sensitive financial information such as account data, transaction records and personal identifiable information poses an ironic threat: the most sensitive systems to the operation of the institution are the most desirable targets to malicious cyber attackers. The level of threat to financial databases is especially high, which includes not only advanced extrusion attacks such as SQL injection to steal funds but also insiders who have privileged access as well as ransomware attacks that target essential financial documents and advanced persistent threats that steal data quietly during the long term. Financial services have been targeted more than any other industry, with database-related breaches resulting in gigantic financial damages, an average of millions per breach, and lengthy detection times, which are devastating to the response effort.

History Database security in the financial industry has followed the trend of wider technological progressions, starting with the basic access controls to teller systems and administrators, to the strong encryption of data-on-rest to meet a compliance standard such as the PCI DSS and modern tracking of real-time fraud. Although this has been technologically advanced, there exists a critical gap. These security measures have generally been applied individually, resulting in a disjointed defence that is reactive by nature. Such a strategy does not combine proactive forensic preparedness and preventive controls, which will result in the banks being at a basic level with regard to post breach investigations. Such disconnection frequently leads to unacceptable delays in the process of establishing the scope of a compromise, possible contamination of digital evidence, and the inability to quickly attribute an attack, and contributes to an increase in financial loss, regulatory fines, and reputation.

Research Problem Statement

Financial institutions are based on core database systems which are the underlying stores of key data assets, such as transactional records, client account data, and proprietary trading algorithms. The centrality notwithstanding, the systems continue to be attacked by such advanced threats as organized frauds, insider abuse, and sophisticated cyber- attacks that threaten financial integrity and regulatory reputation. Although banks have implemented traditional security mechanisms such as encryption and access controls, they have three key weaknesses: (1) these security mechanisms are by definition reactive, focusing on containing the breach after it has occurred, rather than proactively prepared to respond to a breach in a forensic manner, resulting in investigative timeframes that take excessive time during a critical financial event; (2) the current

forensic strategies against database breaches are ad hoc and not standardized, and are thus unable to provide the evidence standards needed in financial litigation and audit by regulators; and (3) the industry This loophole exposes banks to significant operational, reputational, and financial losses since they are poorly equipped to collect and build admissible digital evidence more efficiently and may threaten legal proceedings, regulatory adherence, and even the quality of the incident response in itself.

Research Aim and Objectives

This study intends to create and test an overall Digital Forensics Readiness Framework (DFRF) of financial databases in particular. This framework will combine active security measures with the readiness to conduct a forensic investigation so that the banks and other financial entities have the ability to quickly identify, capture, store, and analyze admissible digital evidence in the aftermath of a security incident.

- To review in a systematic manner the current database security structures, digital forensic preparedness models, and financial incident investigation processes with the view of identifying key gaps and unique needs of forensic ready database structures in the banking industry.
- To develop a theoretically based DFRF that would combine the best practices of the financial database security, digital forensics, and financial crime incident response. The framework will include built-in features essential to banking, like: financial risk assessment, data classification, at sensitivity ,database firewalls, data-at-rest and in-transit encryption, privileged access, granular monitoring and audit logging to detect fraud, secure data backups and data recovery, incident response plans that are regulatory responsive, forensic preparedness, and security education and awareness.
- To map the proposed DFRF components to the international digital forensics standards (ISO/IEC 27037:2012 on evidence handling, ISO/IEC 27043:2015 on incident investigation, ISO/IEC 27041:2015 on tool assurance, ISO/IEC 27042:2015 on the analysis and interpretation) to confirm regulatory compliance and interoperability and the admissibility of financial evidence in legal and regulatory proceedings.
- To conduct a systematic comparative study of the DFRF in comparison with the available database forensics models and financial security models through specified quality indicators such as comprehensiveness, threats to the banking sector, flexibility to various financial institutions, compliance support, and financial crime investigation.
- The objectives of conducting the research are to synthesize the results of the research, determine whether the proposed DFRF applies to the banking industry, and come up with a set of evidence-based recommendations applicable to the financial practitioners and further research directions in financial database forensics preparedness.

Research Significance

This study fills a serious gap in scholarly literature on financial cybersecurity by offering the Digital Forensics Readiness Framework (DFRF), which, in theory, will transform the highly disjointed aspects of the field, including investigation processes, technical controls, and organizational governance, into one model that integrates forensic preparedness into an active security framework of a bank. Practically speaking, the framework has transformative advantages to the financial sector by allowing objective improvements to operations, including a significantly shorter investigation timeline and reduced investigation cost, and at the same time makes the industry more compliant with strict regulations, by maintaining an effective audit trail and a defensible evidence handling. In the end, these developments can play an important role in securing financial information of the population and reinforcing the base of trust in the whole system of digital banking.

Literature Review

This literature review is a critical review of the current body of scholarly work relating to digital forensics readiness frameworks for database systems, with special reference to the financial and banking sector. The purpose of the review is to identify some of the trends, theoretical bases, technical approaches, and issues that represent the critical gaps in the existing research and justify the proposed Digital Forensics Readiness Framework (DFRF) for financial database systems. The scope covers the literature published mainly in the last five years (2019-2024), which focuses on database forensics investigation models, forensic readiness approaches, database security mechanisms in banking, regulatory compliance approaches and integration of proactive security controls with forensic capabilities.

Evolution of Database Forensics Investigation Models

The field of database forensics has seen a lot of evolution, however it is still very much fragmented and has limited integration with financial sector requirements. Albugmi's in-depth investigation found that there were 57 digital forensic models related to database systems between 2004 and 2020, and forensic readiness was only covered by 1 model, whereas the majority of research focused on reactive investigation processes such as analysis, examination, collection, and preservation. This reactive orientation is a fundamental limitation considering that organizations are not ready to collect evidence systematically until incidents occur. Al-Dhaqm et al. proposed a unified Database Forensic Metamodel that consists of synthesizing various investigation frameworks into a unified and abstract model, which addresses the interoperability and heterogeneity issues in various database management systems. Recent technical contributions have put a step into evidence reconstruction capabilities. Fruhwirt et al.'s work on InnoDB database forensics showed how techniques such as reconstructing data manipulation queries from redo logs can be used to allow investigators to retrace unauthorized database manipulations. However, these technical capabilities are isolated from organizational preparedness frameworks and have no integration with practices for pre-incident security controls that may improve the quality of evidence in financial environments.

Database Security in Financial Institutions

The financial services industry is disproportionately targeted by sophisticated cyber adversaries with database systems being key attack surfaces. Recent research confirms that web application breaches (which often take advantage of backend databases via SQL injection) account for 43% of breaches. The Verizon Data Breach Investigations Report continues to rank financial services as one of the most targeted industries with database-related compromises leading to average losses of millions of dollars and detection time periods lasting more than 200 days. These longer periods of time for detection make financial damage, regulatory penalties, and reputational harm that much worse.

Current database security practices in banking focus on preventive controls such as encryption, privileged access management, database activity monitoring and regulatory compliance such as PCI DSS, GLBA, SOX and Basel III. While such measures offer very basic protection, studies have found deepening gaps including silos for security controls across the organization, overloading of alerting systems which need significant analyst effort to sort eventually, and compliance mechanisms that force security posture rather than forensic evidence characterization. The literature shows that traditional security architectures are still inherently reactive, responding to security incidents after they are compromised, instead of proactively establishing security forensics.

Forensic Readiness Frameworks

Forensic readiness is a proactive paradigm shift from being reactive to incidents to being systematically prepared for digital investigations, but it has not been well developed for financial database environments. Kebande and Ray's seminal work laid down the basic requirements in line with the standards of ISO / IEC 27043:2015 and focused on pre-incident preparation, evidence sources identification, and automatic logging means. Their research proved that forensic readiness should maximize the potential usage of digital evidence while minimizing the costs of the investigation. Research on cloud-based environments postulated forensic readiness models that include terminal information collection, user account tracking and timeline analysis capabilities.

However, current models of forensic readiness have serious limitations in banking database systems. First, they do not have explicit mapping to financial regulatory requirements governing evidence handling and audit trail requirements. Second, existing models fail to adequately account for the unique features of financial databases, such as high transaction volumes, the need for real-time processing and the need for evidence that can meet legal standards for admissibility in financial litigation. Third, the literature shows little integration of forensic readiness processes with existing database security controls and disconnected architectures.

International Standards and Regulatory Compliance

Digital forensics standards are important when dealing with evidence. ISO/IEC 27037:2012 defines procedures related to the identification, collection, acquisition and preservation of digital evidence, so that the integrity of the chain of custody is ensured. ISO/CEI 27043:2015 provides incident investigation principles which apply to organizational situations. Research shows that following these standards has increased the admissibility of the evidence in legal proceedings and examinations by regulators, which is a key requirement for financial institutions which may be facing litigation and regulatory scrutiny.

Financial sector cybersecurity is subject to very strict regulatory requirements such as PCI DSS for payment card data security, GLBA for financial privacy, SOX for financial reporting integrity

and Basel III for operational risk management. Recent studies reflect the fact that regulatory compliance is still fragmented and time consuming and that cybersecurity regulations often lead to confusion about practical implementation of cybersecurity regulations. Critically, current compliance frameworks focus on security controls and risk management not forensic investigation preparedness and there is a disconnect between regulatory compliance and evidence collection preparedness in the event of an incident.

Critical Gaps and Research Positioning

Synthesis of the literature leads to the identification of three basic gaps for the proposed DFRF research. First, the existing models of database forensics are largely reactive, focusing on the post incident investigation process, rather than on proactive forensic preparedness along with preventive security controls. Second, current frameworks for forensic readiness are not geared towards the needs of the financial sector in particular (e.g. regulatory compliance mapping, evidence requirements for financial sector banking litigation). Third, organizational siloing of security controls and forensic capabilities is documented in the literature with no holistic framework that incorporates risk assessment, access controls, encryption, monitoring, incident response and forensic readiness.

The proposed DFRF addresses these lacunae by making three unique contributions. First, it includes proactive forensic readiness as an integral part of security with the ability to collect evidence as part of preventative controls to ensure systematic preparation for investigation. Second, it explicitly maps the components of the framework to international standards for forensic (ISO/IEC 27037, 27043, 27041, 27042) and financial regulatory compliance (PCI DSS, GLBA, SOX) which ensures admissibility of evidence as well as compliance demonstration. Third, the DFRF synthesizes technical database forensics techniques with organizational governance and financial sector contexts and this leads to a holistic framework that overcomes the current fragmentation.

Literature Summary

The reviewed literature establishes that although database forensics and forensic readiness have been the subject of scholarly attention, there are still significant gaps in their application in financial database systems. Current research is still marked by reactive investigation models, technical solutions that do not integrate with organizational preparedness, and lack of integration with financial sector regulatory requirements. The lack of a coherent framework, which brings together proactive forensic readiness with preventive security controls, is a critical lack. The proposed DFRF research is a response to this, as it aims to develop an integrated, theoretically grounded framework that moves this field closer to holistic forensic preparedness for financial database environments.

Research Methods and Materials

Research Methods

Overview of Research Approach

This research follows a qualitative approach under a Design Science Research (DSR) research paradigm to build and test a Digital Forensics Readiness Framework (DFRF) for financial databases. This approach is mandatory for three basic reasons: the explorative nature of framework development requires a profound, contextual understanding beyond quantitative measures; the study involves a synthesis of diverse domains such as database forensics and financial compliance through interpretive analysis; and validation is necessarily based on a qualitative expert assessment of the applicability and effectiveness of the framework. The methodology is ideally suited to explore the central "how" and "why" questions of integrating forensic readiness with security controls, in line with the constructivist epistemology of DSR where the knowledge is built by iteratively creating and refining practical solutions.

Research Strategy: Design Science Research Methodology

This study uses Design Science Research Methodology (DSRM) as the main research strategy in particular in cybersecurity framework development. DSR is eminently suitable for this research for a number of reasons. First, the central objective is to develop a novel artifact (the DFRF) that solves a clearly defined practical problem - the absence of integrated forensic preparedness in the area of financial database security . Second, with DSR, there is a deliberate effort to bridge the gap between the theoretical rigor and practical relevance of a framework in order to ensure that the framework is both academically grounded and industry-applicable. Third, the methodology offers systematic guidelines for artifact design, development, demonstration and evaluation so that scientific validity can be ensured .

The research follows a six phase DSRM process adapted from Peffers et al. and contextualized for forensic framework development:

Phase 1: Problem Identification and Motivation

This phase lays the foundation for the research by identifying the critical gap in the current database forensics approaches - the reactive nature of investigation models and lack of integrated forensic readiness in financial institutions. Through preliminary literature analysis, the following problems were defined in the phase: extended detection times of over 200 days, fragmented security controls and insufficient preparation for evidence collection after the incident in banking environments. The motivation for this comes from the need of the financial sector for quick incident response, demonstrating compliance with regulations, and admissible evidence in litigation.

Phase 2: Objectives of the Solution

This step characterizes clear, quantifiable goals of the DFRF artifact. The framework should: (1) unify proactive forensic preparedness and preventive security controls, (2) offer overall coverage of threats to the financial database and requirement in the investigation, (3) map elements to the international forensic standards (ISO/IEC 27037, 27043, 27041, 27042), and financial rules (PCI DSS, GLBA, SOX), (4) should exhibit versatility to various types of banking institutions and database platforms, and (5) should support systematic gathering of evidence that These are goals that govern further design choices and act as measurement standards.

Phase 3: Design and Development

This step represents the main artifact development stage, which utilizes a methodical search of the literature and comparison of the available models. DFRF is created in a series of syntheses of: (a) database forensics investigation models found in literature, (b) financial database security best practices, (c), and (d) international regulations and standards, and regulatory requirements. This design is done in a thematic integration approach in which the components are arranged in consistent categories (risk assessment, preventive controls, monitoring and logging, incident response, forensic readiness, compliance and governance) that exist based on functional relationships and operational dependencies.

Phase 4: Demonstration

The relevance of the framework is illustrated with the help of elaborate mapping tasks that reveal how the DFRF elements respond to: (1) particular threats of financial databases (SQL injection, insider attacks, ransomware), (2) forensic investigation steps (identification, collection, preservation, analysis), (3) the compliance of major financial standards, and (4) processes of handling evidence according to ISO/IEC 27037:2012 chain of custody principles.

Phase 5: Evaluation

The validation of framework is based on a multi-criteria comparative analysis methodology in which the DFRF is compared to available database forensics models based on a set of quality criteria (described in Data Analysis section below). This qualitative assessment carries the determination on whether or not the artifact does the intended work and is a great step forward regarding the existing methods.

Phase 6: Communication

The outcomes of the research are disseminated by academic publication (this proposal and its final thesis), which produces the theoretical background of the framework, reasons behind its design, the outcomes of the validation process, and suggestions to financial practitioners.

Systematic Literature Review Protocol

The study will use the PRISMA 2020 guidelines on conducting a systematic literature review to guarantee the provision of a transparent and reproducible knowledge synthesis. It is

accomplished by searching four major academic databases on the specific keywords on database forensics, financial security, and forensic preparedness, but only on the recent peer-reviewed materials (2020-2024). Two-step title, abstract, and full-text screening will be conducted using stringent inclusion criteria in order to identify the most meaningful and quality studies. Lastly, thematic analysis will be employed in extracting and synthesizing the data of the eligible studies to determine the best practices and gaps and will directly inform the creation of the proposed Digital Forensics Readiness Framework.

DFRF Architecture and System Design

The suggested Digital Forensics Readiness Framework (DFRF) is organized into five different layers with integrated components within each of them that represents logical operational dependencies. The basic, or Layer 1, provides the background basis with the systematic Risk Assessment and Threat Modeling to detect vulnerabilities in the financial database, as well as the Data Classification and Sensitivity Mapping to classify the information, such as PII and transaction records, by their regulatory and forensic significance.

On this foundation, Layer 2 is composed of the necessary Preventive Security Controls. The technologies level consists of hard technical controls like Database Security Controls to encrypt and use firewall, strong Access Management to regulate privileged user permissions, and complete Monitoring and Audit Logging to produce real-time and secure record of all activity on a database. The framework then proposes its own forensic components in Layer 3 that entails Forensic Readiness Planning to pre-incident preparation as well as Secure Backup and Recovery procedures that are meant to maintain evidence integrity and chain of custody.

The next levels are active management and oversight. The fourth layer is Response and Investigation, which covers the structured Incident Response Planning according to the international standards and formal Forensic Investigation Procedures of evidence gathering and investigations. Lastly Layer 5 touches on Governance and Compliance whereby the framework is required to address the demands of regulatory requirements with specific mapping to regulations such as PCI DSS and GLBA, and sustaining organizational competence with regular Training and Awareness initiatives.

Data Analysis and Evaluation Methods

The framework will be assessed by conducting a systematic comparative evaluation to the existing models in terms of five criteria of quality. The evaluation will be based on Comprehensiveness in regard to all elements of forensic preparedness and Banking Sector specificity, such as its applicability to the financial risks of fraud and support of major regulations such as PCI DSS and GLBA. Additional requirements are the Adaptability of the framework to the needs of the various types and sizes of financial institutions and other database platforms and its Standards Alignment with international standards of digital forensics and

cybersecurity. Lastly, the Assessment will determine the Practical Feasibility of applying the framework in gaming banking settings bearing in mind such factors as resources needs and cost-effectiveness.

Materials

Research Data Sources

The focus of this study is reduced to the analysis of secondary data only that is explained by the fact that the approach was chosen due to the necessity to create a framework based on the synthesis of existing knowledge. To obtain peer-reviewed literature in the field of cybersecurity and digital forensics, the academic background will be formed using major scholarly databases which comprise IEEE Xplore, ACM Digital Library, Scopus and Web of Science. The research is strictly in accordance with international guidelines, namely, the ISO/IEC 27037, 27043, 27041, and 27042 of the digital evidence, and financial standards, such as the PCI DSS, GLBA, and SOX. In order to be useful, the research also includes industry reports like the Verizon Data Breach Investigations Report (DBIR) and other threat analyses in the financial sector, based on which the framework is developed on the basis of the existing operations and available threat intelligence.

Data Collection Methods and Tools

This study is systematic in its data collection and data analysis in order to achieve rigor and transparency. It starts with search in structured databases with specific Boolean operators, which are reported according to PRISMA-S standards, and all the found references are processed in Zotero. Then, the screening and the selection of the studies proceed according to preconceived criteria, and the whole process is visually recorded in a PRISMA flow diagram and tracked in structured spreadsheets. In case of the included studies, data is systematically retrieved with the help of specially designed forms, which record the main features and results in the data, and the obtained material is subjected to the thematic coding procedure that would bring it to the level of the components of the DFRF being developed. Lastly, mapping matrices are used to make a direct connection between regulatory requirements and control objectives to the relevant aspects of the proposed framework through a specific analysis of the international standards.

Justification of Data Collection Approach

The data collection methods and the sources selected are suitable in this study because of a number of reasons. The coverage of the relevant literature is extensive in academic databases (IEEE, ACM, Scopus, Web of Science), and it guarantees systematic finding of the existing database forensics models, forensic preparedness models, and financial security studies, . The multi-database strategy reduces the publication bias and covers the variation in points of view. The documents of the international standards are authoritative documents about the best practices

in digital forensics that have validated procedures that can guarantee the DFRF conformity to the known professional standards. Regulatory frameworks (PCI DSS, GLBA, SOX) are mandatory provisions of financial institutions and hence their implementation is a crucial element to applicability in the framework. Transparency, reproducibility, and rigor in synthesizing knowledge are ensured by the systematic literature review methodology in accordance with PRISMA 2020, which deal with possible bias in the selection and interpretation of the studies, .

Ethical Considerations

In this study, only secondary data, i.e., data published publicly (published literature, standards documents, regulatory specifications, public technical reports), will be used, thus eliminating human subjects research ethical concerns and ethical issues concerning primary data collection. No personal information, confidential documents, or proprietary content is accessed and examined. All the literature references are properly cited according to the principles of academic integrity, and there are no cases of copyright abuse due to adequate use of quotations, paraphrasing, and citations. The study adheres to the university policies of research ethics that regulate the analysis of secondary data and a literature-based research. Since the research constructs a theoretical framework, which is not executed in the operational banking setting or allowed access to financial institution systems, data protection rules (GDPR, financial privacy laws), are not applicable to the research process, but the research design clearly reflects the principles of privacy and data protection that should be considered in the implementation context in the future.

Hardware & Software Requirements

Software and Tools

This research will employ a practical suite of easily accessible software tools for data analysis, documentation, and visualization.

Software Tool	Primary Function	Key Features / Use Case
Microsoft Excel	Qualitative Data Analysis	Performing thematic coding, organizing literature extracts, and creating comparative evaluation matrices.
Zotero 6.0	Reference Management	Organizing bibliographic data, collecting sources from databases, and generating citations.
Microsoft Word	Documentation	Writing the systematic literature review, framework design, and final dissertation document.

Draw.io	Diagramming & Visualization	Creating the DFRF architecture diagrams and process flowcharts to illustrate component relationships.
-------------------------	-----------------------------	---

Hardware Requirements

The proposed research requires only a standard computing setup, as its activities are confined to literature review and analysis rather than computational modeling.

Requirement Category	Specification	Purpose
Processing & Memory	Multi-core processor, 8GB RAM	Adequate performance for running Microsoft Office applications (Word, Excel) and multiple browser tabs simultaneously.
Storage	500GB (or equivalent)	Sufficient space for storing academic papers, software installers, and all research documentation.
Peripheral	Reliable Internet Connection	Essential for accessing online academic databases, digital libraries, and software tools.

Expected Outcomes & Impact

Anticipated Results

The Digital Forensics Readiness Framework (DF RF) is suggested to be elaborated and tested to become a more secure relational database management system. It is hoped that a detailed framework will be designed successfully, whereby, integrated security features, which include, but are not limited to risk assessment, data classification, encryption protocols, database firewalls, and monitoring systems, will be integrated. With the comparative analysis against the existing models, better coverage of crucial security dimensions is anticipated to be shown thus filling the gaps that have been identified on forensic preparedness. Through incorporation of proactive and reactive elements, the incident response capacity is likely to be enhanced in an impressive manner and the important forensic evidence is expected to be saved. The sparse technical documentation, implementation guidelines, and best practice recommendations are likely to be generated so that the practical deployment on a variety of database platforms can occur and the efficacy of the framework should be justified within a framework of systematic comparison to the established standards.

Implications

The Digital Forensics Readiness Framework (DFRF) has a considerable implication on several areas of operation. Hypothetically, it contributes to the development of knowledge in digital forensics by creating a new paradigm in which forensic investigation is reset as an active part of the security strategy, which further adds value to the academic discourse. It offers better threat detection, efficient incident response, and overall recovery to the practitioners, especially to data-intensive industries such as the finance and health sector using a single approach that minimizes the complexity of implementation. To the research world, the systematized and replicable methodology is provided to integrate fragmented methodologies, which can be applied to emerging technologies, and the combination of technical measures and staff education of the framework meets the issues of human-technology gap, which present the fundamentals of adaptation in the future.

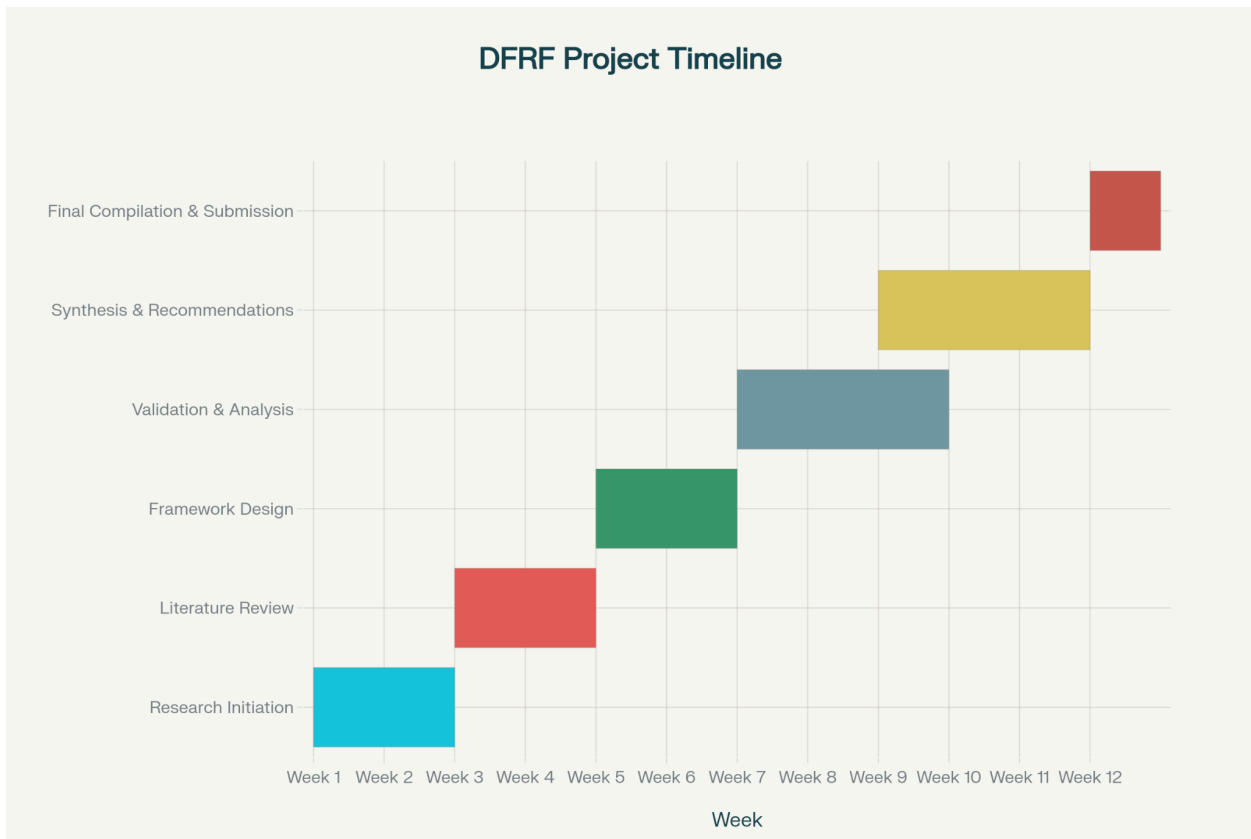
Limitations

It can be said that several limitations are worth recognition in order to be academically rigorous. The area covered in this research will majorly rely on traditional relational database architecture, the newer forms of database architecture like graph databases, NoSQL databases or blockchain based databases might necessitate a notable change in the framework. The validation is done against the existing models and norms and not on a big scale as applied to real world situations in many organizations and this may restrict the overall practical applicability evaluation. The study schedule might not allow an extensive testing on all the major DBMS platforms. Also, the practicality of the framework is heavily reliant on the commitment of the organization to the

implementation process and the compliance of employees with security measures, which cannot be entirely controlled by technical means. The contextual challenges to the applicability of universal frameworks are also geographic and jurisdictional differences in regulatory compliance requirements and data protection laws. Future studies ought to deal with validation of large scale real world implementation, testing on a variety of organizational contexts and other emerging database technologies, and testing framework efficacy in a hybrid cloud and distributed computing environment.

Project Timeline

The 12-week research project is structured into six distinct phases, each aligned with the research objectives for developing a comprehensive Framework for financial database systems.



Project Phases

Phase 1: Research Initiation (Week 1 - 2): Determines the foundation of the project by defining the scope of the research, defining the methodology, making necessary approvals and establishing communication infrastructure. The research protocol and the project charter are the deliverables.

Phase 2: Literature Review (Week 3-4): Regularly carries out methodical research on the available database protection models, models of digital forensics, procedures of financial incidents as well as the needs of banking sector. Measures important lapses in present methods and records research bases.

Phase 3: Design of the Framework (Weeks 5-6): Develops the end-to-end DFRF capability by designing the integrated features (financial risk analysis, data classification, database firewalls, encryption, privilege access management), the mapping to the standards ISO/IEC 27037, 27043, 27041, 27042 and the alignment of the NIST CSF 2.0 and ISO 27001:2022.

Phase 4: Validation and Analysis (Week 7- 9): Conducts formal comparative study of DFRF to existing models, assesses comprehensiveness, threats to banking model, adaptability, compliance support and evidence admissibility criteria. Indicates the effectiveness of documents and validation results.

Synthesis & Recommendations (Weeks 10-11) Phase 5: Summarizes all the research results, invents recommendations to the financial practitioners which are evidence-based, creates further research directions, and prepares overall implications analysis.

Phase 6: Final Literature Review and submission (Week 12): Synthesizes all the research parts into a unified dissertation, provides the final editing and quality control and sends the final version of the dissertation.

Conclusion

This research proposal has set a clear-cut roadmap to the development of an innovative Digital Forensics Readiness Framework (DFRF) that can fill the most important gap between proactive and forensic investigation of financial database systems. The described approach, based on Design science research, represents a strict route to build and justify the multi-layered DFRF that is aimed to consolidate prophylactic measures with the forensic preparedness measures that are clearly defined in accordance with the needs of the financial sphere. Successful implementation of this proposed work in the following dissertation will thus provide a drawn and tested structure, and presents the financial institutions with an effective, standards-based solution to their cyber resilience, evidence admissibility, and greatly improve the results of incident response.

References

1. A. Albugmi, "Digital Forensics Readiness Framework (DFRF) to Secure Database Systems," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13732-13740, 2024. doi: 10.48084/etasr.7116
2. A. Al-Dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. A. Mohammed, "A Unified Forensic Model Applicable to the Database Forensics Field," *Electronics*, vol. 11, no. 9, p. 1347, Apr. 2022. doi: 10.3390/electronics11091347
3. A. Al-Dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. A. Mohammed, "Development and validation of a Database Forensic Metamodel (DBFM)," *PLoS ONE*, vol. 12, no. 2, p. e0170793, Feb. 2017. doi: 10.1371/journal.pone.0170793
4. C. Frühwirth, P. Kieseberg, P. Schrittwieser, M. Huber, and E. R. Weippl, "Digital Forensic InnoDB Database Engine for Employee Performance Appraisal Application," in *E3S Web of Conferences*, vol. 125, p. 25002, 2019. doi: 10.1051/e3sconf/201912525002
5. O. E. Ajayi, "Securing financial data storage: A review of cybersecurity challenges and solutions," *International Journal of Science and Research Archive*, vol. 11, no. 1, pp. 2543-2553, Feb. 2024. doi: 10.30574/ijrsra.2024.11.1.0267
6. The 2020 Data Breach Investigations Report – a CSO's perspective. *Forensic Science International: Digital Investigation*, vol. 33, Jun. 2020. doi: 10.1016/j.fsidi.2020.301012
7. R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. R. C. Fontaine, A. Filippoupolitis, and E. Roesch, "After the Breach: Incident Response within Enterprises," arXiv preprint arXiv:2406.07559, Jun. 2024.
8. O. E. Ajayi, "A critical review of emerging cybersecurity threats in financial technologies," *International Journal of Science and Research Archive*, vol. 11, no. 2, pp. 2996-3004, Feb. 2024. doi: 10.30574/ijrsra.2024.11.2.0284
9. S. K. Sharma, M. Gupta, and P. Gupta, "Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review," arXiv preprint arXiv:2503.22710, Mar. 2025.
10. M. T. Khurma and A. Y. Dalalah, "Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded U.S. Companies," *Future Internet*, vol. 16, no. 6, p. 201, Jun. 2024. doi: 10.3390/fi16060201

11. O. E. Ajayi, "Evaluation of the cyber security models implemented across common attack vectors: A review of literature," *World Journal of Advanced Engineering Technology and Sciences*, vol. 11, no. 1, pp. 285-296, Jan. 2024. doi: 10.30574/wjaets.2024.11.1.0023
12. R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. R. C. Fontaine, A. Filippoupolitis, and E. Roesch, "After the Breach: Incident Response within Enterprises," arXiv preprint arXiv:2406.07559, Jun. 2024.
13. A. L. Opdahl, M. G. Jaatun, and G. Sindre, "Weathering the storm: examining how organisations navigate the sea of cybersecurity regulations," *Information Systems Frontiers*, Apr. 2024. doi: 10.1080/0960085X.2024.2345867
14. M. S. Alkahtani and A. M. Cherif, "The Role of Deep Learning in Advancing Proactive Cybersecurity Measures for Smart Grid Networks: A Survey," arXiv preprint arXiv:2401.05896, Jan. 2024.
15. M. A. Rahman, M. M. Hossain, M. S. Islam, and M. A. Hossain, "Securing the Future: Proactive Threat Hunting for Sustainable IoT Ecosystems," arXiv preprint arXiv:2406.14804, Jun. 2024.
16. G. R. KEBANDE and I. Ray, "Adding Digital Forensic Readiness as a Security Component to the IoT Domain," in *Proceedings of the 11th EAI International Conference on Digital Forensics & Cyber Crime*, Feb. 2018, pp. 1-15. doi: 10.1007/978-3-030-05487-8_1
17. G. R. KEBANDE and I. Ray, "Functional Requirements for Adding Digital Forensic Readiness as a Security Component in IoT Environments," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 2, pp. 420-429, Mar. 2018. doi: 10.18517/ijaseit.8.2.2121
18. H.-J. Kim, S.-H. Lee, and J.-I. Lim, "Research on Digital Forensic Readiness Design in a Cloud Computing-Based Smart Work Environment," *Sustainability*, vol. 10, no. 4, p. 1203, Apr. 2018. doi: 10.3390/su10041203
19. N. A. Jaber, "Criminal Investigation of Financial Crimes," *Journal of Forensic Investigation*, vol. 9, no. 1, pp. 1-9, 2021.
20. K. Ciftci, "The standard of forensic report veracity in criminal proceedings," *Khazar Journal of Humanities and Social Sciences*, vol. 24, no. 4, pp. 94-113, Dec. 2021. doi: 10.5782/2223-2621.2021.24.4.94
21. S. A. Almula, M. N. A. Bakar, Z. A. Zukarnain, and A. Udzir, "A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1-16, Feb. 2022. doi: 10.1155/2022/8002963

22. R. Alnanih and O. Ormandjieva, "Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014," *JUITA: Jurnal Informatika*, vol. 10, no. 1, pp. 89-98, May 2022.
23. A. Kurniawan and I. Riadi, "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework," *Information Technology Journal of UNEJ*, vol. 6, no. 1, pp. 27-34, Feb. 2022.
24. D. Carvalho and S. Proenca, "The Value Connotation of Evidence Evaluation on Forensic Conclusions," *International Journal of Education and Applied Business*, vol. 19, pp. 104-111, 2021.
25. H. S. Al-Ashhab, M. S. Al-Ashhab, N. D. A. Halim, S. M. Drus, and N. Mustapha, "Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 Framework," *La Multiapp*, Aug. 2024.
26. S. Alqahtani, E. E. Eghan, and J. Rilling, "Risk-Based Cybersecurity Compliance Assessment System (RC2AS)," *Applied Sciences*, vol. 13, no. 10, p. 6145, May 2023. doi: 10.3390/app13106145