Faculty of Computing and Informatics

Department of Computer Science

Design of a Model for Augmenting Digital Forensics into Information System Audit in The Financial Sector

Thesis

Submitted in the fulfillment of the requirements for the degree of

Master of Computer Science

at

Namibia University of Science and Technology

Submitted by: Ericky Iipumbu

Student Number: 212069594

Supervisor: Mr Isaac Nhamu

Co-Supervisor: Dr Mercy Bere-Chitauro

Date of Submission: September 2024

METADATA

TITLE: Mr

STUDENT NAME: Ericky Iipumbu

SUPERVISOR: Mr Isaac Nhamu

CO-SUPERVISOR: Dr Mercy Chitauro

DEPARTMENT: Cyber Security

QUALIFICATION: Master of Computer Science

SPECIALISATION: Digital Forensics

STUDY TITLE: Design of a Model for Augmenting Digital Forensics into Information System Audit in the Financial Sector

MAIN KNOWLEDGE AREA: Digital Forensics, Information System Audit

KEYWORDS: Information system audit, digital forensics, cyber threats, internal controls

TYPE OF RESEARCH: Action Research

METHODOLOGY: Design Science Research (DSR) methodology

STATUS: Thesis (Final)

SITE: Namibia University of Science and Technology

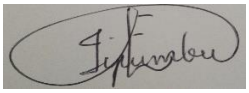
DOCUMENT DATE: October 2024

SPONSOR (or Cluster/ Research lab): Namibia University of Science and Technology

DECLARATION

I, Ericky Iipumbu, hereby declare that the work contained in the proposal for the degree Master of Computer Science project, entitled:

"Design of a Model for Augmenting Digital Forensics into Information System Audit in the Financial Sector" is an original work, and I have not previously, in its entirety or part, submitted it at any university or other higher education institution for the award of a degree. I further declare that I will fully acknowledge any sources of information I will use for the research in accordance with the institution's rules.

Signature:  Date: _____September 2024_____

SIGNATURE OF THE SUPERVISOR

I, __Isaac Nhamu_____, herewith declare that I accept this thesis for my supervision

Signature: _____ Date: ____Sept 2024_____

SIGNATURE OF THE CO-SUPERVISOR

I, Dr Mercy Chitauro_____, herewith declare that I accept this thesis for my supervision

Signature: _____ Date: 14/10/2024_____

DEDICATION

This thesis is dedicated to AFROSAI-E for their unwavering support and guidance throughout. It is also dedicated to SAI Namibia, SAI South Africa, SAI Gambia, SAI Uganda, SAI Kenya, SAI Zambia, and SAI Norway for their continuous support and their readiness to establish a forensic audit department in their respective countries as a result of this study.

ACKNOWLEDGMENTS

Firstly, I would like to thank and praise the Almighty God for his loving kindness, great mercy, and guidance throughout the academic years.

Secondly, I would like to thank my supervisors, Dr. Mercy Chitauro and Mr. Isaac Nhamu, for their perseverance, guidance, and continuous support during this study. It is because of your efforts and guidance that I managed to accomplish this milestone.

Lastly, I would like to thank the officials and experts who participated in this study. Their participation helped me achieve the study objectives.

Abstract

Audits of information systems demonstrate whether IT controls are effective in protecting company property, ensuring data integrity, and aligning with the organisation's overarching objectives. Information System auditors evaluate all components of financial and business controls, including information technology systems and physical and logical security protocols. As long as cyberattacks continue to occur in the financial sector, it is increasingly important to take robust measures to ensure the integrity and security of information systems. New models that incorporate digital forensics methods into the audit process have emerged as a result of the fact that traditional audit processes frequently fail to meet evolving objectives. Based on the findings of a systematic literature review that demonstrated that the evidence-gathering techniques employed in information system audits are inadequate for assessing the efficacy of internal controls, this study proposes a model that integrates digital forensics into information system auditing that was designed using Design Science Research techniques. The model is envisaged to improve the information system auditing process by augmenting digital forensics processes into information system auditing. The model incorporates key digital forensic components embedded into audit procedures to enhance the accuracy and reliability of evidence collection, ensure the integrity and authenticity of digital evidence, and facilitate a more detailed analysis of audit data. The inclusion of these digital forensic techniques is essential for addressing complex cyber threats and fraud within the financial sector, providing auditors with robust tools to conduct more thorough and defensible investigations, and ensuring compliance with industry standards and regulatory requirements. In summary, the proposed approach offers a structured approach to the integration of digital forensic methodologies into the auditing process and establishes guidelines, in a manner that ensures audit opinions for information systems auditors are unqualified rather than qualified and disclaimer.

Keywords: Information system audit, digital forensics, cyber threats, internal controls

PUBLICATIONS

Iipumbu, Ericky and Nhamu, Isaac and Chitauro, Mercy, A Comparative Analysis of Information Systems Audit and Digital Forensics Processes (November 29, 2023). Available at SSRN: https://ssrn.com/abstract=4648699 or http://dx.doi.org/10.2139/ssrn.4648699

Iipumbu, Ericky and Nhamu, Isaac and Chitauro, Mercy, Factors Affecting Information Systems Audit Conclusion (November 29, 2023). Available at SSRN: https://ssrn.com/abstract=4648690 or http://dx.doi.org/10.2139/ssrn.4648690

Contents

Abstract v
Table of Figures xi
List of tables xii
CHAPTER 1: INTRODUCTION AND BACKGROUND OF THE STUDY 1
1.0 Introduction 1
1.1 Background of the study 1
1.2 Problem Statement 2
1.3 Research Objectives 3
1.3.1 Research Main Objective 3
1.3.2 Research sub-objectives: 3
1.3.3 Research Questions 3
1.4 Significance of the study 4
1.5 Motivation of the Research 4
1.6 Delineation 5
1.7 Assumptions 5
1.8 Thesis Outline 5
1.9 Chapter Summary 6
CHAPTER 2: LITERATURE REVIEW 7
2.0 Introduction 7
2.1 Digital Forensics Process 7
2.1.1 Collection of Digital Evidence 8
2.1.2 Chain of Custody Management 9
2.1.3 Preservation of Digital Evidence 9
2.1.4 Digital Forensic Imaging 10
2.1.5 Examination of Digital Evidence 11
2.1.5 Analysis of Digital Evidence 12
2.1.6 Reporting and Documentation 13
2.1.7. Presentation of Findings 13
2.2 Bridging the Gap: The Synergy between Digital Forensics and Information System Audit 14
2.2.1 Importance of Digital Forensics in Information System Audit 14
2.2.2 Key Areas of Synergy 15
2.3 Information System Audit 16

2.3.1 Information System Audit Process 17
i. Planning 18
ii. Fieldwork and Documentation Phase 19
iii. Reporting and Follow-up Phase 19
2.3.2 Evidence-gathering techniques 19
i. Inspection 20
ii. Observation 21
iii. Inquiry 21
iv. Confirmation 21
v. Recalculation 22
vi. Re-performance 22
vii. Analytical Reviews 22
2.4 The use of Computer Aided Audit Techniques (CAATS) when conducting an IS audit 23
2.5 Background on Financial Statement Auditing 24
2.6 The Concept of Audit Evidence 25
2.7 Characteristics of Audit Evidence 26
2.8 Audit Procedures to Obtain Audit Evidence 27
2.9 Techniques of Collecting Evidence 28
2.10 Standards and Frameworks Used in Information System Auditing 30
2.10.1 ISACA Standards and Guidelines 30
2.10.2 COBIT Framework 31
2.10.3 NIST Frameworks 31
2.10.4 ISO/IEC Standards 32
2.11 Enhancing IS Audit Effectiveness through Standards and Frameworks 32
2.12 Addressed objectives 33
2.13 Research Finding 35
2.14 Model Selected Components 36
i. Preservation of Evidence Integrity 36
ii. Recovery of Deleted or Concealed Data 36
iii. Comprehensive Investigation Capabilities 36
iv. Supports Legal Compliance 36
v. Detecting Insider Threats 37
vi. Enhanced Incident Response 37

vii. Risk Mitigation and Prevention 37
viii. Digital Evidence Handling 37
2.15 Integration of Digital Forensic Components in Information System Audits: Ensuring Security and Evidence Validity 38
2.16 Optimizing Information System Audits with Integrated Digital Forensics 38
2.17 Chapter Summary 39
CHAPTER 3: RESEARCH METHODOLOGY 40
SECTION A: GENERAL SECTION 40
3.0 Introduction 40
3.1 Research Paradigm 40
3.2 Design Science Research Strategy Overview 41
3.3 Data Collection Techniques and Instruments 42
3.4 Data Analysis 43
SECTIION B: MODEL DESIGN 43
3.5 Model design 43
3.5.1 The Model's Rationale 44
3.6 Phase 1: Identification of the problem 45
3.7 Phase 2: Definition of objectives for a solution 46
3.8 Phase 3: Design and development 46
3.8.1 Model Selected Components 46
3.8.2 Information System Auditing Phases 47
3.8.3 Proposed Integrative Forensic Information System Audit Model (IFISAM) 48
3.9 Chapter Summary 51
CHAPTER 4: DEMONSTRATION AND EVALUATION 52
4.0 Introduction 52
4.1 Phase 4 Demonstration 52
4.1.1 Hypothetical Scenario 52
1. Planning Phase 53
2. Fieldwork and Documentation Phase 53
1. Imaging 56
2. Chain of Custody 56
3. Analysis 56
4. Document the Findings 56

4.2 Phase 5 Evaluation 57
4.2.1 Evaluation Criteria 57
4.2.2 Expert reviews 58
4.2.3 Model Evaluation Tool 59
4.2.4 Biographical information of the reviewers 59
4.2.5 Evaluation findings 61
i. Overall Performance 62
ii. Recommendations 62
4.2.6 Validated Model 63
4.3 Phase 6 Communication 65
4.4 Chapter Summary 65
CHAPTER 5: CONCLUSION AND RECOMMENDATIONS 66
5.0 Introduction 66
5.1 Achievements of the Study Objectives 66
5.2 Research Contributions 68
5.3 Limitations 69
5.3.1 Shortage of Literature on Information System Audit 69
5.4 Future Considerations 69
5.6.1 Optimal Utilisation of Hypothetical Scenarios 70
5.7 Concluding Remarks 71
References 72
APPENDIX A: EXPERT REVIEW QUESTIONNAIRE 84
SECTION A: Demographic 84
SECTION B: PRESENTATION 85
SECTION C: QUESTIONS AFTER PRESENTATIONS 85
SECTION D: DISCUSSIONS 86
APPENDIX B: Selected publications used in answering research questions one and two 87

Table of Figures

Figure 1: The digital forensics process (Kent et al., 2006; Alazab et al., 2023; Yusoff et al., 2011). 8
Figure 2: Typical audit process phases (ISACA, 2019) 17
Figure 3: IS Audit process in detail (ISACA,2019)..... 18
Figure 4: Evidence-gathering Techniques (ISACA, 2019; AFROSAI-E, 2017) 20
Figure 5: CAATs (Wicaksono et al., 2018) 24
Figure 6: The audit planning procedure (AICPA, 2012). 25
Figure 7: Design science research methodology (Peffers et al. (2007) 42
Figure 8: Used Design Science Research by Peffers et al. (2007) 45
Figure 9: Typical Information System Audit Process (ISACA,2019) 47
Figure 10: shows how the fieldwork phase will be modified 48
Figure 11: Proposed Integrative Forensic Information System Audit Model (IFISAM) 48
Figure 12: Scale of agreement 62
Figure 13: Expert-validated model 64

List of tables

Table 1:IS Audit Evidence Characteristics (AICPA, 2012; Brown-Liburd & Vasarhelyi, 2015; ISACA, 2019; AFROSAI-E, 2017). 27
Table 2:Techniques of Collecting ISA Evidence (AICPA, 2012; Brown-Liburd, & Vasarhelyi, 2015; ISACA, 2019; AFROSAI-E, 2017) 28
Table 3:Participants Biography 60
Table 4: Addressed objectives 71

Abbreviations/Acronyms

AICPA	American Institute of Certified Public Accountants
AFROSAI-E	African Organisation of English-speaking Supreme Audit Institutions
APO	Aligning, Planning, and Organizing
BACC	Bachelor of Accounting
BAI	Building, Acquiring, and Implementing
CAATs	Computer-Assisted Audit Techniques
CAWFE	Certified Advanced Windows Forensic Examiner
CFE	Certified Forensic Examiner
CIA	Confidentiality, Integrity, Availability
CISA	Certified Information Systems Auditor
CMA	Certified Management Accountant
CRISC	Certified in Risk and Information Systems Control
DF	Digital Forensics
DSS	Delivering, Service, and Support
DSR	Design Science Research
FCCA	Fellow Chartered and Certified Accountant
FZICA	Fellow Member of Zambia Institute of Chartered Accountants
GDPR	General Data Protection Regulation
GIAC	Global Information Assurance Certification
IAASB	International Auditing and Assurance Standards Board
IEC	International Electrotechnical Commission
IFAC	International Federation of Accountants
IFISAM	Integrative Forensic Information System Audit Model
INTOSAI	International Organization of Supreme Audit Institutions
ISA	Information System Auditing
ISAP	Information Systems Audit Professional
ISMS	Information Security Management System
ISO	International Organization for Standardisation

IS	Information Systems
ISSA	Information Systems Security Association
IT	Information Technology
MBL	Master of Business Leadership
MEA	Monitoring, Evaluating, and Assessing
NIST	National Institute of Standards and Technology
PCAOB	Public Company Accounting Oversight Board
PCI DSS	Payment Card Industry Data Security Standard
PF	Privacy Framework
RAIT	Risk Arising from IT
RMF	Risk Management Framework
SAI	Supreme Audit Institution
SAI	Supreme Audit Institutions
Sec	Security
VM	Virtual Machines

CHAPTER 1: INTRODUCTION AND BACKGROUND OF THE STUDY

1.0 Introduction

This chapter gives an overview of the research background by presenting current developments in Information System Audit. It outlines the problem statement and the purpose of the study. The chapter further highlights the overall objectives and research questions for the study. A brief research methodology used to meet the research objectives is also introduced in this chapter. Lastly, the chapter concludes with the research overview.

1.1 Background of the study

The financial industry's information systems auditing (ISA) is a dynamic process that necessitates innovative solutions to the increasing challenges posed by sophisticated intrusions. ISA must now more than ever guarantee the availability, confidentiality, and integrity of data as companies increasingly rely on digital technologies. However, the identification and prevention of sophisticated cyber-attacks are frequently inadequately addressed by existing procedures and computer-assisted audit tools (CAATs) (Whitman and Mattord, 2018; Krombholz et al., 2015; Information Systems Audit and Control Association [ISACA], 2020; Mantha et al., 2021). Unidentified security vulnerabilities pose a threat to corporate entities, and they also undermine public confidence in financial institutions. The objective of this study is to investigate the development of a model that will improve digital forensics within the ISA framework, thereby bridging the distance between the requirements of the modern financial sector and traditional auditing methods. Auditors are capable of gathering and evaluating digital evidence at a faster pace when they combine digital forensics concepts with cutting-edge technology (Casey, 2011). The objectives of this study are to improve the efficacy of Information System Auditing (ISA) processes, increase the precision of the data collected by IS auditors, and simplify the precise evaluation of information system security in the financial sector.

Numerous forms of cybercrime frequently target the financial sector due to its significance to the global economy's stability (PwC, 2022). Insider trading, money laundering, ransomware attacks, and data exposures are among the ever-evolving hazards. To protect their assets and the financial

security of their clients, financial institutions must implement cutting-edge technologies and processes.

In an era in which data is a form of currency and trust is essential, it is no longer feasible to respond promptly and aggressively to threats and breaches (Javed et al., 2022). In the contemporary digital era, it may be challenging to distinguish between digital forensics and security. This approach of integration of digital forensics into the Information System (IS) audit process within the financial sector is a ground-breaking initiative that aims to equip financial institutions with the tools necessary to remain at the forefront of the industry (Davies., 2022). It is an appeal to financial institutions to embrace innovation, resilience, and a firm commitment to the preservation of the integrity of financial systems in the future.

According to Springmi (2017), as cited in Alagi, Turulja, and Bajgori (2021), an information systems audit is a methodical process that evaluates the effectiveness and efficiency of information technologies and information systems in supporting business objectives, as well as the management and control procedures in place at various hierarchical levels. In contrast, "digital forensics" (DF) is a subfield of forensic science that is dedicated to the identification, acquisition, processing, analysis, and reporting of electronically stored data (Ahn and Lee, 2018). Digital forensics support is indispensable for law enforcement investigations, as electronic evidence is implicated in nearly all unlawful activities. Recognising, controlling, and eliminating cyber hazards by conducting assessments of suspected attacks is a critical component of digital forensics investigations and a critical component of the financial sector, according to the authors.

1.2 Problem Statement

Information systems auditing (ISA) is a critical process in business informatics. However, process and computer-aided audit tools (CAATs) are not enough to detect complex cyber threats (Whitman & Mattord 2018). Moreover, relying solely on automated auditing tools can lead to undetected security breaches, potentially compromising data confidentiality, integrity, and availability (Krombholz et al., 2015). Therefore, ISACA (2020), and Mantha et al. (2021) emphasised the importance of addressing the limitations of CAATs and the need for augmenting

traditional auditing methods with advanced techniques to mitigate the increased risk of cyberattacks. This can affect the overall effectiveness of the ISA process, and the validity of evidence collected by IS auditors, potentially leading to inaccurate system assessments.

1.3 Research Objectives

1.3.1 Research Main Objective

To develop a model that seamlessly integrates digital forensics into the information systems audit process in the financial sector, with the goal of upholding confidentiality, integrity, and availability. The model aims to ensure compliance with information technology activities aligned with company policies, industry best practices, and government laws and regulations. The model also intends to validate the evidence gathered during the audit by information systems auditors.

1.3.2 Research sub-objectives:

1. To analyse how the current steps employed in the information system audit process guarantee the CIA of information systems and validate the evidence collected.
2. To evaluate the standards used by IS auditors when conducting IS audits.
3. To design a model that integrates digital forensics into IS audit to ensure the confidentiality, integrity, and availability of information systems, as well as the validity of the evidence collected.
4. To evaluate the proposed digital forensics-infused information systems audit process model.

1.3.3 Research Questions

The following research questions were answered:

1. What are the existing steps within the information system audit process that guarantee the CIA of the information system and validate the evidence collected?
2. What are the key standards and frameworks commonly used by IS auditors during the IS audit process, and how do these standards contribute to the effectiveness and reliability of IS audit activities?
3. What are the model components and how can they work together to ensure the confidentiality, integrity, and availability of information systems, as well as the validity of the evidence collected?

4. How does the proposed model ensure the CIA of information and the validity of the evidence collected?

1.4 Significance of the study

The study's goal was to advance the techniques of information system auditing. The procedures that ensure the integrity, confidentiality, and availability of information systems (CIA) were particularly beneficial. Additionally, they verified the accuracy of the data collected throughout the audit. The knowledge that was acquired was instrumental in enhancing the security and efficiency of information systems. In addition, the primary objective of this investigation was to extensively evaluate the standards that information systems (IS) auditors employ during their IS audits. This study sought to improve the general effectiveness, uniformity, and quality of IS auditing procedures by introducing significant new information. Moreover, the initiative aims to advance academics by establishing a novel paradigm for the integration of digital forensics into information system (IS) audits. This architecture is designed to enhance the security and dependability of information systems by ensuring the confidentiality, integrity, and availability of data. Additionally, the data collected is to be rendered more reliable. The methodology previously described was believed to provide a methodical framework that would enhance the effectiveness and scope of information systems auditing operations. Ultimately, the objective of this study was to advance the field of academia by conducting a thorough assessment of the sustainability and efficacy of the proposed method for incorporating digital forensics into the information systems audit process. The study's findings provide critical insights into the potential repercussions of implementing this paradigm to improve the security of information systems and auditing procedures.

1.5 Motivation of the Research

The rising complexity and frequency of financial cybercrimes and data breaches motivated the researchers to conduct the study "Design a Model to Integrate Digital Forensics into Information System Audit in the Financial Sector". In the financial sector, where sensitive financial data and transactions are heavily targeted, traditional audit approaches frequently fail to discover sophisticated fraud or security risks. Integrating digital forensics into the information system

auditing process is intended to improve the ability to detect, investigate, and respond to these advanced threats. By creating a model adapted exclusively for the financial sector, the study addresses the crucial need for more robust and proactive audit processes, guaranteeing that financial institutions can better protect their data and comply with regulatory obligations.

1.6 Delineation

The goal of the research was to establish a paradigm that integrated digital forensics into information system audits to enhance the efficiency and effectiveness of the information system audit process ensures the confidentiality, integrity, availability of information, and IT operations adhere to pertinent corporate policies, industry best practices, and legal and regulatory requirements. The investigation was limited to the integration of digital forensics into the Information System (IS) audit process within the financial sector, despite the fact that auditing is a complex and extensive subject found not only in the financial sector becausethe financial sector is significantly more vulnerable to cybercrime and fraud, requires rigorous regulatory compliance mandates, and the essential necessity for operational continuity usually because it is part of Nation's Critical Infrastructure. The research focused on the financial sector, although the established model can be extended for application in other businesses facing comparable risk and compliance issues.

1.7 Assumptions

The study is predicated on the following assumptions: Digital forensic methods can be integrated in information system auditing to facilitate the search for evidence of criminal activity and security violations to enhance conventional audit procedures and methodologies.

1.8 Thesis Outline

The rest of the thesis is arranged as follows:

Chapter 2: Addresses research objectives one and two using a systematic and targeted literature review. The chapter also discussed the digital forensics components to be integrated into the information system audit process.

Chapter 3: Delineates the design science research (DSR) methodology employed to construct the Proposed Integrative Forensic Information System Audit Model. The DSR encompasses problem

identification, objective definition, and design, which are elaborated upon here, whereas demonstration and evaluation are addressed in a subsequent chapter.
Chapter 4: Chapter 4 presents the demonstration and evaluation of the model established in Chapter 3. This chapter demonstrates the application of the Proposed Integrative Forensic Information System Audit Model (IFISAM) in actual contexts, highlighting its functionality and significance to the study aims.
Chapter 5: Constitutes the concluding section of the study, summarising the principal findings and debates from the other chapters. It underscores the importance of the Proposed Integrative Forensic Information System Audit Model (IFISAM) and delineates the research's contributions to practitioners and future investigations.

1.9 Chapter Summary

This chapter presented an overview of the study's backdrop, encompassing the background material essential for comprehending the research's scope and purpose. It delineated the problem statement, elucidating the particular obstacles and deficiencies in incorporating digital forensics into information system audits within the banking sector. The chapter described the study's objectives, which seek to formulate a model that improves the efficacy of the IS audit process through the integration of digital forensic methodologies. The research topics guiding the inquiry were presented, focussing on how digital forensics may enhance audit outcomes and ensure regulatory compliance. The study's significance was addressed, emphasising its potential to enhance security protocols and audit dependability within the banking sector. The thesis framework was presented, outlining the upcoming chapters and their contributions to the overall research.

Chapter 2: Literature Review will examine the scientific literature to investigate existing research and hypotheses concerning the incorporation of digital forensics into information system audits. This review will establish the theoretical framework for the investigation, pinpointing deficiencies in existing information and substantiating the necessity for the suggested model produced in this research.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

This chapter examines pertinent research findings regarding the incorporation of digital forensics into information system audits, particularly in the financial sector. It analyses current literature regarding the methodology and applications of digital forensics in improving audit practices and assuring regulatory compliance. This chapter also highlights critical deficiencies in existing research, including the absence of complete models that successfully integrate digital forensics into auditing procedures. This chapter addresses study objectives one and two, establishing a foundation for the ensuing consideration of how these insights might guide the construction of a structured model to enhance IS audit outcomes.

2.1 Digital Forensics Process

Electronic data retrieval and analysis are discussed in the field of digital forensics. The method of historical reconstruction is designed to preserve any evidence in its original form while conducting a methodical research process that involves the acquisition, recognition, and verification of digital information (Kent et al., 2006; Alazab et al., 2023; Yusoff et al., 2011). Even though digital forensics has a wide range of applications, the context is typically associated with data usage in court. The digital forensics process is shown in Figure 1.

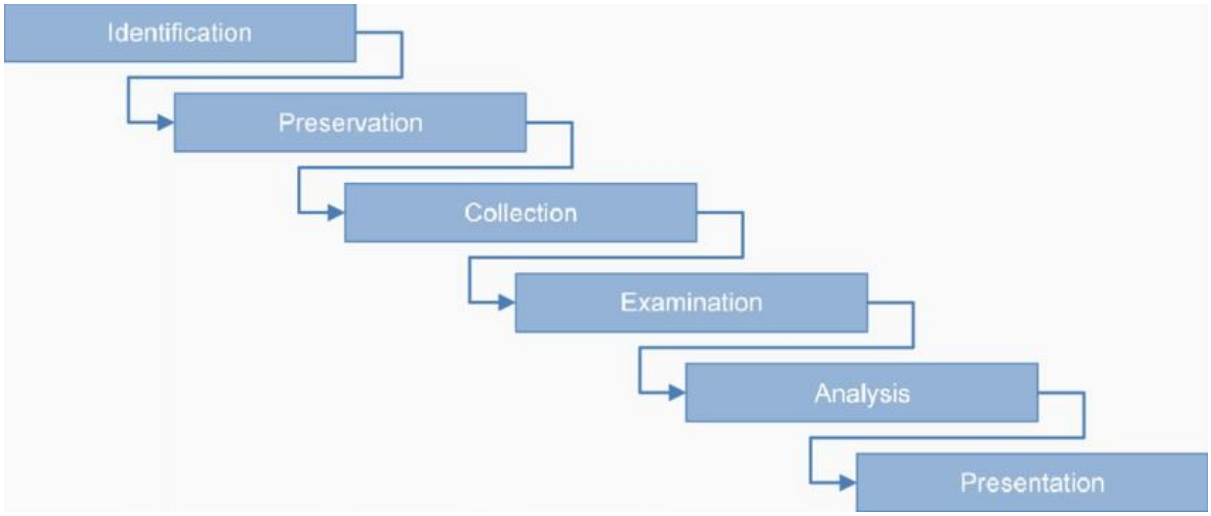


Figure 1: The digital forensics process (Kent et al., 2006; Alazab et al., 2023; Yusoff et al., 2011).

2.1.1 Collection of Digital Evidence

A chain of custody must be established in order to substantiate that the evidence was not tampered with, altered, damaged, or destroyed while in the investigator's custody. In accordance with Kent et al. (2006) and Alazab et al. (2023), a "chain of custody" is a chronological paper trail that documents the individual who collected the evidence, the individual who possessed it at any given time, and the current location of its preservation. This will demonstrate that the evidence is in the same condition as it was when it was initially collected when it is presented in court later in the investigation. Evidence is inadmissible in court if the chain of custody is disrupted, such as when it is impossible to explain the whereabouts and state of the evidence from the time it was acquired until the present. A successful evidence-collection process will result in the production of strong probative value evidence and the establishment of an effective chain of custody.

According to Kent et al. (2006), the primary goal of an inquiry is to accumulate evidence that can be employed in court. Law enforcement must present evidence that establishes the suspect's culpability "beyond a reasonable doubt" in order to successfully prosecute a case in court. Investigators must gather evidence in a manner that ensures the material is not damaged in any way during the collection, packaging, or shipping processes and that allows the material to be admitted as evidence in court. The evidence collected in violation of these guidelines will not be

admissible in court. Data can be easily lost, altered, or deleted. The data may become ineffective due to spoliation, which may result from inadequate evidence collection. Consequently, the investigation may be considered unsuccessful if the evidence gathered is not admissible in court. This emphasises the necessity of a plan for the collection of evidence that will ensure the evidence is protected and preserved in accordance with forensic best practices and that it is in a condition that allows it to be used as evidence in a court of law.

2.1.2 Chain of Custody Management

The chain of custody is a critical component of digital forensics, as it ensures the integrity of evidence throughout its life cycle (Sadiku et al., 2017; Ajijola et al., 2014). To prevent corruption or tampering with the evidence during the collection and administration process, a significant amount of paperwork and procedures are required. Different devices necessitate distinct management methods due to their distinct data storage systems. The chain of custody is the process of collecting, safeguarding, and evaluating evidence to create a chronological record for future management requirements, as defined by Ćosić and Ćosić (2012). This documentation is indispensable to criminal proceedings, as it allows us to identify the witnesses and, if necessary, summon them to testify at trial. Furthermore, the chain of custody upholds the evidence's original state and verifies its importance (Jansen & Ayers, 2004). If appropriate documentation and chain of custody procedures are not adhered to, digital evidence may become distorted and subsequently inadmissible in court (Sule, 2014). Therefore, it is imperative to preserve the chain of custody in order to ensure the legitimacy and admissibility of digital evidence in court.

2.1.3 Preservation of Digital Evidence

'Reliable documentation and evidence collection are essential,' asserts Kent et al. (2006). Evidence must be meticulously and legally acquired due to the occasionally intricate IT environment in which it is present. Neglecting this step may result in the evidence becoming corrupted, spoliated, or contaminated, rendering it ineffective. It is important to remember that the process of obtaining evidence does not have to be destructive. Before any evidence is collected, it is imperative to establish investigative techniques and plans to determine the critical

components of the investigation. By employing filtering and search techniques, it is feasible to minimise the quantity of data that necessitates examination. The evidence must be collected, collated, categorised, and stored securely in order to be utilised at a later time. Evidence must be presented months or even years after the behaviour occurred in cases that have garnered significant attention. Therefore, it is essential to establish an evidence storage system that facilitates the systematic, precise location and retrieval of evidence at any given moment.

The validity of evidence that has been collected and temporarily stored may be called into question at a later date. Subsequently, comprehensive documentation is required. Records should encompass the location, gatherer, type, and condition of the evidence at the time of collection. Logbooks will be very beneficial for the purpose of locating any evidence and will be especially beneficial when transporting it from one location to another.

A well-established process encompasses documentation, collection, storage, and return of evidence. By adhering to these procedures, the evidence will be safeguarded from manipulation or harm and ultimately admissible in court. Digital evidence must be safeguarded due to its fragility and susceptibility to modification or destruction. Additionally, it is highly volatile and can be effortlessly eliminated with a single keystroke. Therefore, comprehensive evidence-preservation equipment will be necessary. Evidence bags, toolboxes, write-protected software and hardware, backup power supplies for unforeseen power disruptions, forms for evidence collection, and specifically designed evidence collection and storage containers—such as Faraday bags for cell phone storage may all be required.

2.1.4 Digital Forensic Imaging

Zhang (2022) defines forensic imaging as the process of reproducing digital storage media while preserving its structure and data for future analysis. Forensic images are frequently captured on digital media such as flash discs, hard discs, and other devices that may contain evidence of criminal activity. Before examining the contents of a digital storage device, an investigator captures a forensic image. This ensures that the data is accurate and prevents any modifications

from occurring during the testing of the device. The creation of a forensic image is an essential initial step in any digital forensics' investigation. Investigators need to ensure that the image is a precise replica of the original storage device, and that all data has been retained.

2.1.5 Examination of Digital Evidence

An essential stage in digital forensics is the examination phase, during which investigators scrutinise the data gathered during the acquisition phase. Following the successful acquisition and imaging of digital evidence, the attention turns to meticulously scrutinising the data in order to discover pertinent information that could bolster the inquiry (Kent et al., 2006). In contrast to the acquisition phase, which focuses on gathering and safeguarding data, the examination phase prioritises the thorough study of the digital evidence to uncover concealed files, retrieve erased information, and analyse system logs or activity profiles that may provide vital insights.In the field of digital forensics, the process of investigation generally incorporates the analysis of complete storage medium rather than individual files. The objective is to identify patterns, timings, and anomalies that were potentially linked to the occurrence being investigated. Ensuring the preservation of evidence integrity is crucial throughout this procedure, particularly when analysing data on forensic workstations or other protected settings. Thorough documentation of all procedures implemented during the examination is necessary to guarantee the integrity and admissibility of the evidence in legal proceedings (Kent et al., 2006).

In addition, the procedure encompasses the movement of data across storage sites, such as from a seized device to a forensic workstation or external drive for scientific examination. It is of utmost importance to preserve the integrity of the evidence during these transfers in order to prevent any compromise to the investigation or the inadmissibility of the evidence (Alagić et al., 2011). The meticulous management and documentation throughout this examination stage are crucial to establish the preservation of the evidence, therefore safeguarding the examiner's reputation and the accuracy of the forensic conclusions.

2.1.5 Analysis of Digital Evidence

According to Kent et al. (2006), the most critical component of digital forensics is the accurate interpretation of the evidence without any distortion of the original data. The analyst must bear in mind that only physical drives mapped or networked drives should be employed during the data extraction process. Virtual machines (VM) are functional provided that their configuration has been documented and the VM image has been verified to be virus-free. It is frequently advantageous to obtain a "bit-stream image" of the suspect's drive. This replica of the original drive can be compressed and saved for future use, rendering it admissible as evidence. To prevent modifications to the source data, the image can be constructed using a write-blocker. Furthermore, it is advantageous to compute the hash value of the original evidence and incorporate it into the case notes. In that event, the hash value will fluctuate in the same manner as any other data item on the drive. This will demonstrate that the study employed identical evidence and data. The disc image can be used as additional evidence in the event that the original is misplaced or damaged. The significance of the evidence should be assessed by comparing it to the claims and case notes during the analysis. The analysis of meaningless data is a waste of time and money and will undermine the research. The material that is made public must be significant forensically and must contribute to the conclusion. This is frequently disregarded, resulting in the arrest of suspects without compelling evidence. In the event that the investigation's future significance changes at any point and the evidence is subsequently determined to be valuable, a record may be maintained.

Digital forensics analysis is the methodical examination of digital devices, data, and networks to identify evidence of criminal activity, security breaches, or illicit conduct, as defined by Kim et al. (2022) and Casey and Rose (2010). This process ensures that digital evidence is collected, preserved, examined, and evaluated in accordance with forensic standards by employing specialised apparatus and methods. File analysis, memory forensics, network traffic analysis, and virus analysis are among the methods that analysts employ to assemble events, identify offenders, and assess the severity of incidents. Digital forensics analysis is intended to provide actionable information regarding cyber incidents, data breaches, and other digital hazards to

facilitate investigations, court cases, incident response activities, and preventative security measures. This study is indispensable for both criminal investigations and organisational security evaluations due to its ability to safeguard data integrity, reinforce regulatory compliance, and enhance the overall cybersecurity posture.

2.1.6 Reporting and Documentation

The final phase in the digital inquiry process is the exportation of the analysis results for use in court or other legal proceedings (Kent et al., 2006). The findings of the analysis can be reported in a variety of ways. The necessity of submitting a more comprehensive report that includes the information you have gathered, the steps you have taken, and your conclusions, or a basic protocol for the process you have followed, will be contingent upon the circumstances and the needs of your organisation. The author asserts that report generation is the most prevalent form of reporting. Typically, a report comprises a summary of the case and accompanying documentation, information regarding the location and method of evidence collection, an explanation of the findings, and an explanation of how the findings relate to the case. Citations to the primary sources should be included in all verifications. Senior management occasionally requests that the report be accompanied by a verbal summary of the content. Archiving one's labour is the optimal form of documentation. This entails the preservation of your report, as well as any data and evidence files, in a secure and readily accessible location. At times, it is necessary to retain reports and evidence for an extended period of time after the case has concluded. In order to preserve the privacy and security of documentation, access may occasionally be restricted. This critical phase significantly safeguards the integrity of the evidence.

2.1.7. Presentation of Findings

The evidence will be presented in court if the case proceeds to trial, and the investigator will be asked questions and cross-examined by opposing counsel (Kent et al. 2006). The evidence must be prepared for testimony by being organised and practiced. The presenter must be able to communicate assurance and comprehension of the facts in order for a casual audience to perceive him as trustworthy. Visual aids and lists of supporting documents will be necessary to

present the case in court. An evidence list is a documented summary of the locations and proprietors of the evidence, similar to a chain of custody.

2.2 Bridging the Gap: The Synergy between Digital Forensics and Information System Audit

In the rapidly changing technical environment of the present day, the integrity, security, and conformance of an organization's IT infrastructure are contingent upon the mutually beneficial relationship between information system auditing and digital forensics. Companies that wish to protect their digital assets and mitigate cyber threats are increasingly recognising the importance of maintaining robust security protocols and adhering to legal obligations. The investigative foundation of digital forensics is the precise procedures for the identification, preservation, assessment, and presentation of digital evidence. This enables a comprehensive examination of security incidents, data intrusions, and unusual behaviour in information systems. In contrast, proactive watchdogs and information system audits meticulously evaluate IT controls, policies, and procedures to determine their effectiveness in mitigating risks and achieving business objectives. Companies can adopt a proactive approach to cyber-security and regulatory compliance by utilising forensic results to improve audit processes, identify vulnerabilities, and conduct focused maintenance activities. This is achieved by combining these areas. In a world that is becoming increasingly interconnected, this logical connection enables companies to enhance their defences, mitigate risks, and maintain the integrity and trust of their digital ecosystems.

2.2.1 Importance of Digital Forensics in Information System Audit

One of the primary responsibilities of an IS auditor is to evaluate the integrity of the information system. This is due to the fact that the admissibility and reliability of evidence have an impact on its overall value. If the data that has been acquired is not verified as genuine, germane, and trustworthy, it will be of minimal value to stakeholders and may never be admissible as evidence in a court of law. In order to ascertain whether digital evidence can still be used as evidence, an IS auditor must implement specific strategies and methodologies. This is similar to the work of a digital forensic analyst, who is responsible for ensuring the integrity and veracity of evidence. By

possessing a comprehensive understanding of forensic concepts and having implemented comparable auditing methodologies, an information systems auditor can acquire a wealth of knowledge regarding data validation. The IS auditor's ability to achieve the highest performance standards is contingent upon the precise relationship between digital forensics and IS auditing.

The practice of "digital forensics" involves the acquisition, identification, validation, and analysis of digital data in order to obtain information for legal purposes. The high esteem that organisations now accord digital forensics is indicative of the proportionate importance of the data they wish to protect. This is due to the ease with which data can be altered or deleted, which allows perpetrators to conceal their activities. These circumstances have made digital evidence—and the concomitant need for digital forensics—essential components of both the personal and professional spheres. This is especially relevant to information system auditing, as auditors frequently discover that the necessary evidence is in this format, as the majority of company data is now stored digitally. This is evidenced by the revision to the US Federal Rules of Civil Procedure (FRCP) that granted the pre-trial stage the capacity to assess digital evidence as an additional form of information (Moore, 2023). The IS auditor will be unable to collect the necessary information to complete the audit successfully if they are not informed of these significant changes. This underscores the necessity for information systems auditors to investigate digital forensics concepts and ascertain how to apply them in their audits.

2.2.2 Key Areas of Synergy

According to Quick and Henrizi (2018), it is frequently advantageous to implement substantive procedures in order to verify specific assertions or to conduct control experiments on a sample of data to accumulate evidence regarding the efficacy of the control. There are numerous methods to establish a connection between the two disciplines when considering the potential of utilising digital evidence to supplement these processes. In terms of the concept of information system control or audit trail, the execution of a programme or data entry should initiate a sequence of events that will result in the documentation of the activities that were performed. Auditors can employ this to directly assess the efficacy of a specific control and to elucidate the

results of the duplicate payment investigation that was previously discussed. In order to evaluate the effectiveness of a user access control system in preventing improper file access, Røstad and Edsberg (2006) implement an access monitoring programme.

The auditor is concerned about the veracity of the process map and the potential for obtaining documentation to substantiate the auditee's claims, as business process mapping generates critical risk areas and control objectives. Digital evidence obtained from an information system can be employed to confirm a pattern that is suspected and to substantiate the behaviour of a system or individual, regardless of whether it aligns with expectations. The information provided can improve the auditor's understanding of the procedure and allow them to create a more precise process map, regardless of the circumstances. For example, digital evidence could be employed to facilitate an audit of the accounts payable cycle and procurement process or to investigate the possibility of duplicate invoice payments (Rozario & Thomas, 2019).

A business process map is a fundamental visual that illustrates the steps required to achieve the desired outcome of a process. Frequently, this is accomplished through the use of a flowchart, which provides a comprehensible visual representation. The auditor's understanding of the process under examination is contingent upon the creation of a successful business process map. Singleton (2012) elucidates that digital forensics can be advantageous in the process of generating a business process map by information systems auditors.

2.3 Information System Audit

A comprehensive information system audit is a valuable safeguard that ensures the integrity and efficacy of digital infrastructure in the complex network of the financial industry, where trust and transparency are essential (Isaca, 2019). An information system audit evaluates an organization's compliance with industry standards and regulations by evaluating its IT systems, procedures, and controls. Each aspect of digital activities is meticulously scrutinised to identify opportunities for growth, constraints, and deficiencies (Isaca, 2019). The following are included: data administration, security protocols, network infrastructure, and software programmes. Due to the substantial stakes and global repercussions of digital malfeasance, information system audits are

intended to accomplish more than merely adhering to banking industry standards. It is essential for the preservation of financial integrity, the cultivation of investor confidence, and the mitigation of systemic risks. Organisations can effortlessly identify and mitigate the risks associated with fraud, data breaches, operational failures, and regulatory noncompliance through the implementation of stringent audit standards and continuous financial system monitoring. Additionally, an information system audit can facilitate financial innovation, expedite operations, and improve data accuracy. Financial institutions require information system audits to fulfill their fiduciary obligations, strengthen their defences, and maintain the integrity of the global financial system. They are both defenders of the economy and investor confidence.

2.3.1 Information System Audit Process

An internal systems auditor examines the control framework, collects data, evaluates the advantages and disadvantages of internal controls using the data, and generates an audit report that identifies deficiencies and provides relevant parties with recommendations for improvement. According to a literature review, an IS audit typically comprises three primary phases, each of which necessitates completion. Figure 2 shows a typical audit process phases and Figure 3 shows the detailed ISA Process.

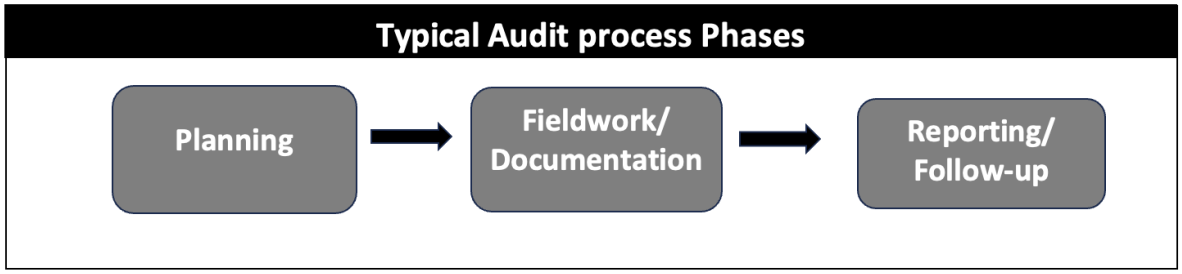


Figure 2: Typical audit process phases (ISACA, 2019)

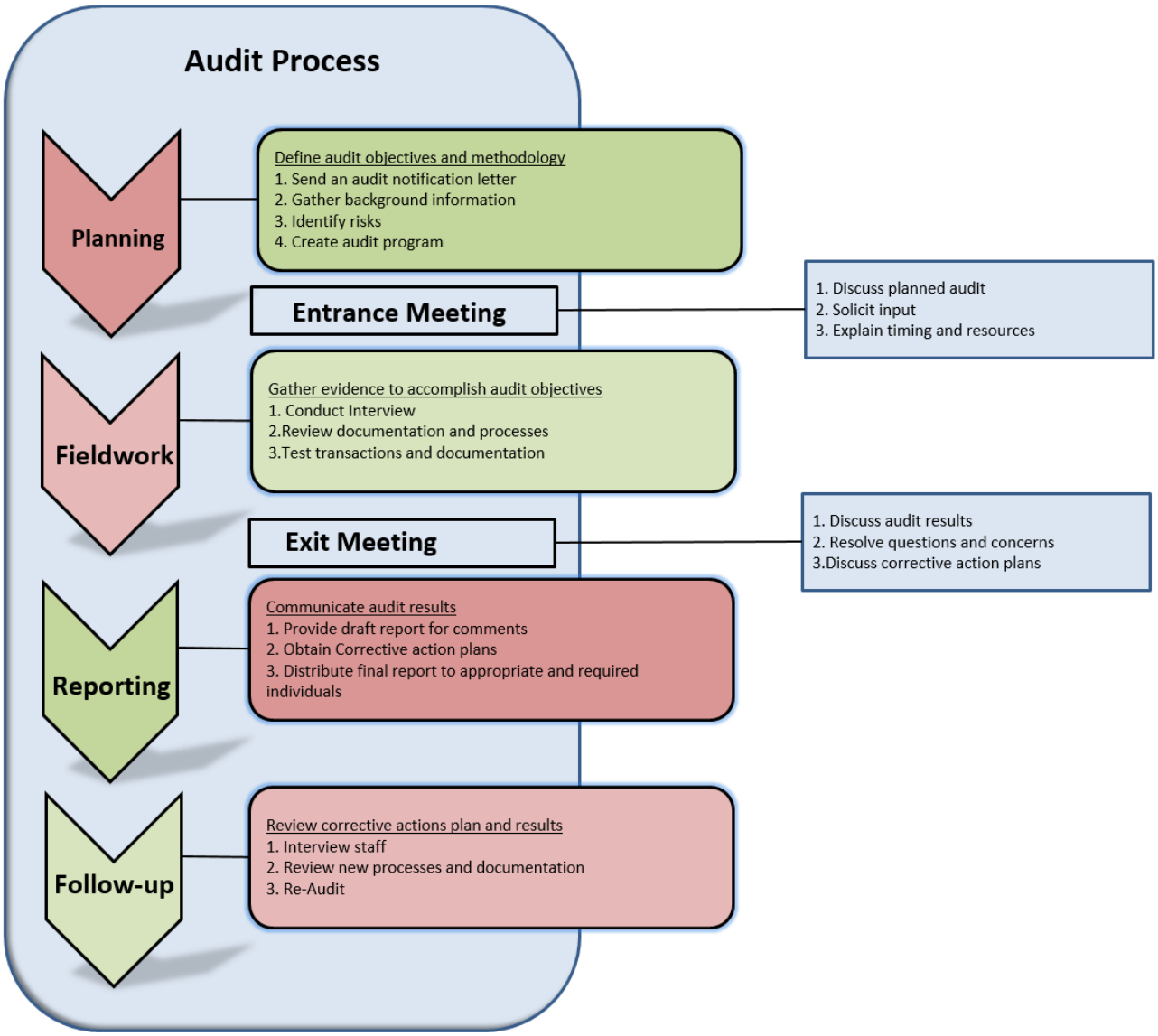


Figure 3: IS Audit process in detail (ISACA,2019)

i. Planning

In order to grasp the extent, duties, and current protocols of the area being scrutinised, the audit team must initially engage with the audit clients and gather crucial background information during the preparation phase, as stated by ISACA (2019) and AFROSAI-E (2017). As per the authors, during this phase, an audit programme is created, encompassing the audit objectives and audit technique. The audit plan is essential for guiding the audit process and successfully

accomplishing the audit objectives. A risk assessment for the department and/or function is usually carried out to ensure comprehensive coverage of all relevant areas.

ii. Fieldwork and Documentation Phase

The audit's evaluation stage, which is occasionally referred to as fieldwork, evaluates the adequacy of internal controls and compliance with industry best practices. By ISACA (2019) and AFROSAI-E (2017). According to the author, this phase involves the examination of assets, documents, and transactions, as well as the completion of any additional procedures necessary to facilitate the audit's objectives. Methods for obtaining evidence are employed to gather evidence that supports the audit objective during this phase.

iii. Reporting and Follow-up Phase

Every audit must conclude with a comprehensive written report that delineates the objectives and scope of the audit, summarises the findings, provides recommendations for improvement, and incorporates the input and corrective action plans of the audit client (ISACA, 2019; AFROSAI-E, 2017). Before being made public, audit reports are initially composed as manuscripts and sent to a small group of individuals, typically the department manager, for a preliminary assessment. The audit client is obligated to provide a written response that includes a plan for corrective action, the individual responsible for implementing it, and a projected completion date in the event that recommendations are made.

2.3.2 Evidence-gathering techniques

As noted in the analysis, evidence is collected during the fieldwork phase through inspection, observation, inquiry, confirmation, recalculation, re-performance, and analytical evaluations. An IS audit is conducted to assess an organization's information systems and ensure their confidentiality, dependability, and availability. Gathering evidence is an essential component of IS auditing, as it provides auditors with the necessary support to formulate conclusions and provide recommendations. This is the most critical stage of all the work steps. The evidence collected during the ISA is authenticated by the procedures outlined below. The methods for obtaining evidence through data analysis are illustrated in the figure below.

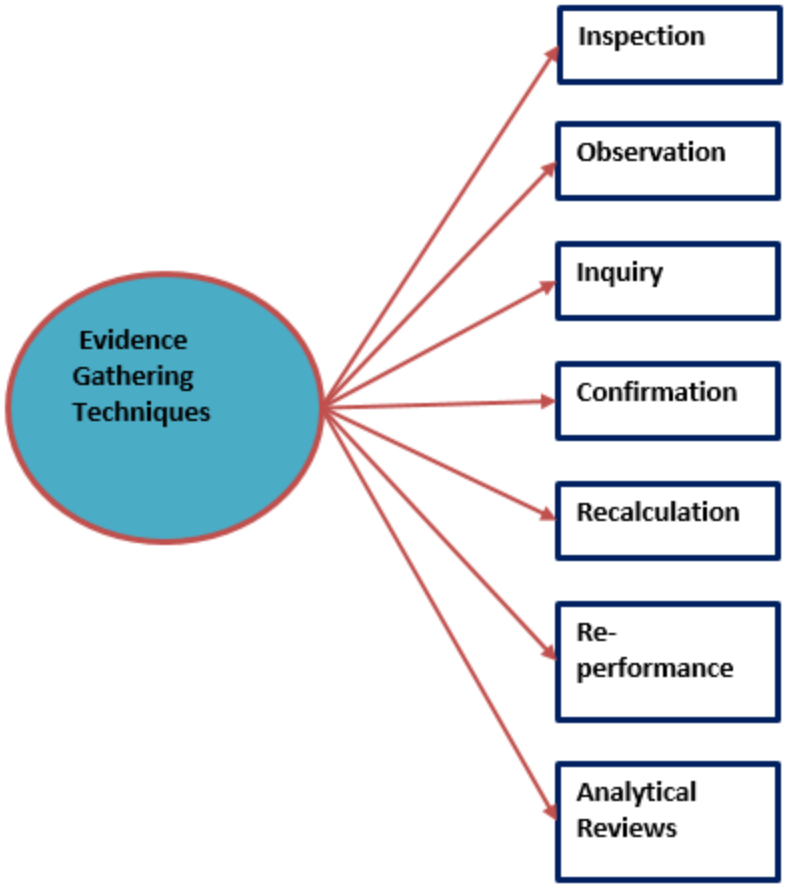


Figure 4: Evidence-gathering Techniques (ISACA, 2019; AFROSAI-E, 2017)

i. Inspection

The purpose of the inspection is to meticulously analyse records, documents, or tangible assets (ISACA, 2019; AFROSAI-E, 2017). Within the realm of information systems (IS) audit, this function facilitates auditors in examining system documentation, configuration settings, security rules, and processes. The full assessment is essential for verifying compliance with set standards and detecting any discrepancies inside the system. During this procedure, auditors acquire an understanding of the integrity of the information systems, guaranteeing that they function in compliance with predetermined norms and rules.

ii. Observation

The fundamental objective is to observe the implementation of a method or activity (ISACA, 2019; AFROSAI-E, 2017). This goal, in the context of an information systems (IS) audit, includes auditors' ability to actively monitor and analyse the efficiency of physical security measures, access protocols, and overall system operation. The role of observation provides critical insights into the practical implementation of security procedures, allowing auditors to identify any deviations from the declared standard. By employing this capability, IS auditors can improve security system inspection by assuring adherence to established standards and swiftly finding instances of noncompliance.

iii. Inquiry

The primary purpose is to gain information or clarification from persons who are knowledgeable in a certain field (ISACA, 2019; AFROSAI-E, 2017). Auditors in the field of information systems (IS) audit achieve this goal by conducting interviews with key stakeholders such as system administrators, users, third parties such as service providers, and management. Auditors gain critical information about system controls, access permissions, and security measures during these interactions. This direct interaction allows auditors to better understand the effectiveness of imposed controls and uncover any dangers or vulnerabilities within the system. By directly getting information from reputable sources, IS auditors improve the full examination of the security environment and overall reliability of information systems.

iv. Confirmation

The main goal is to get a response to a specific question. In the field of information systems (IS) audit, auditors use this goal by requesting verification from third-party service providers, vendors, or other external sources (ISACA, 2019; AFROSAI-E, 2017). This verification procedure is critical for analysing the efficiency of security measures or the current state of contractual services. Auditors improve their ability to validate information collected from internal sources by contacting external entities, ensuring a full and reliable understanding of the security landscape

and the state of contractual services within the system. This proactive strategy helps to ensure a more robust and comprehensive audit process.

v. Recalculation

The goal is to adjust or confirm the accuracy of a certain subset of information. Within the field of information systems (IS) audit, this objective enables auditors to thoroughly examine and authenticate specific financial or statistical data that is handled by information systems (ISACA, 2019; AFROSAI-E, 2017). The primary objective is to guarantee the precision and dependability of automated procedures, revealing any possible discrepancies in calculations. Auditors play a vital role in maintaining the accuracy of information produced by systems through a precision-focused audit. This helps to strengthen the reliability of automated processes and data outputs.

vi. Re-performance

The main goal is to autonomously carry out procedures or controls to evaluate their efficacy ISACA (ISACA, 2019; AFROSAI-E, 2017). Within the realm of information systems (IS) audits, auditors utilize this purpose by independently re-performing specific system functions or security regulations. This proactive methodology enables auditors to validate the effectiveness of these components, specifically when evaluating the dependability of automated systems. Auditors can detect and repair system vulnerabilities by actively re-executing activities. This contributes to a complete review of security policies and operational effectiveness in the information systems environment.

vii. Analytical Reviews

The primary goal is to investigate the relationships between various data sets. Auditors in the field of Information Systems (IS) exploit this goal by conducting analytical evaluations on a variety of data sets, including user access logs, system performance indicators, and security incident reports (ISACA, 2019; AFROSAI-E, 2017). This analytical ability allows auditors to detect trends, abnormalities, or patterns in data, potentially revealing security concerns or detecting weaknesses in control systems. Auditors contribute to a proactive and analytical review of the

system's security landscape by adeptly assessing the interrelationships between different types of data, enhancing the overall effectiveness of control mechanisms.

2.4 The use of Computer Aided Audit Techniques (CAATS) when conducting an IS audit

CAATs are implemented in analytical evaluations or procedures to identify control deficiencies by employing the auditee's data. In order to satisfy the audit objectives, Wicaksono et al. (2018) assert that the IS auditor must accumulate an adequate quantity of pertinent and dependable evidence during the audit. This is required by the Information Systems Audit Standard. The authors assert that the audit's conclusions and findings must be verified through a meticulous analysis and interpretation of the underlying data. Consequently, CAATs are instrumental in achieving this objective. Auditors, both internal and external, can utilise CAATs to collect, extract, investigate, and report on audit data. Thus, CAATs encompass oversight, fraud detection, general audit software, and e-audit working documents (Mahzan and Lymer 2014, as cited in Wicaksono et al. 2018). General audit software, e-audit working documents, fraud detection (GAS), and oversight are among the numerous CAAT categories (Mahzan and Lymer, 2014, as cited in Wicaksono et al., 2018). Word processing, data testing, integrated test facilities, parallel simulation, embedded auditing, and other CAATs are included (Wicaksono et al., 2018). Figure 5 illustrates this.

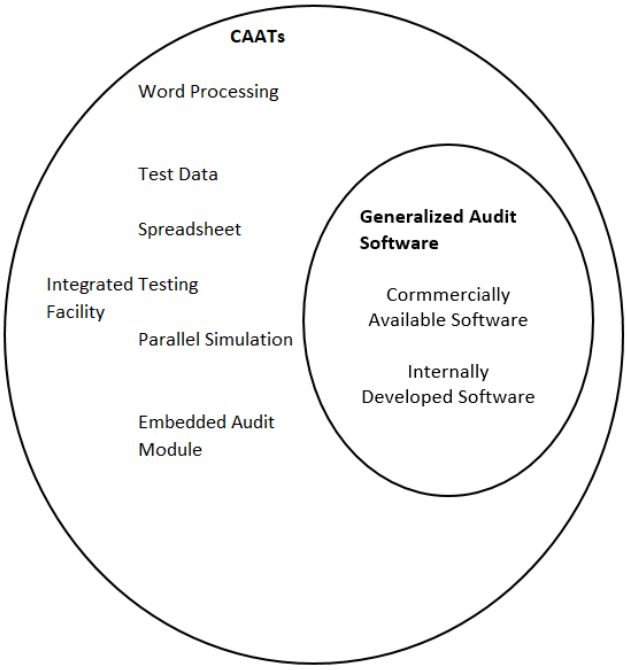


Figure 5: CAATs (Wicaksono et al., 2018)

2.5 Background on Financial Statement Auditing

An impartial auditor evaluates financial statements during a financial account audit. The auditor's opinion is significant in the context of the fair and honest representation of financial statements and associated disclosures. This audit is intended to enhance the company's overall reputation and the financial records that are reported. The audit was conducted in phases to accommodate the changing conditions. Later, it evolved into an auditing procedure that was more automated and involved a larger sample size. The subsequent assessments will encompass the entire population and focus on the identification of anomalies and outliers through pattern recognition and data analysis. The examinations will be conducted in a manner that has never been done before. Auditors employ more contemporary auditing techniques than conventional ones due to the vast quantity of information, which includes big data (AICPA, 2015; PWC, 2013).

2.6 The Concept of Audit Evidence

The collection of audit evidence is a well-known and essential phase of the auditing procedure. The quality of the data collected directly and significantly influences the audit's conclusions and findings. Throughout the audit planning process, the audit team should consider the types of audit evidence that are required. The audit planning procedure involves the organisation of the necessary evidence, as well as the determination of the time, location, and method of collection. Figure 6 shows the planning procedures of the audit.

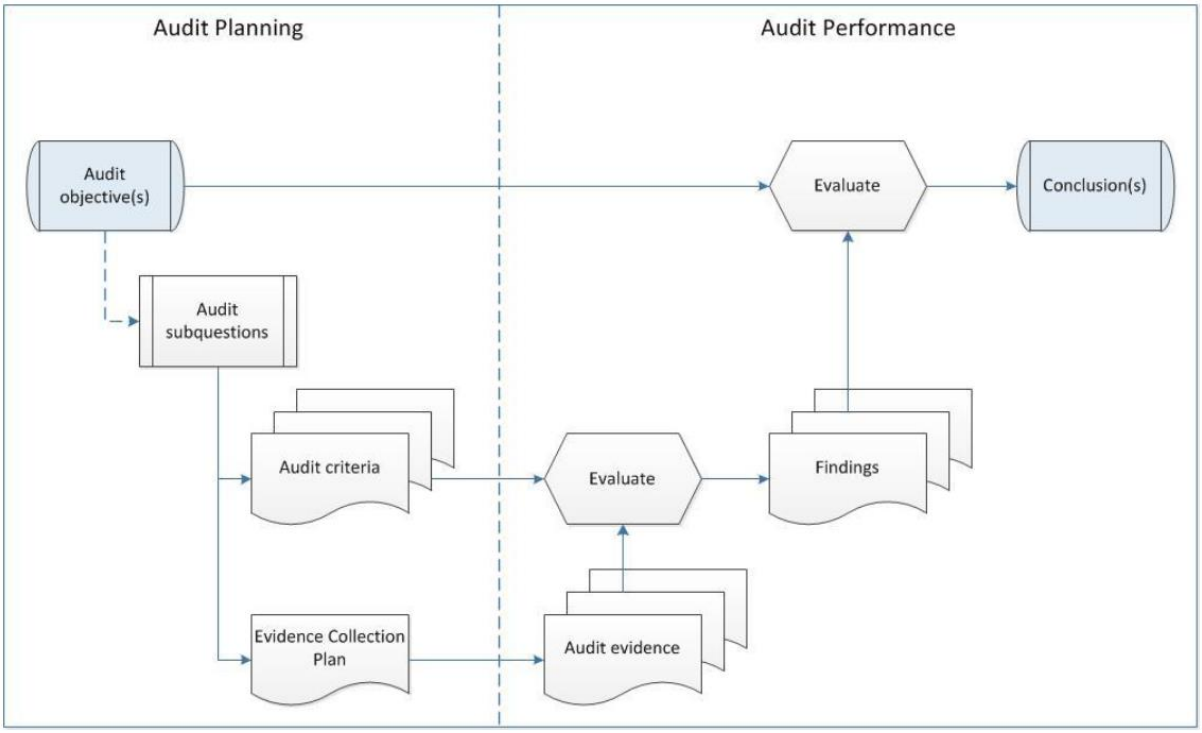


Figure 6: The audit planning procedure (AICPA, 2012).

Throughout the audit process, the audit team is responsible for ensuring that the evidence collected is appropriate and sufficient to support the audit's objectives. To develop reliable audit conclusions and findings, the audit evidence must be assessed in light of the audit criteria and objectives. Audit findings and conclusions must be supported by sufficient and relevant audit evidence in order to withstand challenges and pass both internal and external scrutiny.

For this research:

Audit criteria Refers to a collection of policies, procedures, or requirements that serve as a benchmark for comparing audit evidence. It is the yardstick by which the auditee's activities are evaluated. *Findings The evaluation of the evidence collected during the audit is presented in an unbiased manner.* *Conclusions Statements made by the audit team regarding the audit outcome, taking into account all findings and objectives, but without suggesting any specific actions.*

Auditors use audit evidence to determine whether they have met an audit objective. They do not include all the information acquired during an audit is included in the evidence. Having expertise in acquiring audit evidence and using a reliable process to collect it greatly influences the auditor's judgments. These judgments, in turn, play a crucial role in determining the quality of audit findings and conclusions.

Auditors collect audit evidence from audit methods or other sources to form their opinion. As a certified management accountant (CMA), it's important to consider all relevant and verifiable audit evidence, including any material that may contradict management's claims about financial statements or internal controls over financial reports. The expertise of the auditor who collected the evidence, the reliability of the audit evidence gathered, and the assessment of the technique used to gather the evidence all play a crucial role in determining the accuracy of the audit findings (AICPA, 2012). Traditional viewpoints on audit evidence may not be enough. It is crucial for the audit profession and regulators to recognise the influence of information technology on the nature and composition of audit evidence.

2.7 Characteristics of Audit Evidence

Evidence should be adequate and suitable. The audit evidence can be summarised as follows (AICPA, 2012; Brown-Liburd & Vasarhelyi, 2015; ISACA, 2019; AFROSAI-E, 2017).

Table 1:IS Audit Evidence Characteristics (AICPA, 2012; Brown-Liburd & Vasarhelyi, 2015; ISACA, 2019; AFROSAI-E, 2017).

Sufficient	Amount of evidence considered enough: i) To arrive at a well-founded conclusion (considering factors such as sample size and representativeness) ii) To persuade stakeholders of the credibility of the auditor's opinions. iii) Serving as a representative of the audit universe and the relevant period.
Relevant	The extent to which the evidence demonstrates a clear and logical connection to the audit objectives and criteria.
Reliable	Reliable evidence, characterised by accuracy, credibility, and uncompromised integrity; the probability of obtaining consistent results when conducting an audit test or gathering information from an alternative source or test.
Verifiable	Information that can be verified by comparing it with other evidence
Objective	Unbiased evidence, free from any preconceived notions or biases, that accurately represents the operations of a system, or a specific part of it, as conducted by the auditee, without any intentional support or defence of the auditee's interests.

2.8 Audit Procedures to Obtain Audit Evidence

While the auditor conducts risk assessment methods, these methods alone do not provide sufficient audit evidence to form an audit opinion. Additional audit procedures, such as

evaluations of internal controls and processes, need to be incorporated into the risk assessment methods. Regardless of whether the auditor reviews the controls, it is important to acknowledge that internal control has inherent limitations. These limitations include the potential for management override, human error, and the impact of system modifications. Objective processes are always necessary to obtain sufficient and relevant audit evidence for the categories of disclosures, account balances, and important transactions.

2.9 Techniques of Collecting Evidence

The auditor obtains audit evidence by one or more of the following techniques (AICPA, 2012; Brown-Liburd, & Vasarhelyi, 2015; ISACA, 2019; AFROSAI-E, 2017):

Table 2:Techniques of Collecting ISA Evidence (AICPA, 2012; Brown-Liburd, & Vasarhelyi, 2015; ISACA, 2019; AFROSAI-E, 2017)

Technique	***Definition***	***Examples***
Inquiry	Consists of seeking information of knowledgeable persons inside or outside the entity.	Obtaining written or oral information from the client in response to specific questions during the audit.
Observation	Consists of looking at a process or procedure being performed by others.	The auditor observes user access restrictions in action, such as monitoring employees connecting onto the company's network and accessing sensitive information, during a walkthrough of the company's IT infrastructure.

Inspection	Consists of examining records, documents, or tangible assets.	Inspecting firewall configuration settings and logs to ensure that only authorized network traffic is allowed and to identify any potential security breaches or anomalies in network traffic patterns.
Recalculation	Consists of checking the arithmetical accuracy of source documents and accounting records or performing independent calculations.	Recomputing the totals of financial transactions processed by the system, such as checking the accuracy of interest calculations on loans or verifying the correct application of tax rates on invoices, to ensure the integrity and accuracy of financial data.
Reperformance	Consists of independent execution of procedures or controls that were originally performed as part of the Entity's internal control.	Using CAATs for reperforming reconciliation procedures between financial statements and underlying transactional data to ensure accuracy and consistency, independently verifying the completeness and correctness of financial reporting processes.
Confirmation	Consists of response to an inquiry to corroborate information contained in the accounting records.	Sending confirmation requests to third-party vendors or service providers to verify the accuracy of financial transactions recorded in the system, such as confirming the amounts invoiced and services provided, to ensure the integrity of

		financial data and compliance with contractual agreements.
Analytical procedures	Includes the examination of important ratios and trends, along with the investigation of any fluctuations or relationships that don't align with other relevant information or deviate from expected amounts.	Examining system logs and user activity reports to identify patterns in failed login attempts or unauthorized access, comparing these patterns with established thresholds or benchmarks to assess the effectiveness of access controls and detect potential security threats.

2.10 Standards and Frameworks Used in Information System Auditing

COBIT (Control Objectives for Information and Related Technologies): Provides a comprehensive framework for the governance and management of enterprise IT, including auditing practices.

ISO/IEC 27001: Defines the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).

NIST SP 800 series: Guides information security standards and best practices, including specific guidelines for auditing information systems.

2.10.1 ISACA Standards and Guidelines

According to AFROSAI-E (2017), ISACA is a global organization of IT audit, governance, risk, and security experts that provides certificates, publications, and tools to IT auditors. ISACA created a set of IT audit standards and guidelines that address the general, performance, and reporting

components of IT audit engagements. The Institute of Internal Auditors (IIA) has established the International Standards for the Professional Practice of Internal Auditing (IPPF), which serves as the foundation for these guidelines. They also comply with other important frameworks, including COBIT, ITIL, and ISO/IEC 27000. The author claimed that adhering to and referencing the ISACA principles and guidelines will ensure that IS audit reports are compliant, objective, and reliable.

2.10.2 COBIT Framework

COBIT is a framework for IT governance and management that enables organizations to achieve strategic goals through efficient use of technology (Almeida et al., 2018; Aprilinda et al., 2019; Miranda et al., 2019; Christianto et al., 2022 Isaca, 2018). According to Isaca (2018), COBIT includes procedures, practices, enablers, and goals for aligning, planning, and organizing (APO), building, acquiring, and implementing (BAI), delivering, service, and support (DSS), and monitoring, evaluating, and assessing (MEA). COBIT also includes a collection of maturity models, performance indicators, and risk scenarios to assist IT auditors in determining the existing and desired condition of IT processes and controls (AFROSAI-E, 2017). As a result, AFROSAI-E suggests using the COBIT framework because it standardizes the language and format of IS audit reports and recommendations.

2.10.3 NIST Frameworks

NIST, a federal agency, is responsible for the development and promotion of standards, guidelines, and best practices in a range of scientific and technological domains, including IT. NIST has released multiple frameworks that apply to IT auditors, including the NIST cyber security framework (CSF), the NIST risk management framework (RMF), and the NIST privacy framework (PF) (Force, 2018). These frameworks provide a flexible and adaptable approach for identifying, managing, and mitigating IT-related risks, thereby enhancing cybersecurity and privacy outcomes. By utilizing the NIST frameworks, organisations can evaluate the effectiveness and efficiency of IT controls and processes in line with their risk appetite and tolerance.

2.10.4 ISO/IEC Standards

ISO/IEC is a collaborative technical group formed by the International Organization for Standardisation (ISO) and the International Electrotechnical Commission (IEC). Its purpose is to create and release standards for information technology, information security, and related areas. ISO/IEC standards that are beneficial for IT auditors include ISO/IEC 27000 for information security management systems, ISO/IEC 20000 for IT service management systems, ISO/IEC 38500 for IT governance, and ISO/IEC 31000 for risk management (Almeida et al., 2018; Aprilinda et al., 2019; Miranda et al., 2019; Christianto et al., 2022; Isaca, 2018). Isaca (2018) states that these standards offer a comprehensive collection of regulations, recommendations, and best practices for the establishment, implementation, maintenance, and enhancement of IT systems and processes. ISACA utilises ISO/IEC standards to evaluate and assess an organisation's IT performance and adherence to international norms and expectations.

2.11 Enhancing IS Audit Effectiveness through Standards and Frameworks

IT auditing is critical because it ensures that IT systems are effectively protected, that users are provided with reliable information, and that IT systems are managed properly to reap the intended benefits. The general purpose of IT audits is to assess the trustworthiness of data from IT systems that affects an organisation's financial statements. It can be used to determine the level of compliance with applicable IT laws, rules, and standards. An alternative application for IT audits, similar to that of a certified management accountant (CMA), is to assess whether there are instances of excessive spending, unnecessary extravagance, or significant inefficiencies that lead to inefficient use and administration of IT systems. An auditor develops criteria in this manner by drawing on best practices, frameworks, or standards.

Standardisation and frameworks significantly improve the reliability and efficacy of IS audit activities. Adhering to industry standards and benchmarks improves credibility and trust, provides structured best practices, serves as a reference for auditors and organisations, ensures compliance and consistency, identifies gaps and weaknesses, and enables benchmarking and continuous improvement (Drljača and Latinović, 2017; Isaca, 2019; AFROSAI-E, 2017). IS auditors can examine information security controls, governance procedures, and risk management

strategies using specified standards and criteria. This strategy results in proactive vulnerability discovery, more reliable audit findings and recommendations, and ultimately greater organisational resilience and information security.

Following an assessment of the methodology and standards employed in the information system audit, Audit institutions analyse controls using standards, guidelines, and best practices developed by credible standard-setting agencies and organisations such as NIST, ISO, and others. These organisations create and publish standards that specify requirements, protocols, and best practices for ensuring the security, dependability, and quality of goods, services, and systems. Audit institutions conduct information system audits in accordance with recommendations established by professional bodies such as ISACA and others, relying on frameworks and standards from entities that define standards. However, professional organisations have not developed any frameworks or standards to assist with governance-related responsibilities in the auditing industry, particularly in terms of how audit evidence would be acquired. The purpose of this research is to incorporate digital forensics into information system auditing in order to improve auditors' current evidence-gathering methods in accordance with the information system audit protocol. Financial auditors may rely on the controls that IS auditors approved, and this integration will help to ensure the data's availability, confidentiality, and integrity.

2.12 Addressed objectives

As per the above literature analysis, research objectives one and two were addressed and concluded as follows:

Objective 1: To analyze how the current steps employed in the information system audit process guarantee the CIA of information systems and validate the evidence collected.

Data collected from the literature review showed that steps within the information system audit process that guarantee the CIA information system and validate the evidence collected are:

i. Inspection
ii. Observation
iii. External confirmation

iv. Recalculation
v. Reperformance
vi. Analytical procedures
vii. Inquiry

These are required to ensure information systems' confidentiality, integrity, and availability (CIA). Inspection entails reviewing records to ensure data protection, whereas observation evaluates the efficacy of security procedures. External confirmation validates information accuracy; recalculation assures data integrity; and reperformance confirms system dependability. Analytical processes discover anomalies, whereas investigations uncover insights into system controls. These stages jointly validate evidence, ensuring that information systems adhere to CIA guidelines.

These audit techniques are often carried out during the fieldwork stage of an information system audit. The fieldwork phase entails the actual testing and examination of controls, processes, and data within the information system. During this phase, auditors collect evidence to evaluate the efficacy of internal controls, identify potential risks, and assess information system reliability. The procedures listed above are carried out at this phase to ensure the integrity, confidentiality, and availability of information systems.

Objective 2: To evaluate the standards used by IS auditors when conducting IS audits.

The key standards and frameworks commonly used by IS auditors during the IS audit process are:

i. ISACA Standards and Guidelines
ii. COBIT Framework
iii. NIST Frameworks
iv. ISO/IEC Standards, etc.

The standards used are not limited to the above-mentioned, as different organisations implement different standards and frameworks based on their organisational operations, objectives, and the industry in which they operate.

The framework and standards provide an integrated approach to risk management and internal control, which applies to IS audits. By applying this, organisations can establish and maintain an effective internal control system that supports business objectives, enhances the reliability of financial reporting, and complies with laws and regulations. IS audits utilize the standards and frameworks to help them identify and mitigate IT-related risks and ensure the integrity, confidentiality, and availability of information systems and data. Overall, these standards and frameworks give a structured approach to IS auditing, improve audit quality, and assist organisations in meeting their information security and governance objectives.

2.13 Research Finding

Based on the evidence-gathering techniques used in the fieldwork, the researcher concludes that the evidence-gathering techniques are not sufficient to conclude an audit with an unqualified audit opinion, cannot provide assurance CIA of the data contained in the system, and cannot be relied on by financial audits.

This has a significant implication, as accurate evidence collection could compromise the integrity of the financial audits, potentially misrepresenting a company's financial position and performance. Due to insufficient evidence-gathering techniques, the study underscores the risk of internal control failure leading to unreported errors or anomalies, fraud, insider threats, and undetected cyber-attacks within the systems and the entire organisation network. In an IS audit, evidence is needed to draw conclusions about the effectiveness of an organisation's information system performance. Evidence is any information used by the auditor to determine whether the information systems are safeguarding the assets, maintaining data integrity, and operating effectively and efficiently. The accumulation of sufficient, appropriate evidence is fundamental for drawing valid conclusions on the state of the information system. The quality of evidence will affect the quality of an audit's overall findings.

Therefore, the study proposed a model to set standards and address evidence-gathering techniques to ensure that unqualified audit opinions are obtained in both financial audits and information system audits.

2.14 Model Selected Components

This section aims to achieve research objective 2 and its question by identifying the digital forensics components to be integrated and the model will be developed in the next chapter. Based on the findings presented digital forensic imaging, chain of custody, and analysis are components of digital forensics that have been chosen to be integrated into the ISA. Integrating digital forensics components into information system audits in the financial sector offers several key advantages, making them the best choices for this integration:

i. Preservation of Evidence Integrity

Forensic imaging is the process of generating a bit-for-bit copy or snapshot of a digital storage device (such as hard drives or servers) at a given moment. This approach preserves evidence integrity by recording all data, even hidden or removed information. In financial audits, this is critical for ensuring evidence integrity and admissibility.

ii. Recovery of Deleted or Concealed Data

Forensic analysis techniques can recover deleted or concealed data, which is crucial in financial investigations. Auditors can utilise forensic techniques to find evidence of fraud, unauthorised transactions, or data breaches that have been hidden or erased.

iii. Comprehensive Investigation Capabilities

Forensic imaging and analysis enable auditors to analysed digital artifacts, logs, metadata, and system configurations thoroughly. This level of analysis aids in identifying security weaknesses, audit trails, and potential areas of risk inside financial systems.

iv. Supports Legal Compliance

Digital forensic processes follow legal standards and procedures to ensure evidence acquired during audits is admissible in court. This is critical in the highly regulated financial sector, where meeting legal and regulatory standards is vital.

v. Detecting Insider Threats

Forensic analysis can detect employees who misuse financial systems or access sensitive data for unlawful purposes. Financial firms can discover and mitigate internal risks more effectively by incorporating forensic approaches into audits.

vi. Enhanced Incident Response

Including forensic components in information system audits improves incident response capabilities. In the event of a security incident or data breach, auditors with forensic expertise can quickly investigate and resolve the problem, reducing the effect and preventing recurrence.

vii. Risk Mitigation and Prevention

Digital forensics helps identify vulnerabilities and weaknesses in information systems before they are exploited. This proactive approach assists financial organisations in improving their cyber security posture and protecting against emerging threats.

viii. Digital Evidence Handling

Financial audits require meticulous tracking of evidence to maintain its integrity and admissibility. Integrating the chain of custody management with digital forensics practices ensures that all evidence collected during audits is carefully documented and preserved. This establishes a clear trail of custody, which is vital in financial investigations and regulatory compliance.

All in all, forensic imaging, chain of custody, and analysis are the best components to integrate into information system audits in the financial sector due to their ability to preserve evidence integrity, recover critical data, conduct comprehensive investigations, ensure legal compliance, detect insider threats, enhance incident response, and mitigate cyber security risks effectively. By leveraging these forensic practices, financial institutions can uphold transparency, accountability, and security in their digital operations.

2.15 Integration of Digital Forensic Components in Information System Audits: Ensuring Security and Evidence Validity

Digital forensic imaging, chain of custody, and analysis work together seamlessly to ensure the confidentiality, integrity, and availability of information systems, as well as the validity of the evidence collected. First, digital forensic imaging creates a replica of the original data, safeguarding the original system's confidentiality and ensuring its availability for continued use. Next, the chain of custody meticulously documents every step of handling the forensic image, ensuring that the data remains untampered and that only authorized individuals have access, thus preserving both the confidentiality and integrity of the evidence. Finally, the analysis is conducted on the forensic image, not the original data, ensuring that the original system remains unaffected and available. The analysis must be thorough and based on sound forensic principles to ensure that the findings are valid and can withstand legal scrutiny. In this way, these components form a cohesive process that upholds the core principles of information security while ensuring that the evidence collected is reliable and legally admissible.

2.16 Optimizing Information System Audits with Integrated Digital Forensics

Integrating these three elements of DF into ISA will not eliminate the traditional evidence-gathering techniques, but it will be a key strength when collecting digital evidence that can be used and analyzed to conclude the audit. These three can aid when substantive testing is performed because substantive testing is done when testing of controls alone is not deemed sufficient to assure the integrity of the data and cannot be used to conclude a control being tested. Therefore, with the traditional evidence-gathering techniques, substantive testing is a must to strengthen the conclusion of the controls being tested.

Substantive testing in an information system (IS) audit includes reviewing transactional data, system outputs, and controls to determine the accuracy, completeness, and validity of information handled by an organization's information systems. Its goal is to provide independent verification of financial or non-financial information, guaranteeing that it is accurate and free of serious misstatements. Substantive testing is often used when control testing alone is insufficient to ensure data integrity (Andiola et al., 2021). Forensic imaging is required in information system

audits before substantive testing to preserve original data integrity and reduce alteration risks, ensuring admissibility and full analysis of evidence for effective audit procedures. It enables auditors to acquire a comprehensive dataset, including hidden or deleted data, which is crucial for identifying risks and compliance issues before doing substantial testing.

2.17 Chapter Summary

This chapter focused on a literature review of how information system auditing is conducted and the processes involved, as well as the best practices, frameworks, and standards involved. The researcher found that evidence-gathering techniques used during the information system audit are insufficient to conclude an audit and that financial auditors can rely on them when conducting the financial audit to ensure the integrity, reliability, and security of both financial and non-financial data within organizations' systems. Therefore, the researcher proposed to solve these problems by designing a model that integrates digital forensics into the information systems auditing process in the financial sector, with the goal of upholding confidentiality, integrity, and availability of both financial and non-financial data within organizations' systems. It also aims to ensure compliance with information technology activities aligned with company policies, industry best practices, and government laws and regulations. The model also intends to validate the evidence gathered during the audit by information system auditors. The methodology used to meet objectives one and two in this research will be discussed in the next chapter.

CHAPTER 3: RESEARCH METHODOLOGY

SECTION A: GENERAL SECTION

3.0 Introduction

This section of the research outlines the research design, data collection, and data analysis techniques that were used. This study follows a Design Science Research (DSR) approach, supported by a systematic and targeted literature review, to develop a model for integrating digital forensics into information system audits within the financial sector. Initially, a systematic literature review was conducted to explore existing information system audit processes and the challenges related to IS audits in the financial sector.

3.1 Research Paradigm

In the rapidly evolving field of technology, digital forensics has become a vital aspect of information system audits, particularly as companies increasingly rely on digital systems to store sensitive data. This study adopts a pragmatic research paradigm to develop a model that effectively integrates digital forensics into information system audits, focusing on practical and real-world applications. Pragmatism, known for its emphasis on practicality, relevance, and applicability, allows for the use of mixed methodologies and adaptable research designs to address complex problems (Creswell & Creswell, 2017). This approach is particularly suitable for integrating digital forensics into information system audits, ensuring that solutions are practical and implementable within organisational contexts.

Building on this, pragmatism's flexibility is highlighted in its ability to adapt research methods to specific study needs, making it an ideal choice for tackling interdisciplinary challenges like those found in digital forensics and information system audits (Creswell & Creswell, 2017). By incorporating diverse perspectives from stakeholders such as IT professionals and auditors, and prioritizing practical outcomes, this paradigm ensures that research findings are relevant and actionable (Deng & Ji, 2018). This methodological adaptability is increasingly adopted by IS researchers for its effectiveness in addressing complex, real-world issues, offering a balanced

approach that maintains rigor while promoting practical solutions (Deng & Ji, 2018; Hevner et al., 2004). This pragmatic foundation seamlessly connects to Design Science Research (DSR), which further enhances the practical application by focusing on the creation of innovative artefacts that address real-world problems.

This study focuses exclusively on external information system audits and does not include internal audits. This is because external audits are expressly designed to assess the security and controls of information systems from an external point of view, typically by third-party auditors or regulatory agencies. This study focused exclusively on external audits to offer specific insights and recommendations for organisations looking to improve their information system security and compliance with external evaluations and industry standardsthe focus was on carrying out a thorough and specific examination of external information system audit processes and how they affect the security and compliance of the organization of which internal audits, in contrast, are evaluations carried out internally by an organization's audit department, with a primary focus on broader issues of governance, risk management, and compliance that go beyond the considerations of external audits.

3.2 Design Science Research Strategy Overview

Brocke et al. (2020) described Design Science Research (DSR) as a problem-solving paradigm that seeks to enhance human knowledge through the creation of innovative artefacts. Additionally, the outcome of DSR includes newly designed artefacts and design knowledge that provides a fuller understanding via design theories of why the artefacts enhance the relevant application contexts. Pries-Heje et al. (2008) highlighted that DSR caters for innovative artefacts to solve real-world problems. This study deployed DSR to design a model that integrates digital forensics into information system audits in the financial sector. Figure 7 below shows the design science research methodology by Peffers et al. (2007) that was adopted for this study.

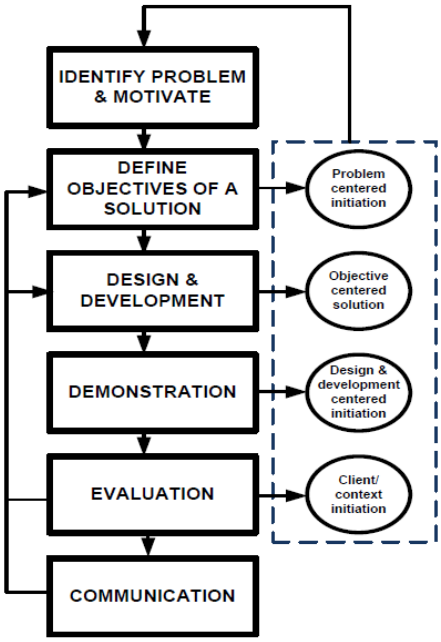


Figure 7: Design science research methodology (Peffers et al. (2007)

The details on how this methodology was adopted and used are found in Section B of this Chapter: Model Design Methodology. As it explained all phases in this model.

3.3 Data Collection Techniques and Instruments

Rouse (2016) defined data collection as a method of acquiring and measuring data on variables of interest in a recognized, systematic manner that enables one to obtain a complete and accurate picture of an area of interest. In this study, a targeted literature review was used as the primary instrument for data collection, focusing on professional publications and standards from authoritative sources in the field, such as ISACA, NIST, ISO/IEC, and audit institutions. Furthermore, according to Snyder (2019), a targeted literature review helps to map and assess the existing knowledge and identify gaps in specific issues, which, in turn, further develops the knowledge base. Additionally, document analysis was employed as the primary data collection technique. This approach involves systematically identifying, selecting, and analysing existing documents, publications, and literature relevant to the research topic. As Özkan (2023) explains,

document analysis systematically examines and interprets documents such as standards, publications, and reports from professional associations to extract meaningful data that can address the research objectives. Thus, this technique focuses on qualitative aspects like content, themes, and patterns within the documents. Refers to APPENDIX B for Selected publications that were assessed to meet the research objectives one and two, respectively.

3.4 Data Analysis

The data collected through the systematic literature review followed by targeted literature review and document analysis was analysed using a qualitative content analysis approach. Initially, the documents were systematically reviewed to identify recurring themes, patterns, and key concepts relevant to the research objectives. Specifically, the analysis focused on extracting and categorizing information related to compliance standards, best practices, and methodologies in information system auditing as outlined by authoritative sources such as ISACA, NIST, INTOSAI, ISO/IEC and other audit governing bodies. Following this, the extracted data was further analysed to map existing knowledge, identify gaps, and draw connections between different sources. This process involved cross-referencing findings across multiple documents to ensure consistency and to triangulate the data, thereby enhancing the reliability and validity of the results. Ultimately, the analysis provided an understanding of the current practices and challenges in the integration of digital forensics within information system audits, forming the basis for Model components. Results of the analysis are found in Chapter 2 sections 2.3 – 2.13. Appendix B shows the targeted literature that was analysed to meet research objectives one and two.

SECTIION B: MODEL DESIGN

3.5 Model design

This section of the chapter focuses on outlining the development process of the model. The proposed model research aims to blend information systems audits in the financial industry with digital forensics. The model was designed following the design science methodology used to design the model as stated in Section 3.2

3.5.1 The Model's Rationale

Based on the systematic literature review outlined in Chapter 2, it was concluded that the evidence-gathering techniques used in the fieldwork phase of the information system audit, are not sufficient to:

- conclude an audit with an unqualified audit opinion,
- provide assurance of CIA of the data contained in the system,
- be relied on by financial audits.

Additionally, there is no corelated element of digital forensics in the entire ISA process. This raises a significant implication, as inaccurate evidence collection could compromise the integrity of the financial audits, potentially misrepresenting a company's financial position and performance. Due to insufficient evidence-gathering techniques, the study underscores the risk of internal control failure leading to unreported errors or anomalies, fraud, insider threats, and undetected cyber-attacks within the systems and the entire organisation network. In an IS audit, evidence is needed to conclude the effectiveness of an organisation's information system performance. Evidence is any information used by the auditor to determine whether the information systems are safeguarding the assets, maintaining data integrity, and operating effectively and efficiently. The accumulation of sufficient, appropriate evidence is fundamental for drawing valid conclusions about the state of the information system. The quality of evidence will affect the quality of an audit's overall findings.

The proposed model aims to incorporate digital forensics into information system audits in the financial sector, ensuring the confidentiality, integrity, and availability of system data while adhering to company policies and regulatory requirements. The approach aims to improve the reliability and accuracy of audit conclusions by evaluating evidence acquired during audits, addressing inadequacies in current evidence-gathering procedures, and mitigating the risks of internal control failures and potential financial deception. Finally, the model seeks to improve the overall efficacy and efficiency of information system performance evaluation by enhancing evidence collection and validation processes, ultimately leading to stronger audit integrity and

regulatory compliance in the financial sector. All in all, the study proposed a model to set standards and address evidence-gathering techniques to ensure that unqualified audit opinions are obtained in both financial audits and information system audits.

Figure 8 outlines the application of Design Science Research (DSR) by Peffers et al. (2007) which was used to design the model that integrates DF into ISA.

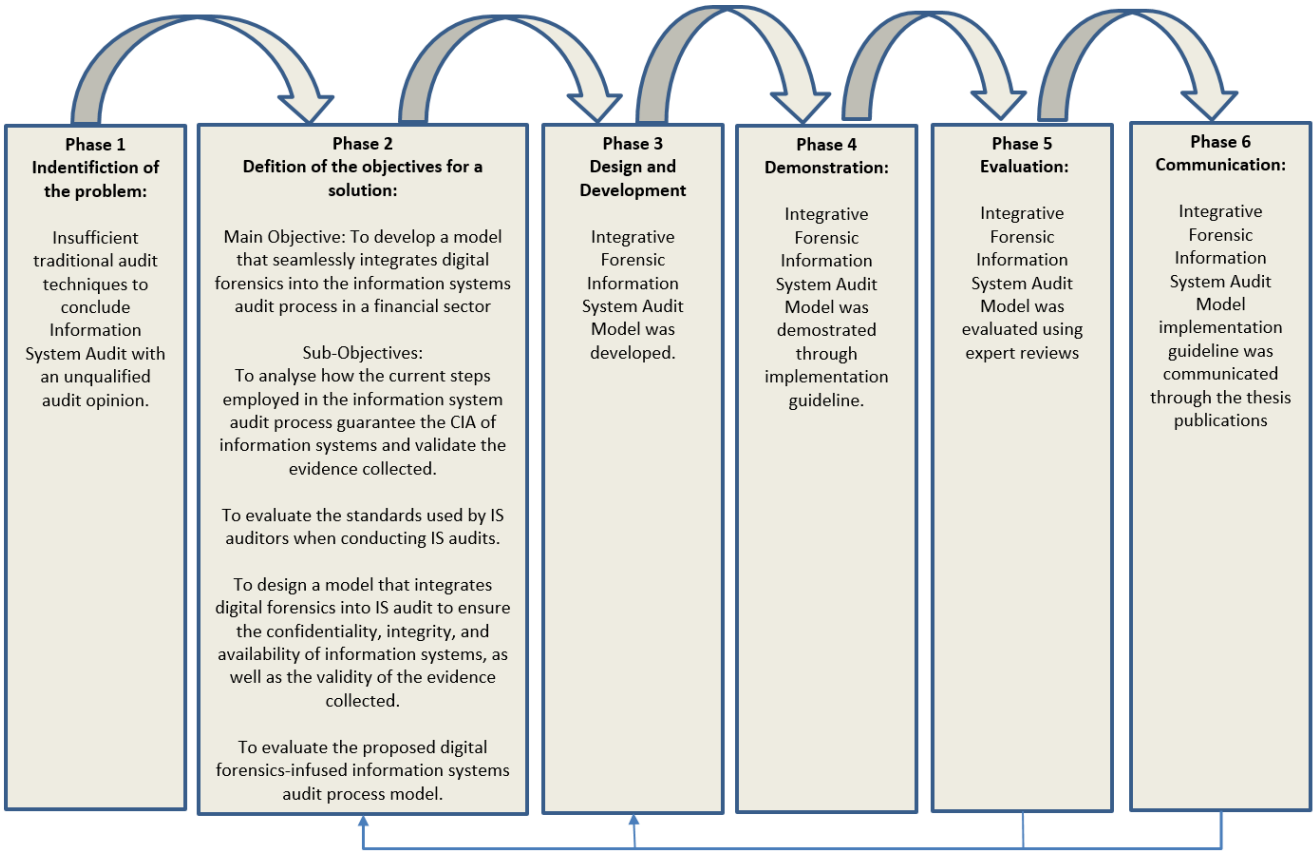


Figure 8: Used Design Science Research by Peffers et al. (2007)

3.6 Phase 1: Identification of the problem

In Chapter 2: Literature Review section '2.13 Research Finding', it was established that evidence-gathering techniques used in the fieldwork phase, are not sufficient to conclude an audit with an

unqualified audit opinion, cannot provide assurance CIA of the data contained in the system, and cannot be relied on by financial audits.

3.7 Phase 2: Definition of objectives for a solution

The second stage was to determine what the model should do. To find out what the model should research questions one and two were answered. Refer to Chapter 2, section 2.12 (a) and (b). The model should:

1. Integrates digital forensics into the financial sector's information systems audit process to ensure confidentiality, integrity, and availability.
2. Ensures that information technology activities are consistent with corporate policies, industry best practices, and government laws and regulations.
3. Validate the evidence gathered during the audit by information system auditors to achieve an unqualified audit opinion.

3.8 Phase 3: Design and development

This phase comprises:

1. Components Identification
2. Model design
3. Model Process flow

3.8.1 Model Selected Components

Based on the findings presented in the previous Chapter 2, digital forensic imaging, chain of custody, and analysis are components of digital forensics that need to be integrated into the ISA. These components are discussed in Chapter 2, Section 2.2, and section 2.13-2.15. To effectively incorporate these digital forensic components into the ISA, it is essential to align them with the existing Information System Auditing phases, which are discussed in section 2.3.1 in detail and summarized in the next section 3.8.2.

3.8.2 Information System Auditing Phases

Information System Audit consists of three phases, Planning, Fieldwork/Documentation, and Reporting/Follow-up. During the Planning phase of an information system audit, auditors define the audit scope, objectives, and methodology while also identifying major areas of risk and determining the resources required. During the Fieldwork/Documentation phase, auditors collect and analyse evidence by testing controls, analysing procedures, and evaluating system configurations to determine compliance and identify vulnerabilities. During the Reporting/Follow-up phase, auditors combine their findings into a report, outlining any shortcomings and making recommendations. They then follow up to verify that the organisation addresses these concerns and takes corrective action as necessary. Figure 9 shows the typical audit process phases.

Figure 9: Typical Information System Audit Process (ISACA,2019)

The main objective of the study is to develop a model that integrates digital forensics into information system audits in the financial sector. Based on the evidence-gathering techniques used in the fieldwork/documentation phase of the information system audit, the researcher concludes that the evidence-gathering techniques are not sufficient to conclude an audit with an unqualified audit opinion, cannot assure Confidentiality, Integrity, and Availability of the data contained in the system, and cannot be relied on by financial audits. Based on the problem that needs to be solved, imaging, chain of custody, and analysis are the digital forensics components that were identified that need to be incorporated into the fieldwork/documentation phase of ISA as illustrated in Figure 10.

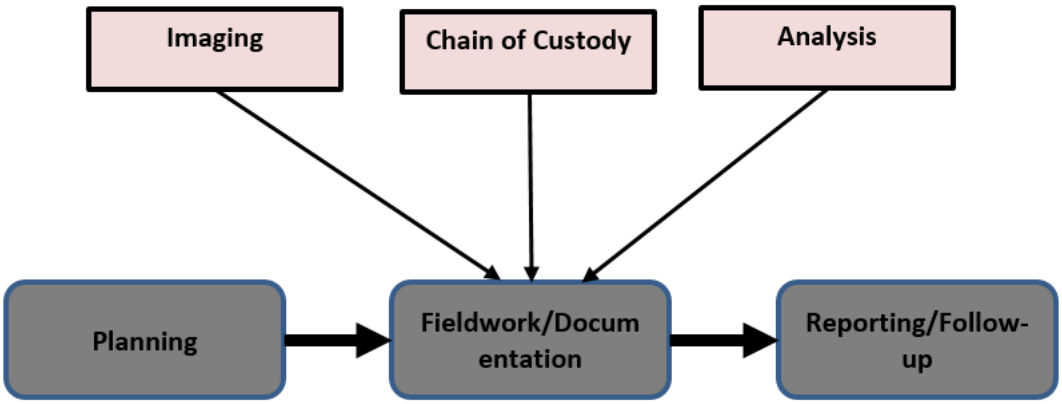


Figure 10: shows how the fieldwork phase will be modified

After imaging, chain of custody, and analysis are incorporated into the fieldwork/documentation phase of the audit process section 3.8.3 shows the full proposed model.

3.8.3 Proposed Integrative Forensic Information System Audit Model (IFISAM)

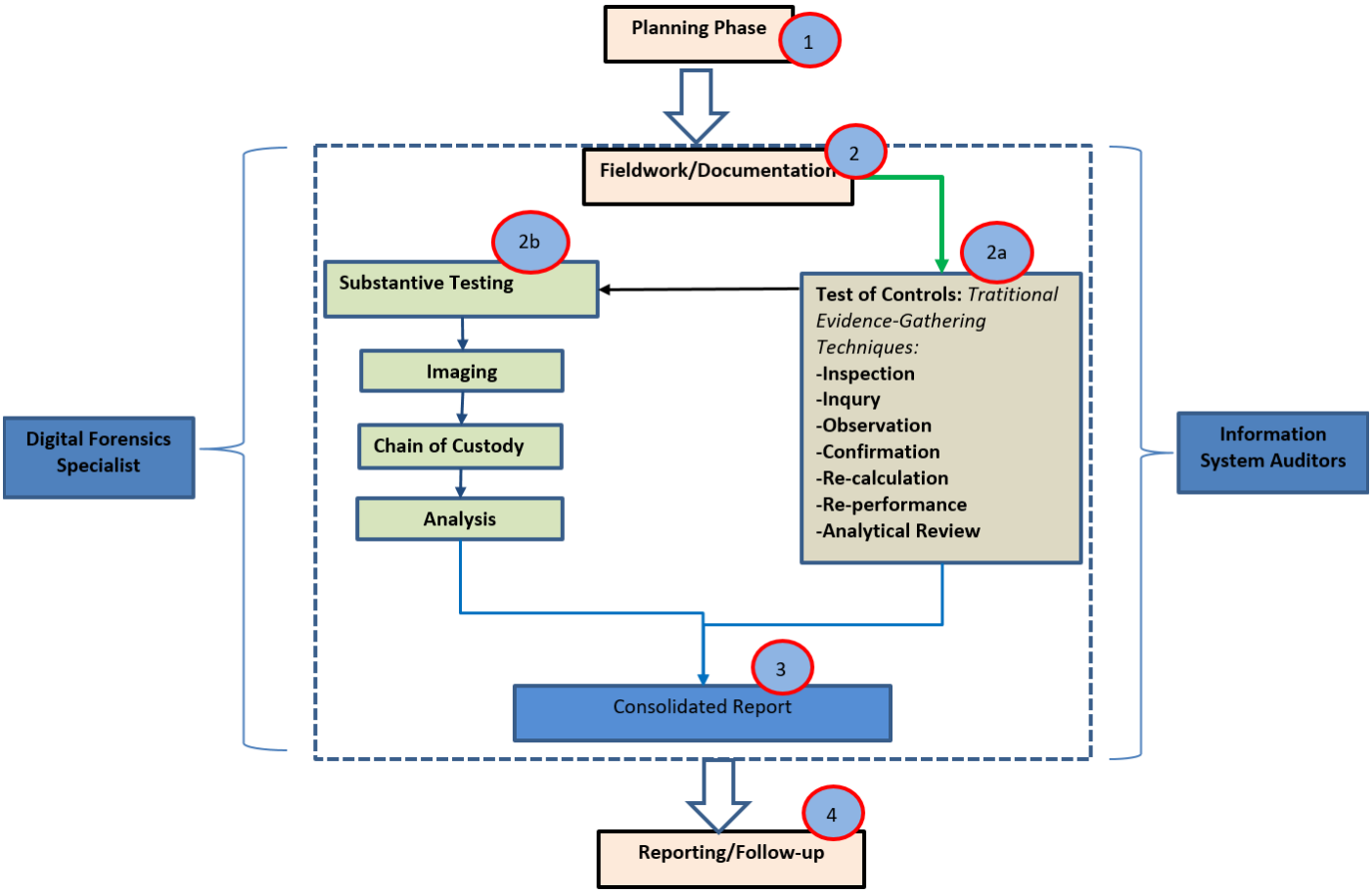


Figure 11: Proposed Integrative Forensic Information System Audit Model (IFISAM)

3.8.3.1 Below is the detail of how the proposed model works.

1. Planning Phase

Audit planning is conducted at the beginning of the audit process to establish the overall audit strategy and detail the specific procedures to be carried out to implement the strategy and complete the audit. The process begins with understanding the organization's IT environment, including its systems, applications, infrastructure, and controls. The auditor assesses the audit's scope, objectives, and criteria based on the organization's risk profile, regulatory requirements, and business needs. This phase involves identifying key areas of risk, critical systems, and potential vulnerabilities, as well as evaluating the adequacy of existing controls. The auditor also reviews relevant documentation, such as IT policies, procedures, and past audit reports, and may conduct interviews with key personnel. Finally, a detailed audit plan is developed, outlining the audit's timeline, resources, testing strategies, and the allocation of tasks among the audit team, ensuring that all critical aspects of the IS are thoroughly examined.

2. Fieldwork/Documentation Phase

Fieldwork/Documentation is considered the heart of an Information System (IS) audit because it involves the core activities of gathering, analysing, and documenting evidence to assess the effectiveness of controls and identify potential risks or vulnerabilities. This phase is where auditors perform detailed testing, review system configurations, and examine processes to ensure they align with the organization's policies, industry standards, and regulatory requirements. The accuracy and thoroughness of this phase directly impact the credibility of the audit findings, and the effectiveness of the recommendations provided, making it the most critical part of the audit process.

a. Test of controls

   During the Test of Controls phase in an Information System (IS) audit, auditors collect, and document evidence focused on high-risk areas identified during the planning phase. They review IT policy documents, compare them against industry standards and regulatory requirements, and conduct interviews with personnel to

understand how these policies are communicated and enforced. Auditors perform walkthroughs and observations to assess the practical application of policies, inspect records and logs for compliance, and re-perform key processes to test control effectiveness. Based on the audit criteria and its objective different evidence-gathering techniques can be used. The auditor can use either of them or a combination of them to test the effectiveness of internal controls. Refer to the traditional evidence-gathering technique that can be used in Figure 11.

b. Substantive testing

According to Isaca (2019), the auditors are to exercise professional judgment, and professional scepticism when conducting an audit. Professional scepticism, according to Isaca (2019) is an attitude that includes a questioning mind, being alert to conditions that may indicate possible misstatement due to error or fraud and a critical assessment of the evidence. With these two professionalisms in auditors, they can be able to determine if the control is subject to substantive testing during the test of control. Substantive testing is to be conducted when the test of control alone can not determine the effectiveness of the control. Once control is identified the forensic specialist will be conducted to gather the data from the system subjected to such testing.

The forensic specialist initiates the process by generating a precise digital replica of the system's data to maintain the original data in its entirety. Subsequently, they meticulously record the sequence of individuals who come into contact with or manipulate the data, guaranteeing the preservation of the evidence's integrity and its ability to be tracked. Ultimately, the expert examines the visualised data employing forensic techniques to identify any irregularities or unauthorised modifications, so verifying the precision and entirety of the data for the audit. The analysis will be based on the audit objective and the criteria in place to determine the effectiveness of the control.

3. Consolidated Report

After the Test of control and substantive testing, a consolidated report will be compiled of all internal controls that were tested for the period under review.

4. Reporting/Follow-up

During the reporting/follow-up phase of an information system audit, the auditor compiles and delivers an audit report to management. This report provides an in-depth analysis of the findings, risks, and recommendations identified during the audit. Management provides its proposed measures for addressing the issue. Subsequently, the auditor oversees the execution of these measures, potentially carrying out a subsequent assessment to verify the resolution of difficulties and may provide a conclusive report that summarises the efficacy of the management's efforts.

3.9 Chapter Summary

This chapter outlines the research methodology and model design, outlining the development of the model through the Design Science Research (DSR) approach. The comprehensive literature analysis and iterative design approach established a robust framework for developing a model to effectively include digital forensics into information system audits in the banking sector. The following chapter will illustrate the demonstration and assessment of the model, highlighting its practical use and evaluating its efficacy in resolving the identified deficiencies in existing audit methods. This assessment will yield significant information regarding the model's efficacy and its prospective influence on improving audit procedures within financial institutions.

CHAPTER 4: DEMONSTRATION AND EVALUATION

4.0 Introduction

This chapter cover the last three phases of DSR, which are demonstration, evaluation, and communication. This chapter demonstrates and evaluates the proposed paradigm for incorporating digital forensics into financial system (IS) audits. The goal is to demonstrate the model's success in improving the audit process by guaranteeing data integrity, correctness, and completeness using forensic approaches. This chapter will go into the methodology utilised for the demonstration and the criteria used to assess the model's performance. Evaluation, demonstration, and communication in this chapter are part of the design science research as it was explained in chapter 3, subsection 3.5.1.

4.1 Phase 4 Demonstration

The Proposed Integrative Forensic Information System Audit Model is working as it was described in the section preceding this section (subsection 3.8.3.1). To understand how the model works a hypothetical scenario was created following the model process flow explained in the section above.

4.1.1 Hypothetical Scenario

Inno-Secure Consultants is an audit firm, and it was given a mandate by the Office of the Auditor General to conduct an external audit on the effectiveness of the Social Security Commission’s Genero for the period 2021 to 2023. The Genero system is used to capture Social Security monthly contributions for all employed people in the country. The system is also used to pay out maternity leave, death benefits, disability or Retirement, and sick leave. As per Social Security’ Standard Procedure for Maternity Claims disclosed to Inno-Secure Consultants, indicates that any female registered with them is allowed to claim maternity benefits if all procedures and requirements listed in such documents are met. All registered beneficiaries are identified by their social security number, National Identification number (ID), or Passport number.

Below is how the above hypothetical scenario will be audited and for this demonstration only one objective of the entire audit will be demonstrated to see how digital forensics integration will fit into the model.

1. **Planning Phase**

In the planning phase of the Information System (IS) audit on the Social Security Commission's GENERO system, Inno-Secure Consultants reviewed the system's functionality and processes related to Social Security contributions and benefit payouts, including maternity leave. Examined Social Security's standard procedures for maternity claims and assessed the associated risks. Identified key objectives, such as verifying transaction accuracy and control effectiveness. Based on this assessment, Inno-Secure Consultants developed an audit plan, including sampling strategies, evidence-gathering techniques, and tools to be used when there is a need for substantive testing.

2. **Fieldwork and Documentation Phase**

The audit team conducted a walkthrough to understand how the system works before executing the audit. Objectives will be formulated based on the system's purpose and its work and then a test of control procedure will be formulated on how the internal controls will be tested for effectiveness and this will be also based on the Policies or standard procedure in place, in case there are no policies and standards in place the industrial best practice will be used as the evaluation criteria.

One of the objectives to be tested is as follows:

Objective: To determine if the system allows a beneficiary to claim maternity benefits after her death.

Internal Control in place: The system restricts maternity benefits claims linked to the social security number, ID number, or Passport number of the beneficiary after the death.

Test of Controls Procedure:

Below are the procedures formulated by the auditor to test if the listed internal controls are enforced and it is effective.

1. Obtain the number of all female beneficiaries who passed away for the period under review.
2. Use stratified sampling to select the samples from the total population.
3. Conduct a walkthrough by using the sample selected from the total population, use the social security number of the selected beneficiary who passed away for the financial year under review, and instruct the Registry Officer at Social Security to use such a claim number to create a new claim for maternity benefits in the GENERO system.
4. Observe if the system allows such claims to be registered or not. If registered Proceed to the Head of Claims to authorise the claim for payment.
5. Use Computer-assisted audit tools (CAATs) to determine if there is any beneficiary who came to claim maternity leave after death.
6. Document the findings.

Below is the test of control results and the procedure taken to conclude and results must be supported by evidence well documented and show all steps taken when assessing such evidence. Anything not documented in ISA then it is not done.

Test of Control Results: Based on the walkthrough done on 15 May 2024 by the audit team, with the Registry Officer and Head of Claims at Social Security. A total number of 22 6718 female beneficiaries passed away for the period under review was extracted and a stratified sample was used to select 50 beneficiaries. During the walkthrough, the audit team observed 50 claims created in the GENERO system using the social security number of the sampled beneficiaries by the Registry Officer. The audit team observed that the system restricts the claims to be registered as the social security number used was for someone who passed away. Therefore, the audit team did not proceed to the Head of Claims for the claim to be authorised for payment. Additionally, a forensic tool was used to determine cases in which the claim was done after death, and nothing

was found of that nature. *(See Annexure A for the supporting evidence of the test of control results and procedure taken to conclude. This is a hypothetical scenario, no Annexure A.)*

Control Conclusion: Control Operating effectively.

Risk Arising from IT (RAIT): High

There is a possibility of inherent risk due to the large volume of transactions or the potential for errors or fraud occurring despite the existence of this control.

This inherent risk might be:

- **Risk of System Bypass:** There is a risk that the control might be bypassed or overridden due to system vulnerabilities or weaknesses, allowing fraudulent claims to be processed.
- **Risk of Incorrect Implementation:** The control might not be correctly implemented or maintained, leading to unintended access or processing of additional claims for deceased beneficiaries.
- **Risk of System Errors:** Errors or bugs in the system could result in the control failing to restrict claims correctly, allowing improper claims to be processed.

  Due to the inherent risks and possibility that even with the control in place, the system could still face issues like bypasses, incorrect application, or technical failures, leading to potential unauthorized claims or fraud, these internal controls are subjected to substantive testing. *(According to Isaca (2019), the auditors are to exercise professional judgment, and professional scepticism when conducting an audit. With these two professionalisms in auditors, they can be able to determine if the control is subject to substantive testing during the test of control.)*

This is how the Forensics expert will come in, in the current substantive testing done the data from the system is provided by the auditee themselves, it can be either extracted in the presence of the auditor or not. This will not guarantee the CIA of the data contained and can conclude the ISA with either qualified, adverse, or disclaimer opinion. With a forensics specialist in the team, data needed for an audit can be obtained in a forensics-sound manner following the rules of digital evidence as insider threats can be detected, and other fraudulent activities.

Substantive testing Procedure

1. Imaging

Using a forensic tool creates a digital image of the GENERO system's database and transaction logs, focusing on the data related to claims processing. *(This ensures that the original data remains untouched while allowing for detailed analysis. This image will include all transaction records, user access logs, and system activity logs for the period under review, particularly focusing on data after a death claim has been recorded.)*

2. Chain of Custody

Documents the entire process of data imaging, including who created the image, when it was created, and every instance of handling the data. *(This documentation includes timestamps and detailed descriptions of each step to ensure that the data's integrity is maintained throughout the audit process. The chain of custody documentation ensures that any evidence gathered during the audit is reliable and can be used to support audit conclusions.)*

3. Analysis

3.1 Analyse the imaged data with a forensics tool to identify any claims processed using the social security numbers of deceased beneficiaries. Specifically, look for any maternity claims that were made after the beneficiary's death.

3.2 Cross-referencing the imaged data with external databases (with the Ministry of Home Affairs and Immigration's Death Registry database) to ensure that all deceased beneficiaries' social security numbers are correctly flagged, and no benefits claims were made posthumously.

4. Document the Findings

(Findings from the procedure carried out will be documented here)

Substantive Testing Results: On 23 May 2024, substantive testing was done on the GENERO system to determine if the system restricts any other benefits claim linked to the social security number of the beneficiary after the death claim. The audit team instructed the forensic team to make a replica of the GENERO system for data analysis. A forensic tool was used for imaging the

system, and all steps taken during the process were documented to ensure data integrity. The data were analysed using the forensics tool. It was noted during the analysis that the total number of female beneficiaries extracted from the database by the Auditee was less compared to the one extracted by the Forensics team. Additionally, it was noted that of 4468000 females passed on, 1680 claimed maternity benefits after their death, and a total amount of N$ 2 790 650 was linked to such claims. *(See Annexure B for the total number of extracted beneficiaries that passed on and Annexure C for maternity claims done after the passed-on of beneficiaries. This is a hypothetical scenario no such Annexures are attached).*

4. Control Conclusion

Based on the substantive testing conducted, the control is ineffective as it was noted that one can claim maternity leave after death.

5. Recommendation

The auditor recommends immediate system enhancements to ensure that claims linked to deceased beneficiaries are automatically flagged and prevented from processing. Additionally, a thorough review of the system's data integrity protocols should be conducted to address discrepancies in beneficiary records.

4.2 Phase 5 Evaluation

The experts' reviewers were engaged evaluate the model using a round table discussion., the results from the round table discussion and the expert study were used to modify the model, and the model was then given to the experts to ensure that all their proposed changes had been incorporated.

4.2.1 Evaluation Criteria

According to Brocke et al. (2020), the purpose of evaluation in DSR is to assess the progress reached by designing, constructing, and using an artefact in relation to the identified problem and the design objectives. Furthermore, to methodically demonstrate if such progress is attained, evaluation should be guided by evaluation criteria. Evaluations can also be crucial in highlighting

areas of the artefact that may require further testing (Brocke et al., 2020). Case studies, experiments, and expert reviews are examples of evaluation techniques (Brocke et al., 2020). The evaluation of the Integrative Forensic Information System Audit Model was conducted to assess how well the proposed artefact addresses the objective it was intended to support.

Hall (2017) defined an expert review as the technique where an expert reviews an artefact and notes potential usability issues. He further highlighted that such reviews can be effective at giving meaningful feedback in less time and at a reasonable cost than other methods. According to Tory and Moller (2005), in an expert review, the reviewer brings in his/her expertise in a given substantive domain, and at times his/her personal choices or biases. Expert reviews were used to evaluate the model because they were deemed relevant as suggestions from the experts would improve the model and make it practically implementable. Obtaining an expert evaluation is essential when developing a model that incorporates digital forensics into financial sector audits. This assessment ensures that the model is accurate, feasible, and in line with industry standards. The validation process ensures credibility, identifies any dangers, and improves the model to make it more realistic. This eventually leads to successful acceptance and effective implementation in a complex and regulated context.

4.2.2 Expert reviews

According to Harrison et al. (2017), an expert review involves a thorough examination of an object by a knowledgeable individual to identify any possible usability problems. He emphasised that these assessments could provide valuable input in a faster and more cost-effective manner compared to other approaches. As per Tory and Moller (2005), during an expert review, the reviewer utilises their expertise in each subject area, occasionally incorporating their own biases or preferences. Experienced information system audit specialists conducted a thorough analysis to assess the model's strengths, weaknesses, and alignment with the desired objective. Six experts carefully evaluated the approach, prioritising in-depth feedback and real-world experiences over a one-size-fits-all approach. The expert reviews focused on evaluating the model based on:

- Relevance
- Practical Implementation
- Usability
- Applicability
- Impact

4.2.3 Model Evaluation Tool

An expert panel was assembled to assess the model using predetermined criteria through a roundtable discussion. During this session, experts were posed specific questions that were in line with the evaluation criteria, which led to a collaborative conversation. Refer to Appendix A for the questions that were used. After the questions were asked, the experts engaged in a comprehensive discussion where they shared their views and viewpoints. The inputs collected from the round table debate were carefully analysed and considered to continuously improve and perfect the model, utilizing the valuable comments given by the panel of experts. This iterative strategy seeks to consistently enhance the quality and efficacy of the model by engaging in expert engagement and incorporating their advice. Even though the discussion occurred after the model was presented to the experts, a request to record the discussion was made, to which seven of the experts refused. The experts noted that the presence of a recording device may limit their ability to speak freely, potentially leading to less open and honest remarks. Experts also claimed that without the added pressure of being recorded, they could successfully share thoughts, raise concerns, and engage in productive discourse.

4.2.4 Biographical information of the reviewers

The biographical details of the participants can be found in Table 3. Notably, six out of the eight participants have extensive experience ranging from 10 to 30 years in their respective fields, while two participants have between 6 and 10 years of experience. These participants are experienced auditors and forensics experts who possess both theoretical knowledge and hands-on experience, and some hold managerial positions within their field of expertise.

Table 3:Participants Biography

No.	Reviewer's position	Years of experience in ISA	Qualification (s)
Reviewer 1	IS Audit Manager	29+ years	MBL, BACC, FCCA, FZICA, CISA, CRISC, SAP, Sec
Reviewer 2	IS Audit Manager	18 years	Bachelor of Informatics & CISA
Reviewer 3	IS Assistant Manager	6 + years	Certified Information Systems Auditor (CISA
Reviewer 4	Information Systems Audit & Assurance Specialist	20 years	CISA & CRISC
Reviewer 5	Associate Director: Risk Advisory	12 years	Bachelor of Accounting, CISA & COBIT 5
Reviewer 6	Deputy Director of Information System Audit	9 years	CISA, Post Graduate Certificate Information System Auditing
Reviewer 8	Principal Cyber Forensic Investigator	15 + years	Bachelor's degree in Information Systems, IACIS Certified

			Mobile Device Examiner, Certified Advanced Windows Forensic Examiner (CAWFE), AccessData Certified Examiner, AccessData Mobile Examiner, and Certified Forensic Computer Examiner
Reviewer 8	Forensic Investigator	13+ years	Bachelor of Commerce-BCom (Hons) Cyber/Computer Forensics, GIAC-GCFE-Certified Forensic Examiner, Advanced Computer Forensics, Higher National Diploma, Police Administration

4.2.5 Evaluation findings

Information System Auditors and Digital forensics experts were selected to be the expert reviewers for the proposed model.

i. Overall Performance

A round table discussion was held with the expert reviewers, and Appendix A was used as a guide for this process. The graph below shows the scale of agreement that was agreed upon by the experts based on the criteria they were evaluating the model on.

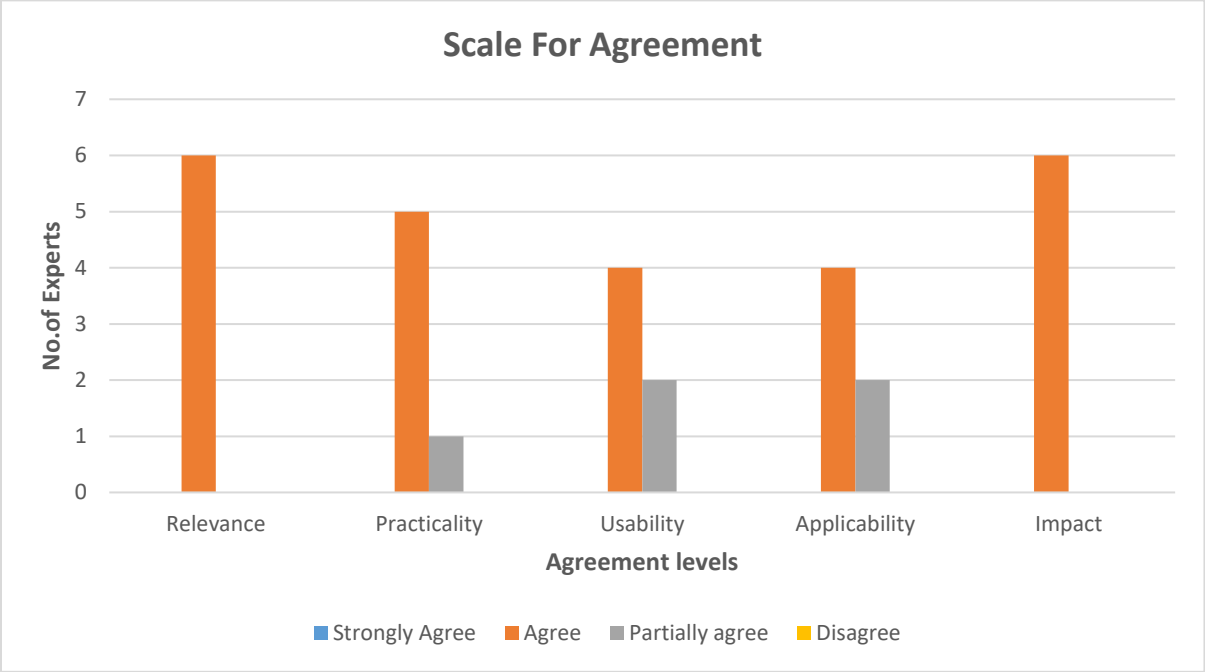


Figure 12: Scale of agreement

Based on the expert review, the overall conclusion regarding the evaluation of the model for integrating digital forensics into information system audits in the financial sector is positive. The experts collectively agree that the model demonstrates a high degree of relevance by effectively incorporating digital forensics concepts and methodologies to address evidence-gathering techniques and critical information system security risks. It aligns well with industry standards and best practices, offering a valuable framework for enhancing cybersecurity resilience and ensuring the confidentiality, integrity, and availability (CIA) of information within audits.

ii. Recommendations

- Feasibility Considerations: Resource constraints and potential resistance to change are identified as key challenges. Experts suggest allocating specific resources for training

auditors on digital forensics concepts, implementing change management strategies tailored to address challenges, and conducting readiness assessments to ensure organizational readiness.

- Practical Implementation: The practical application of the model is deemed feasible but may require minor modifications to address resource constraints and align with existing audit practices. Recommendations include developing clear implementation guidelines, providing robust training programs, and adapting the model to work seamlessly with current audit techniques and instruments.
- Usability and Clarity: Experts note that the model's usability could be improved by adding role players in each phase, clearly differentiating phases, and providing comprehensive guidelines and training support for information system auditors to facilitate adoption.
- Applicability: While the model shows broad applicability across various industries and information system environments, customization for specific organizational needs and legal requirements is recommended. Enhancing scalability and flexibility within the model would further enhance its applicability.
- Impact: The model has the potential to significantly improve the effectiveness and efficiency of information system audits in the financial sector by enhancing evidence-gathering techniques, strengthening CIA principles, and optimizing cyber security incident examination and risk management. Successful implementation and ongoing monitoring are emphasized to achieve the desired improvements.

After the recommendation from the expert a detailed process of how the model works was documented to make it easier to follow. Refer to section 3.8.3.

4.2.6 Validated Model

After the expert's recommendation, the researcher made the following adjustments to the model to ensure inputs from the experts were considered:

-To improve the usability of the model the reviewers proposed that role players be added to the model so that there will be no confusion when it comes to the segregation of duties during the

audit and when forensics experts will be required. This was later explained in section 3.8.3 and in section 4.1.

-The expert also requested for the implementation guidelines, or the model process to follow. This will serve as detailed instructions or best practices to help ensure the successful application model and to provide clarity, consistency, and direction for those responsible for carrying out the implementation. The research responded to this with a model process flow in section 3.8.3 which describes how the model will be implemented. Figure 13 shows how the model looks after the recommendations from the experts.

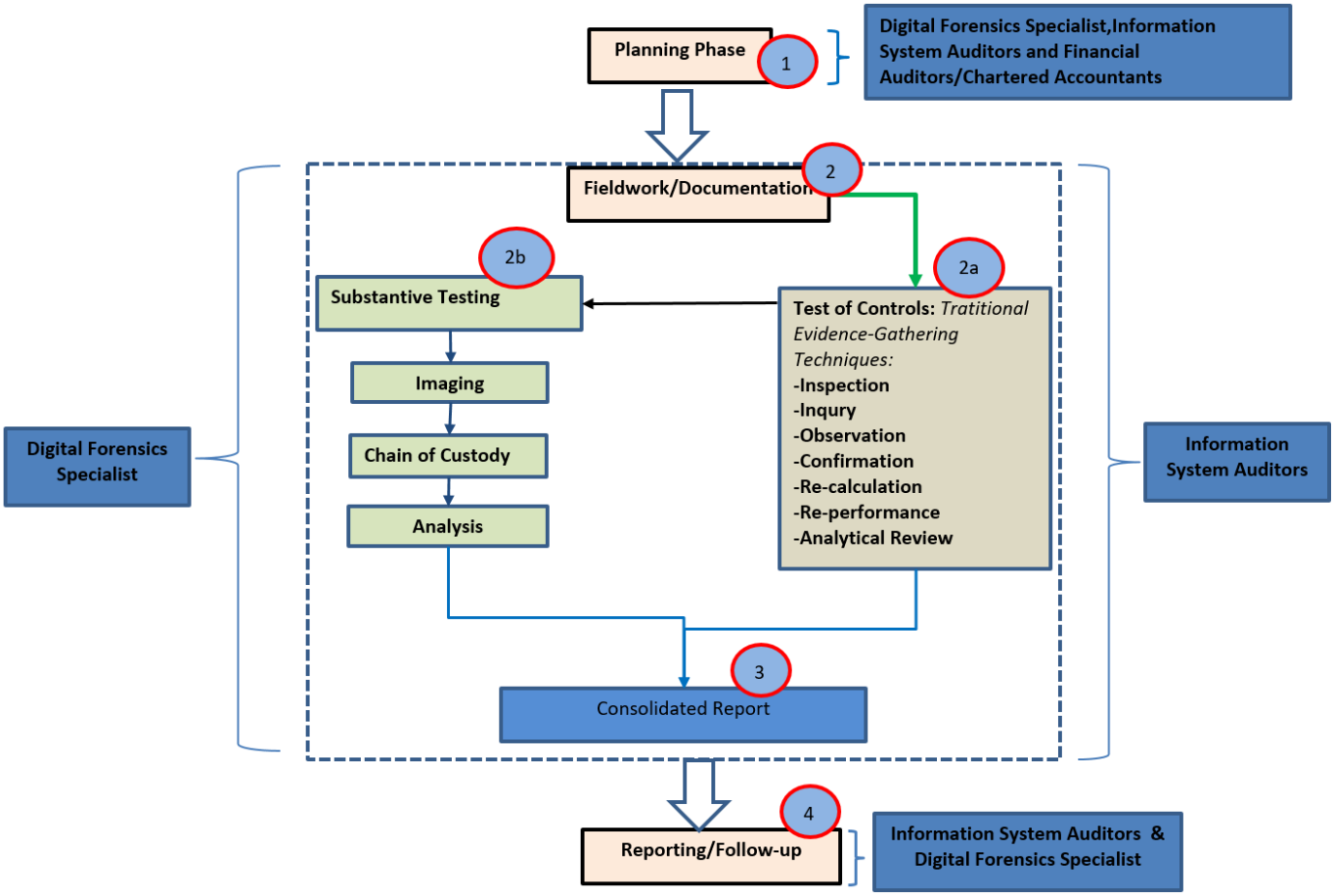


Figure 13: Expert-validated model

4.3 Phase 6 Communication

The findings of this study will be communicated through this thesis and peer-reviewed scholarly publications. Furthermore, For the model to have an impact on the audit domain, it will be shared and assessed for its practicality by the Namibia Supreme Audit Institution (SAI Namibia). Through SAI Namibia, the model will be handed over to the English language subgroup of AFROSAI, the African branch of the International Organisation of Supreme Audit Institutions (AROSAI-E) for further assessment and deployment. After a successful deployment of the model among SAI members under AFROSAI-E. Then after, AFROSAI-E will recommend the model to the International Organization of Supreme Audit Institutions (INTOSAI), which is an umbrella for AFROSAI to recommend and communicate it among its members, the Supreme Audit Institutions (SAIs) of countries around the globe, and with other international organisations and stakeholders in the field of government auditing. If the model needs to be modified, the researcher reserves the right to do so.

4.4 Chapter Summary

This chapter examines the research process used to develop the model, specifically focusing on the Design Science Research (DSR) approach. The chapter explained how the DSR approach was used to direct every stage of the model's creation, guaranteeing a well-organised and thorough process. The proposed model was meticulously constructed by following the fundamental elements of DSR, which encompass problem identification, objective definition, design and development, demonstration, assessment, and communication. Every element was carefully implemented to ensure that the model not only effectively tackles the research topic but also fulfils the practical requirements of the financial industry. The chapter also emphasised the utilisation of repeated cycles of design and evaluation to enhance the model, guaranteeing its relevance, applicability, and resilience. In summary, the chapter emphasised the significance of the DSR methodology in developing a robust, theoretically grounded, and practically feasible model for integrating digital forensics into information system audits in the financial sector. The insights gained from this chapter will be further distilled in the next chapter, which presents the conclusion and recommendations for future research and practice.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

The research study is concluded by this chapter, which presents the research contributions, reflections, lessons learned, research limits, future orientations, and final remarks. The research proposes the integration of digital forensics into financial information system audits which was accomplished by completing 4 objectives. Therefore, this chapter concludes the investigation by outlining the research contributions, reflection, lessons learned, research limitations, future directions, and concluding remarks.

5.1 Achievements of the Study Objectives

The main objective of the study was to develop a model that integrates digital forensics into the information systems audit process in a financial sector, with the goal of upholding confidentiality, integrity, and availability, it aims to ensure compliance with information technology activities aligned with company policies, industry best practices, and government laws and regulations. The model also intends to validate the evidence gathered during the audit by information system auditors. The main objective was reached after accomplishing five preliminary objectives, as delineated as follows:

5.1.1 To analyse how the current steps employed in the information system audit process guarantee the CIA of information systems and validate the evidence collected.

The study used a systematic and targeted literature review to understand how the current information system audit process works and how the collected evidence is validated. Literature from audit governing bodies such as ISACA (Information Systems Audit and Control Association), International Organization of Supreme Audit Institutions (INTOSAI), International Auditing and Assurance Standards Board (IAASB), Public Company Accounting Oversight Board (PCAOB), International Federation of Accountants (IFAC), and Information Systems Security Association (ISSA), among others. Based on the evidence-gathering techniques used in the fieldwork and Documentation of the Information audit process, the research concludes that the evidence-gathering techniques are not sufficient to conclude an audit with an unqualified audit opinion,

cannot provide assurance CIA of the data contained in the system, and cannot be relied on by financial audits. This research objective was met in Chapter 2, section 2.3, and concluded in the same chapter in Section 2.12. Literatures from IS audit governing bodies were selected for this objective as they represent the highest level of authority in the field, and these organizations are responsible for establishing and maintaining the globally recognized standards and frameworks that define the IS audit process. The study contributes by creating a model for efficiently incorporating digital forensics into information system audits. This model provides a systematic approach to incorporating digital forensic principles into the IS audit process, increasing the identification and response to security incidents and compliance concerns. Furthermore, the research fills a vacuum in the existing literature by investigating the convergence of digital forensics and information system audits, laying the groundwork for future research and development in this new topic.

5.1.2 To evaluate the standards IS auditors use when conducting IS audits.

The study used a systematic and targeted literature review to understand and evaluate the effectiveness of the standards used by the IS auditor on which they are benchmarking the audit criteria. The study findings indicated that various standards, such as ISACA's COBIT (Control Objectives for Information and Related Technologies), ISACA's ITAF (Information Technology Assurance Framework), The IIA's International Standards for the Professional Practice of Internal Auditing (Standards), ISO/IEC, and other applicable standards.

The study determined that the standards employed in Information System (IS) audits are exceedingly efficient as they offer a strong, industry-validated structure that guarantees uniform assessment of IT systems, governance, and security. By following these guidelines, IS auditors can methodically recognise and tackle hazards, guarantee adherence to regulatory obligations, and encourage ongoing enhancement in IT procedures. This results in IT environments that are more secure, efficient, and robust, eventually improving organisational trust and alignment with business objectives. The wide adoption and versatility of these standards in various industries further strengthen their efficiency in protecting and optimising IT systems. The research objective was met in Chapter 2, section 2.10 and concluded in the same chapter, section 2.12.

5.1.3 To design a model that integrates digital forensics into IS audit to ensure the confidentiality, integrity, and availability of information systems, as well as the validity of the evidence collected.

After the first two research objectives were met, the digital forensics components to be integrated were identified and discussed in Chapter 2 section 2.15. To meet this objective design science research methodology was employed as discussed in Chapter 3 Sections A and B. The Proposed Integrative Forensic Information System Audit Model (IFISAM) was developed as shown in Chapter 3 subsection 3.8.3.

5.1.4 To evaluate the proposed digital forensics-infused information systems audit process model.

After the design of the Proposed Integrative Forensic Information System Audit Model, it was evaluated using expert reviews. The Proposed Integrative Forensic Information System Audit Model was evaluated for its relevance, practicality, usability, applicability, and impact on which changes proposed by the reviewers were implemented. Lastly, the reviewers agree with the proposed model.

5.2 Research Contributions

The study contributes to both financial and information system audits through the proposed model, as it ensures unqualified audit opinions are provided to the stakeholders. The accumulation of sufficient, appropriate evidence is fundamental for drawing valid conclusions about the state of the information system. The quality of evidence will affect the quality of an audit's overall findings. Until now, in the information system audit field, there have been no standard techniques for gathering evidence, even though many research studies have been done to find effective techniques for conducting evidence-gathering in information system audits, and several studies have provided alternative techniques. However, there is no sign of a standard technique yet. Therefore, the proposed model has the potential to set standards for evidence-gathering techniques in information system audits. Overall, the study's contribution lies in its

practical application of the model to address pressing challenges in the financial sector, reinforcing the sector's ability to navigate complex cybersecurity landscapes and maintain regulatory compliance. Evidence-gathering techniques play a major role in ISA and financial audits; enhancing these techniques will improve decision-making and good financial governance, and better governance will increase transparency and accountability, and reduce corruption and misuse of funds.

5.3 Limitations

During the research processes, the following limitation was encountered:

5.3.1 Shortage of Literature on Information System Audit

There is a shortage of literature on Information System (IS) auditing due to the field's rapid evolution, the specialised and interdisciplinary nature of the work, and confidentiality issues over proprietary information. IS audit techniques frequently change in response to technology changes, making it challenging to keep up with the most recent, complete literature. Furthermore, the sector has historically gotten less academic attention, with a stronger emphasis on practical, hands-on expertise rather than theoretical research. Many best practices are also established and commercialised by consulting companies and vendors, which reduces the availability of thorough public literature. To overcome this limitation, the researcher subscribed to ISACA membership, allowing access to their publications on information system audits. This step was necessary due to the lack of sufficient academic publications from audit regulatory bodies.

5.4 Future Considerations

Some areas of interest for future work are:

Given that AI and ML are increasingly used in a variety of industries and are expected to be key economic drivers, their impact on ISA findings is profound. Specifically, AI and machine learning algorithms that can analyse enormous amounts of data faster and more correctly than previous approaches. This functionality enables auditors to discover patterns, abnormalities, and potential hazards more precisely. For example, AI can automate the detection of unexpected transactions or departures from anticipated behaviour, highlighting potential vulnerabilities that would

otherwise go unnoticed during manual review. As a result, the ISA process becomes more robust, allowing for earlier risk identification and mitigation, perhaps leading to more trustworthy audit conclusions and better overall risk management. Overall, AI should be integrated into the ISA process to improve risk assessment by predicting potential hazards based on past data, hence boosting the accuracy and reliability of audit results. Furthermore, by conducting case studies or pilot projects, researchers can compare the effectiveness of AI-driven audits to traditional methodologies. This analysis will look at how artificial intelligence improves the audit process, resulting in more credible audit reports and improved overall risk management.

5.5 Reflections

The research followed a systematic scientific approach and methodology. It began with a review of current literature to address the basic aims and develop a theoretical foundation. Following that, a model was created using Design Science Research Methodology and evaluated by experts in the field of information system audit and digital forensics.

5.6 Lessons learned

The study on the incorporation of Digital Forensics (DF) into Information System Audits (ISA) produced numerous significant insights:

5.6.1 Optimal Utilisation of Hypothetical Scenarios

The use of hypothetical scenarios was crucial in showcasing the actual use of the approach. This method offered a distinct and tangible illustration of how the model operates in a simulated setting, facilitating stakeholders' comprehension of its potential advantages and capabilities.

5.6.2 Significance of Design Science Research Methodology

The utilisation of Design Science Research Methodology demonstrated its effectiveness in developing a novel and functional model. This methodology enabled a systematic approach to developing models, guaranteeing that the answer was both theoretically rigorous and practically

feasible. It emphasised the significance of iterative development and improvement through expert feedback.

5.7 Concluding Remarks

The main aim of the study was to design a model for augmenting digital forensics into information system audit in the financial sector to ensure confidentiality, integrity, and availability (CIA) of information. The findings of the study showed that the evidence-gathering techniques used in the information system audit are insufficient; therefore, the study designed a model for integration. Additionally, the proposed model brings to light the need for DF in information system audits and the need for any audit institution to have a DF department.

Table 4 shows which sections of the research paper the research objectives were met.

Objectives	**Section**
Objective 1	Chapter 1, Section 2.12 a
Objective 2	Chapter 1, Section 2.12 b
Objective 3	Chapter 2, Sections 2.1, 2.14, and Chapter 3 section 3.8.3
Objective 4	Chapter 4, Section 4.2

Table 4: Addressed objectives

References

African Organisation of English-Speaking Supreme Audit Institutions [AFROSAI-E]. (2017). *IT AUDIT MANUAL (ITAM)* (1st ed.). AFROSAI-E. https://afrosai-e.org.za/wp-content/uploads/2019/07/IT-Audit-Manual-2017-1st-Edition.pdf

Ahn, E., & Lee, G. (2018). A Study on the Improvement of Domestic Internal Audit Technique Using Digital Forensics. *International Journal of Advanced Science and Technology*. https://doi.org/10.14257/ijast.2018.110.05

Ajijola, A., Zavarsky, P., & Ruhl, R. (2014). A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012. *World Congress on Internet Security (WorldCIS-2014)*. https://doi.org/10.1109/worldcis.2014.7028169

Alagić, A., Turulja, L., & Bajgorić, N. (2021). Identification of Information System Audit Quality

Alazab, A., Khraisat, A., & Singh, S. (2023). A review on the Internet of Things (IoT) forensics: challenges, techniques, and evaluation of digital forensic tools. *IntechOpen eBooks*. https://doi.org/10.5772/intechopen.109840

Almeida, P., De Abreu, J. F., Silva, T., Varsori, E., Oliveira, E., Velhinho, A., Fernandes, S., Guedes, R. M. C., & De Oliveira, D. B. C. (2018). Iterative user experience evaluation of a user interface for the unification of TV contents. In *Communications in computer and information science* (pp. 44–57). https://doi.org/10.1007/978-3-319-90170-1_4

Almeida, R., Lourinho, R., Da Silva, M. M., & De Sousa Pereira, R. F. (2018). A model for assessing COBIT 5 and ISO 27001 simultaneously. *ResearchGate*. https://www.researchgate.net/publication/326507013

American Institute of Certified Public Accountants (AICPA). 2012. Statement on Auditing Standards No. 122, AU-C Section 500: Audit Evidence. New York.

American Institute of Certified Public Accountants [AICPA]. (2015). *AUDIT ANALYTICS CONTINUOUS AUDIT: Looking Toward the Future*. imc.

and Mixed Methods Approaches. 4th Edition, Sage, Newbury Park.

Andiola, L. M., Downey, D., Earley, C. E., & Jefferson, D. (2021). Wealthy Watches Inc.: The Substantive testing of accounts receivable in the evolving audit environment. *Issues in Accounting Education*, *37*(2), 37–51. https://doi.org/10.2308/issues-2020-037

Antunes, M., Maximiano, M., & Gomes, R. (2022). A Client-Centered Information Security and Cybersecurity Auditing framework. *Applied Sciences*, *12*(9), 4102. https://doi.org/10.3390/app12094102

Aprilinda, Y., Puspa, A. K., & Affandy, F. N. (2019). The use of ISO and COBIT for IT governance audit. *Journal of Physics: Conference Series*, *1381*(1), 012028. https://doi.org/10.1088/1742-6596/1381/1/012028

Berrisford, A. J. (2012). Smart Meters should be smarter. *2012 IEEE Power and Energy Society General Meeting, Power and Energy Society General Meeting, 2012 IEEE*, 1–6. https://doi.org/10.1109/PESGM.2012.6345146

Brocke, J. V., Hevner, A. R., & Maedche, A. (2020). Introduction to Design Science Research. In *Progress in IS* (pp. 1–13). Springer International Publishing. https://doi.org/10.1007/978-3-030-46781-4_1

Brocke, J. V., Winter, R., Hevner, A. R., & Maedche, A. (2020). Special issue Editorial – Accumulation and Evolution of Design Knowledge in Design Science Research: A Journey Through Time and Space. *Journal of the Association for Information Systems*, *21*(3), 520–544. https://doi.org/10.17705/1jais.00611

Brown-Liburd, H. L., & Vasarhelyi, M. A. (2015). Big data and audit evidence. *Journal of Emerging Technologies in Accounting, 12(1), 1–16. https://doi.org/10.2308/jeta-10468*

Calder, A., & Watkins, S. (2015). *IT governance: An International Guide to Data Security and ISO27001/ISO27002* (6th ed.). Kogan Page.

Casey, E. (2011). *Digital Evidence and Computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press. http://ci.nii.ac.jp/ncid/BB06007590

Casey, E., & Rose, C. W. (2010). Forensic analysis. In *Elsevier eBooks* (pp. 21–62). https://doi.org/10.1016/b978-0-12-374267-4.00002-1

Chimwanda, E. (2022). Essentials for an Effective Cybersecurity Audit. *ISACA Journal*, *2022*. https://www.isaca.org/resources/news-and-trends/industry-news/2022/essentials-for-an-effective-cybersecurity-audit

Christianto, K., Gunadi, J., Ferdinal, R., & Hendrawan, T. F. (2022). Audit of Finance Application using COBIT 5 Framework (Case Study in Banking). *ResearchGate*.

Cooke, I. (2018). IS Audit Basics: Innovation in the IT Audit Process. *ISACA Journal*, *2*(2018). https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/is-audit-basics-innovation-in-the-it-audit-process

Cooke, I., & Raghu, R. V. (2019). IS Audit Basics: Auditing Cybersecurity. *ISACA Journal*, *2*(2019). https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/is-audit-basics-auditing-cybersecurity

Ćosić, J., & Bača, M. (2010). Improving chain of custody and digital evidence integrity with time stamp. In *International Convention on Information and Communication Technology, Electronics and Microelectronics* (pp. 1226–1230). http://ieeexplore.ieee.org/document/5533653/

Ćosić, J., & Ćosić, Z. (2012). Chain of custody and life cycle of digital evidence. *ResearchGate*. https://www.researchgate.net/publication/279175015

Creswell. J.W. and Creswell, J.D. (2017) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4th Edition, Sage, Newbury Park.

Davies, D. (2022, August 24). *Digital Transformation & Innovation in Auditing: Insights from a Review of Academic Research*. IFAC. https://www.ifac.org/knowledge-gateway/discussion/digital-transformation-innovation-auditing-insights-review-academic-research

Deloitte Touche Tohmatsu [Deloitte]. (2023).Stepping into the Future of Cyber - Financial Services. *Deloitte*. https://www.deloitte.com/global/en/services/risk-advisory/blogs/stepping-into-the-future-of-cyber-financial-services.html

Deng, Q., & Ji, S. (2018). A review of Design Science Research in Information Systems: Concept, Process, Outcome, and Evaluation. *Pacific Asia Journal of the Association for Information Systems*, 1–36. https://doi.org/10.17705/1pais.10101

Drljača, D., & Latinović, B. (2017). Frameworks for audit of an information system in Practice. *Journal of Information Technology and Applications*, *12*(2). https://doi.or/10.7251/jit1602078d

Force, J. T. (2018). *Risk management framework for information systems and organizations:* https://doi.org/10.6028/nist.sp.800-37r2

Force, J. T. (2020). *Security and privacy controls for information systems and organizations*. https://doi.org/10.6028/nist.sp.800-53r5

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *Management Information Systems Quarterly*, *37*(2), 337–355. https://doi.org/10.25300/misq/2013/37.2.01

Guttman, B., & White, D. R. (2022). *Digital evidence preservation: Considerations for Evidence Handlers* (NIST Interagency Report NIST IR 8387). NIST. https://doi.org/10.6028/nist.ir.8387

Harrison, H., Birks, M., Franklin, R. C., & Mills, J. (2017). Case Study Research: Foundations and Methodological Orientations. *FQS*, *18*(1), 17. https://doi.org/10.17169/fqs-18.1.2655

Hevner, A. R., & Chatterjee, S. (2010). Design research in information systems. In *Integrated series on information systems/Integrated series in information systems*. https://doi.org/10.1007/978-1-4419-5653-8

Hevner, March, Park, H., & Ram. (2004). Design science in Information Systems Research. *Management Information Systems Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

Hevner, March, Park, H., & Ram. (2004). Design science in Information Systems Research. *Management Information Systems Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

Information Systems Audit and Control Association [ISACA]. (2019). *CISA Review Manual* (27th ed.). ISACA.

Information Systems Audit and Control Association [ISACA]. (2020). State of Cybersecurity 2020. In *The Impact of Uncertain Times.* ISACA. *Information Systems Research Seminar in Scandinavia*, The IRIS Association, Haikko

Isaca. (2018). *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution*. Isaca.

Isaca. (2018). *COBIT 2019 Framework: Introduction and Methodology*. Isaca.

Isaca. (2019). *CISA Review Manual, 27th Edition*.

ISO 27001 simultaneously. *ResearchGate*. https://www.researchgate.net/publication/326507013

Jansen, W., & Ayers, R. P. (2004). *Guidelines on PDA forensics*. https://doi.org/10.6028/nist.sp.800-72

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-Art, tools, techniques, challenges, and future directions. *IEEE Access*, *10*, 11065–11089. https://doi.org/10.1109/access.2022.3142508

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems. *MIS Quarterly*, *12*(4), 571–586. Retrieved from http://www.jstor.org

Kassa, S. G. (2016b). Information Systems Security Audit: an ontological framework. *ISACA Journal*, *5*(2016). https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/information-systems-security-audit-an-ontological-framework

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response*. https://doi.org/10.6028/nist.sp.800-86

Khan, A. K., & Zimmer, E. C. (2016). *Audit Analytics: A Framework for Control Enhancing Assurance*. Lulu.com.

Kim, M., Shin, Y., Jo, W., & Shon, T. (2022). Digital forensic analysis of intelligent and smart IoT devices. *˜the œJournal of Supercomputing/Journal of Supercomputing*, *79*(1), 973–997. https://doi.org/10.1007/s11227-022-04639-5

Krombholz, K., Hobel, H., & Huber, M. (2015). Research on the Detection of Web Vulnerabilities in Practice: A Survey. *International Journal of Information Security*, *14*(3), 199–223.

Kuechler, B., & Vaishnavi, V. (2008). On theory development in design science research: anatomy of a research project. *European Journal of Information Systems*, *17*(5), 489–504. https://doi.org/10.1057/ejis.2008.40

Lu, Z., & So, E. (2010). A proposal for verifying the performance specifications of certain functions of smart meters in distribution power line networks. *Precision Electromagnetic Measurements (CPEM), 2010 Conference on, 271–272*. https://doi.org/10.1109/cpem.2010.5544816

Mantha, B. R. K., & De Soto, B. G. (2021). Cybersecurity in construction: Where do we stand and how do we get better prepared. *Frontiers in Built Environment*, *7*. https://doi.org/10.3389/fbuil.2021.612668

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Miranda, N. B., Rodavia, M. R., & Miranda, M. I. (2019). IT Infrastructure Auditing using COBIT Framework. *2019 6th International Conference on Technical Education (ICTechEd6)*. https://doi.org/10.1109/icteched6.2019.8790861

Moore, P. W. H. (2023). Can litigation Analytics tell us whatever became of the 2015 proportionality amendments to the Federal Rules of Civil Procedure? *Social Science Research Network*. https://doi.org/10.2139/ssrn.4623622

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a design science research process.

Proceedings of the 4th International Conference on Design Science Research in Informa tion Systems and Technology. https://doi.org/10.1145/1555619.1555629

Özkan, U. B. (2023). Validity and Reliability in Document Analysis Method: A theoretical review in the context of educational. . . *ResearchGate*. https://www.researchgate.net/publication/376787211_Validity_and_Reliability_in_Document_Analysis_Method_A_Theoretical_Review_in_the_Context_of_Educational_Science_Research

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *ResearchGate*. https://www.researchgate.net/publication/284503626

Pries-Heje, J., Baskerville, R., & Venable, J. R. (2008). Strategies for Design Science Research Evaluation. AIS Electronic Library (AISeL). https://aisel.aisnet.org/ecis2008/87

Quick, R., & Henrizi, P. (2018). Experimental evidence on external auditor reliance on the internal audit. *Review of Managerial Science*, *13*(5), 1143–1176. https://doi.org/10.1007/s11846-018-0285-0

Radovanovic, D., Radojević, T., Lucic, D., & Šarac, M. (2010). IT audit in accordance with Cobit standard. *ResearchGate*. https://www.researchgate.net/publication/224162993

Rossi, M., and Sein, M.K. "Design research workshop: a proactive research approach," in: *26th Information Systems Research Seminar in Scandinavia, The IRIS Association, Haikko Finland, 2003.*

Røstad, L., & Edsberg, O. (2006). A study of access control requirements for healthcare systems based on audit trails from access logs. *22nd Annual Computer Security Applications Conference (ACSAC 2006)*. https://doi.org/10.1109/acsac.2006.8

Rozario, A. M., & Thomas, C. (2019). Reengineering the Audit with Blockchain and Smart Contracts. *Journal of Emerging Technologies in Accounting*, *16*(1), 21–35. https://doi.org/10.2308/jeta-52432

Rouse, S. V. (2016). Of Teacups and t Tests: Best Practices in Contemporary Null Hypothesis Significance Testing. *Psi Chi Journal of Psychological Research*, *21*(2), 127–133. https://doi.org/10.24839/2164-8204.jn21.2.127

Rusman, A., Nadlifatin, R., & Subriadi, A. P. (2022b). Information System Audit using COBIT and ITIL Framework: Literature review. *Sinkron : Jurnal Dan Penelitian Teknik Informatika*, *7*(3), 799–810. https://doi.org/10.33395/sinkron.v7i3.11476

Sadiku, M. N. O., Shadare, A. E., & Musa, S. M. (2017). Digital chain of custody. *International Journal of Advanced Research in Computer Science and Software Engineering*, *7*(7), 117. https://doi.org/10.23956/ijarcsse.v7i7.109

Samarakoon, K. W., Ekanayake, J., & Wu, J. (2010). Smart metering and self-healing of distribution networks. *2010 IEEE International Conference on Sustainable Energy Technologies (ICSET)*. https://doi.org/10.1109/icset.2010.5684937

Sayana, A. (2022). The evolution of Information Systems Audit. *ISACA Journal*, *1*(2022). https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/the-evolution-of-information-systems-audit

Singleton, T. W. (2012). Evaluating access controls over data. *ISACA*, *1*(2012). https://www.isaca.org/resources/isaca-journal/past-issues/2012/evaluating-access-controls-over-data

Siponen, M. T., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *Management Information Systems Quarterly*, *34*(3), 487. https://doi.org/10.2307/25750688

Shadiev, R., Hwang, W., Yeh, S., Yang, S. J. H., Wang, J., Han, L., & Hsu, G. (2014). Effects of Unidirectional vs. Reciprocal Teaching Strategies on Web-Based Computer Programming Learning. *Journal of Educational Computing Research*, *50*(1), 67–95. https://doi.org/10.2190/ec.50.1.d

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Suryani, N. P. S. M., Ardiada, I. M. D., & Janardana, I. G. N. (2018). Audit of Governance Information Technology Services Using ITIL v3 Focuses on Service Operation Domain in. . . *ResearchGate*. https://www.researchgate.net/publication/346515506

Thanh, N. C., & Thanh, T. T. (2015). The interconnection between interpretivist paradigm and qualitative methods in education. *American Journal of Educational Science*, *1*(2), 24–27.

Tory, M., & Moller, T. (2005). Evaluating visualizations: do expert reviews work. *IEEE computer graphics and applications*, *25*(5), pp. 8–11.

Tory, M., & Möller, T. (2005). Evaluating visualizations: do expert reviews work? *IEEE Computer Graphics and Applications*, *25*(5), 8–11. https://doi.org/10.1109/mcg.2005.102

Vadacchino, V., Denda, R., & Fantini, G. (2013). First results in ENDESA smart metering roll-out. *22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013)*. https://doi.org/10.1049/cp.2013.0850

Whitman, M. E., & Mattord, H. J. (2018). *Management of information security* (6th ed.). Cengage Learning.

Wicaksono, A., Laurens, S., & Novianti, E. (2018). *Impact Analysis of Computer Assisted Audit Techniques Utilization on Internal Auditor Performance*. https://doi.org/10.1109/icimtech.2018.8528198

Wynn, D. C., & Eckert, C. (2016). Perspectives on iteration in design and development. *Research in Engineering Design*, *28*(2), 153–184. https://doi.org/10.1007/s00163-016-0226-3

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer Forensics investigation models. *International Journal of Computer Science and Information Technology/International*

Journal of Computer Science and Information Technology (Chennai. Print), *3*(3), 17–31. https://doi.org/10.5121/ijcsit.2011.3302

Zhang, M. (2022). Forensic imaging: a powerful tool in modern forensic investigation. *Forensic Sciences Research*, *7*(3), 385–392. https://doi.org/10.1080/20961790.2021.2008705

Zhang, Z., Lee, W., Wetz, D. A., Shrestha, B., Shi, J., Jackson, A., Honang, H., & Fielder, J. (2014). Evaluation of the switching surges generated during the installation of legacy and smart electric metering equipment. *IEEE Transactions on Industry Applications*, *50*(3), 2164–2172. https://doi.org/10.1109/tia.2013.2288424

APPENDIX A: EXPERT REVIEW QUESTIONNAIRE

<this questionnaire was not handed to the expert reviewers. It was used by the researcher as a guidance in a round table discussion with the reviewers>

DESIGN OF A MODEL FOR AUGMENTING DIGITAL FORENSICS INTO INFORMATION SYSTEM AUDIT IN THE FINANCIAL SECTOR

This study is aimed to develop a model that seamlessly integrates digital forensics into the information systems audit process in a financial sector, to uphold confidentiality, integrity, and availability, it aims to ensure compliance with Information Technology activities aligned with company policies, industry best practices, and government laws and regulations. The model also intends to validate the evidence gathered during the audit by Information System Auditors.

SECTION A: Demographic

1. What is your current Position?

   _____

2. For how long you have been in that position and what are your total years of experience?

   _____

   _____

   _____

3. List all the relevant qualifications you currently have.

_____

_____

_____

SECTION B: PRESENTATION

The researcher will present the model to the expert before commencing with asking them questions.

SECTION C: QUESTIONS AFTER PRESENTATIONS

As an expert, answer this question positively and negatively, this is the external audit we are referring to not the internal audit to give you details on what was integrated into Information system audits are digital forensic imaging and digital forensics analysis. The purpose is to evaluate the model.

DESIGN OF A MODEL FOR AUGMENTING DIGITAL FORENSICS INTO INFORMATION SYSTEM AUDIT IN THE FINANCIAL SECTOR

1. Does the model address the issue of evidence-gathering techniques in the information system audit?

   Scale of Agreement

   Strongly Agree ☐ Agree ☐ Partially Agree ☐ Disagree ☐

2. What key considerations and challenges need to be addressed to successfully implement the proposed model?

3. Can a model be easily implemented in the real-world world to in any IT environment and achieve the intended results to support financial audits and produce a qualified audit opinion?

Scale of Agreement

Strongly Agree ☐ Agree ☐ Partially Agree ☐ Disagree ☐

4. Is the model user-friendly and easy to understand for information system auditors?

Scale of Agreement

Strongly Agree ☐ Agree ☐ Partially Agree ☐ Disagree ☐

5. By following the proposed model steps, does it demonstrably improve the effectiveness and efficiency of information system audits in the financial sector?

Scale of Agreement

Strongly Agree ☐ Agree ☐ Partially Agree ☐ Disagree ☐

SECTION D: DISCUSSIONS

This section allows experts to analyze the content thoughtfully, providing valuable perspectives, feedback, and suggestions that can improve the quality, relevance, and effectiveness of the proposed model. Its purpose is to gain a better understanding of the model's functionality and to consider additional factors that were not included in the initial review but are important to consider.

APPENDIX B: Selected publications used in answering research questions one and two

No	Authors	Title	Published by
1	Information Systems Audit and Control Association [ISACA]. (2019)	*CISA Review Manual* (27th ed.). ISACA.	ISACA
2	Suryani, N. P. S. M., Ardiada, I. M. D., & Janardana, I. G. N. (2018)	Audit of Governance Information Technology Services Using ITIL v3 Focuses on Service Operation Domain in X Institution	CISA
3	Rusman, A., Nadlifatin, R., & Subriadi, A. P. (2022b)	Information System Audit using COBIT and ITIL Framework: Literature review	CISA
4	Force, J. T. (2018)	*Risk management framework for information systems and organizations*	NIST
5	African Organisation of English-Speaking Supreme Audit Institutions [AFROSAI-E]. (2017).	*AUDIT MANUAL (ITAM)* (1st ed.)	AFROSAI-E
6	Miranda, N. B., Rodavia, M. R. D., & Miranda, M. I. (2019)	IT infrastructure auditing utilising the COBIT Framework.	CISA
7	Isaca (2018)	*COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution*	ISACA
8	Christianto, K., Gunadi, J., Ferdinal, R., & Hendrawan, T. F. (2022)	Audit of Finance Application using COBIT 5 Framework	CISA
9	Almeida, R., Lourinho, R., Da Silva, M. M., & De Sousa Pereira, R. F. (2018)	A model for assessing COBIT 5 and ISO 27001 simultaneously	CISA
10	Aprilinda, Y., Puspa, A. K., & Affandy, F. N. (2019).	The use of ISO and COBIT for IT governance audit	CISA
11	Radovanovic, D., Radojević, T., Lucic, D., & Šarac, M. (2010)	IT audit in accordance with Cobit standard.	CISA
12	Antunes, M., Maximiano, M., & Gomes, R. (2022).	A Client-Centered Information Security and Cybersecurity	CISA
13	Kassa, S. G. (2016)	Information Systems Security Audit: An Ontological Framework.	ISACA & Written by ISACA members
14	Khan, A. K., & Zimmer, E. C. (2016)	*Audit Analytics: A Framework for Control Enhancing Assurance*	CISA

15	Sayana, A. (2022)	The evolution of Information Systems Audit	ISACA & ISACA members
16	Cooke, I., & Raghu, R. V. (2019)	IS Audit Basics: Auditing Cybersecurity	ISACA & ISACA members
17	Cooke, I. (2018)	IS Audit Basics: Innovation in the IT Audit Process.	ISACA & ISACA members
18	Chimwanda, E. (2022)	Essentials for an Effective Cybersecurity Audit.	ISACA & ISACA members
19	Isaca. (2018)	*COBIT 2019 Framework: Introduction and Methodology*.	ISACA
20	Force, J. T. (2020)	*Security and privacy controls for information systems and organizations*.	NIST
21	Calder, A., & Watkins, S. (2015)	*IT governance: An International Guide to Data Security and ISO27001/ISO27002*	IT Governance Publishing
22	Isaca. (2019)	*CISA Review Manual, 27th Edition*.	ISACA
23	[AFROSAI-E]. (2017)	*IT AUDIT MANUAL (ITAM)*	AFROSAI-E
24	American Institute of Certified Public Accountants [AICPA]. (2015)	*AUDIT ANALYTICS and CONTINUOUS AUDIT:*	AICPA
25	PWC, (2013)	Understanding a financial statement audit.	PWC
26	American Institute of Certified Public Accountants (AICPA). 2012.	Statement on Auditing Standards	AICPA
27	Brown-Liburd, H. L., & Vasarhelyi, M. A. (2015)	Big data and audit evidence. *Journal of Emerging Technologies in Accounting*	Journal of Emerging Technologies in Accounting
28	Drljača, D., & Latinović, B. (2017)	Frameworks for audit of an information system in Practice. *Journal of Information Technology and Applications*	CISA