Arab American University – Palestine

Faculty of Graduate Studies

Digital Forensics Framework for Early Detection and Response to Internal Cybersecurity Incidents in Financial Environment.

By

Ahmad Nizar Mousa Abu Eisheh

Supervisor

Dr. Majdi Owda

Co-Supervisor

Dr. Amani Owda

This Thesis Was Submitted in Partial Fulfillment of the Requirements for the

Master's Degree in Cybercrimes and Digital Evidence Analysis.

July / 2023

Thesis Approval

Digital Forensics Framework for Early Detection and Response to Internal Cybersecurity Incidents in Financial Environment.

By

Ahmad Nizar Mousa Abu Eisheh

This Thesis was Defended Successfully on the 5th of July 2023 and Approved by:

Committee members	Signature
1. Dr. Majdi Owda	
2. Dr. Amani Owda	
3. Internal Examiner: Dr. Huthaifa Ashqar	
4. External Examiner: Dr. Mohammed Hussien	M.Hussein

Declaration

I declare that the thesis titled "Digital Forensics Framework for Early Detection and Response to Internal Cybersecurity Incidents in Financial Environment" is my work, has been composed solely by myself and does not contain work from other researchers, and has not been submitted for any other degree or scientific work except the reference is made.

Name: Ahmad Nizar Mousa Abu Eisheh

Signature:

Date: 12/09/2023

Student ID: 202012730

Dedication

I dedicate this thesis to my family and friends for their unconditional love and support. To my mother and my father, for their unlimited support, which has not left me throughout my life. Also, I dedicate this thesis to my little daughter "Meryama", the most beautiful thing that happened in my life. To my dear friends and work colleagues, for their continued support throughout my learning and work journey.

Acknowledgments

I would like to use this space to express my deep gratitude to Dr. Majdi Owda and Dr. Amani Owda for their advice, help, and valuable time, which they spent reviewing and correcting my work. Dr. Majdi & Dr. Amani provided useful suggestions and advice that have had an important effect and helped in overcoming many obstacles in preparing this work in the best way possible.

Abstract

The cyberspace and technology environment, especially within the financial sector are subject to cyberattacks and malicious activities initiated by insider or outsider perpetrators motivated by malicious intents. While insider malicious forms the biggest risk to organizations, effective handling of their activities is considered very important to reveal incident information and protect origination's digital assets, which requires designing a reliable process for digital investigation and incident responses to insider activity within an organization’s digital environment.

This dissertation presents a conceptual forensic framework used in the early detection and response to insider malicious activities, within the financial sector. By adapting grounded theory as a systematic qualitative research and data collection methodology, the proposed framework model was developed by examining and enhancing several generic digital forensic and incident response models encountered within current literature comprehensive research. As well as by exploring current international practices of cybersecurity incident response and digital forensics through assessment surveys, to introduce proper enhancements to current frameworks.

The proposed framework is supported by five essential pillars and consists of (14) sub-requirements (pillars enablers) and (134) processes (to-do- list). The resulting framework was validated by an expert focus group, tested, and found effective and efficient for insider threat activities detection and response within the financial sector. The outcome and scientific contribution of the proposed framework, are achieved by providing the organization's cyber professionals, with a novel framework to assist them during the cyber investigation process followed by insider security incidents. As well as filling the gap within the majority of generic digital forensics frameworks by designing dedicated novel framework for the financial sector.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ADFM	Abstract Digital Forensic Model
CD ROM	Compact Disc Read-Only Memory
CERT	Computer Emergency Response Team
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
COBIT	Control Objectives for Information and Related Technologies
CSIRT	Cyber Security Incident Response Team
DF	Digital Forensics
DFIR	Digital Forensics and Incident Response
DFRWS	Digital Forensic Research Workshop
DLP	Data Loss Prevention
EDA	Exploratory Data Analysis
EDR	Endpoint Detection and Response
EIDIPM	Enhanced Integrated Digital Investigation Process Model
EMCI	Extended Model of Cybercrime Investigations
EP	Endpoint
FI	Financial Institutions
FIM	File Integrity Monitoring
FTP	File Transfer Protocol
HW	Hardware
IDIPM	Integrated Digital Investigation Process Model
IDS	Intrusion Detection System
IMF	International Monetary Fund
IOA	Indicator of Attack

IOC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
KRI	Key Risk Indicator
Malware	Malicious Software
NIST	The American National Institute of Standards and Technology
NIST CSF	NIST Cybersecurity Framework
PAM	Privileged Access Management
PMA	Palestine Monetary Authority
PMA CSF	PMA Cybersecurity Framework
PCI DSS	Payment Card Industry Data Security Standard
PIR	Post Incident Review
RDP	Remote Desktop Protocol
SANS	SysAdmin, Audit, Network, and Security
SHA	Secure Hashing Algorithm
SIEM	Security Information and Event Management
SOC	Security Operation Center
SP	Special Publication
SRDFIM	Systematic Digital Forensic Investigation Model
SW	Software
SWIFT	Society for Worldwide Interbank Financial Telecommunications

SWIFT CSP	Swift's Customer Security Program
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TOR	Onion Routing Network
USB	Universal Serial Bus
UTM	Unified Threat Management
VPN	Virtual Private Network
WAF	Web Application Firewall
ZT	Zero Trust

Chapter 1

1. Introduction

1.1 Introduction to Digital Forensics

Digital forensics, shortly “DF” is defined by the “American National Institute of Standards and Technology”, shortly “NIST” as "the application of science to the identification, collection, examination, and analysis, of data while preserving the integrity of the information and maintaining a strict chain of custody for the data" [1].

Digital forensics is considered a formal process to identify, collect, examine, and analyze incident information and evidence in the digital world, one of the most related and applicable areas of interest to digital forensics is investigating, collecting, and analyzing incident evidence from the cybersecurity world[2].

Cyberspace and its environment especially in financial sector organizations are subject to various cyberattacks and incidents initiated by internal and external perpetrators for several purposes (i.e. Intentional destruction of assets, gaining benefits… etc.). Such incidents should be deeply detected, investigated, and responded to, through a formal and well-designed process model to effectively collect and analyze all related information to such attack incidents [3].

External and outsider expert attackers aren’t the source of the only threat that modern organizations need to consider in their strategic cybersecurity planning. Insider malicious is a serious and growing risk to organizations. As the “2022 Cost of Insider Threats [4]: Global

Report reveals", insider threat security incidents have risen 44% over the past two years, with total costs per each incident up more than a third to $15.38 million. The bellow list highlights the major report's cost of breach conducted by insider threats :

- The cost of credential theft to organizations increased 65% from $2.79 million in 2020 to $4.6 million at present.
- The time to contain an insider threat incident increased from 77 days to 85 days, leading organizations to spend the most on containment.
- Incidents that took more than 90 days to contain cost organizations an average of $17.19 million on an annualized basis.

Handling cyber security incidents is a very important process to reveal incidents of information committed by perpetrators within financial origination's digital environment. Such a handling process requires deep forensics and investigation practices within different digital network components [5]. These forensics practices should be well defined, organized, and enforced by designing a conceptual digital forensics framework for detection and response to internal cybersecurity incidents. This is the core goal and idea behind our proposed research topic.

This chapter includes a conceptual introduction to Digital forensics, in addition to the following sub-sections:

- Section 1.2, presents the research motivations and problem statement.
- Section 1.3, presents the research aim and objectives.
- Section 1.4, presents the research's main question and sub-questions.
- Section 1.5, presents the thesis organization and chapter overview.
- Section 1.6, presents the chapter Chapter Conclusions and Summary.

1.2 Research Motivations and Problem Statement

The study was motivated by the current gap and lack of comprehensive forensics and investigations framework that financial services firms can employ for detection and response to insider cybersecurity incidents.

Considering the current gap, as well as the fact that the financial sector is an attractive target for experienced attackers who use sophisticated techniques to commit cyber-attacks within this critical sector, forms a significant research problem that cannot be addressed until this research is conducted.

1.3 Research Aim and Objectives

The major aim of this proposed study and research is to provide organizations' cyber security professionals, forensics investigators, and incident handling teams, within the financial sector, with a digital forensics framework and process model to assist them during the cyber investigation process followed by internal cyber incidents. The proposed model also aims to provide the financial sector organizations with well-designed and mature digital forensics and incident response, shortly the "IR" capability model, to ensure early detection and effective responses to internal cybersecurity incidents, as well as reduce and mitigate the potential impact and consequences of incidents on time. In some scenarios, prevent its occurrence. The objectives of the research that support achieving the research aims are as follows:

- **To conduct comprehensive data collection and analysis**: this objective will be achieved by conducting the following phases:
  - ✓ Conducting a comprehensive literature review from several research resources and publications (journals, conferences, books, standards, good practices) in the field of DF

and IR with more than 100 diverse papers and published data to identify the gap in current literature as well as extracting relevant processes from identified source models and grounded literature into the proposed framework.

- ✓ Develop an assessment questionnaire, to understand the actual practice, capabilities, and real needs in the area of cyber security, incident response, and digital forensics within the financial sector, and to explore missing data within the current literature. Survey responses were collected from sample financial institutions from different countries (inside and outside Palestine with 21 participant banks and payments companies) to introduce all possible enhancements into the extracted process as well as to fill any gaps and process missing processes extracted within prior steps.
- ✓ Identifying the baseline and essential model processes, requirements, and readiness factors required for developing forensics frameworks for the financial sector.
- ✓ Identifying source frameworks model that supports baseline framework requirements.

- **To develop a comprehensive state of art integrated digital forensics framework and process model for the financial sector**: this objective will be achieved by conducting the following phases:
  - ✓ Conducting framework model development based on the extracted core digital forensics and incident response processes, sub-processes, and other typical digital forensics and incident response framework components, that were extracted from the literature reviews, and based on identified digital forensics framework baseline and essential requirements.

- ✓ Enhancing the extracted processes by extraction of actual DF and IR practices collected by financial sector institutions through exploratory surveys to enhance the extracted process.

- **To conduct in-depth forensics framework validation and testing**: this objective will be achieved by conducting the following phases:
  - ✓ Conduct comprehensive theoretical model validation by using a focus group in the form of online interviews with an expert group of cyber and digital forensics professionals (focus group) to validate and revise the theoretical part of the proposed framework. (framework validated without changes).
  - ✓ Identifying framework technical implementation requirements and proper implementation models. and technically testing framework by conducting testing simulation scenarios based on NIST Framework.

1.4 Research Question

This study will answer the questions on what the major process and forensics model elements should be developed to ensure proper integration between the DF process and the information security incident handling process to ensure early and effective detection and response to internal cybersecurity incidents within financial organizations. Below are the research sub-questions:

- What is the maturity level of cybersecurity and forensics practices in the financial sector?
- Is there an actual gap in knowledge within this area of study and the financial sector?
- Is the resulting process model valid and relevant for the use of the financial sector?

1.5 Thesis Organization and Chapters Overview

To achieve the defined research aims and objectives stated within section 1.3, this dissertation has been organized into seven chapters as follows:

Chapter 1: Introduction

The current chapter includes an introduction, motivation for the study, problem statement, and research objectives. The high-level research methodology is presented.

Chapter 2: Literature Review

This chapter presents a summary and analysis of the relevant publications on thesis topics on digital forensics and incident response framework and the integrations between current models.

Chapter 3: Research Strategy and Data Collection Methods

This chapter explains the researcher's approach to answering the research questions and explains the most appropriate research strategy and data collection methods for the proposed research.

Chapter 4: Data Collection and Exploratory Data Analysis

This chapter describes the data analysis and explains how the researcher used grounded theory and theory techniques to analyze the collected data.

Chapter 5: The Methodology and Framework Development

This chapter describes the methodology followed for the framework development process.

Chapter 6: Results, Discussion, and Framework Validation

This chapter presents and discusses a summary of the research results, as well as the framework validation, implementation, and testing process (theoretical and technical validation).

Chapter 7: Conclusion and Future Work

This chapter presents research conclusions, community contributions, and recommendations.

1.6 Chapter Conclusions and Summary

This chapter identified a conceptual introduction to Digital forensics, in addition, this chapter covered the following items relevant to research:

- The research motivations and problem statement.
- The research aims and objectives.
- The research's main question and sub-questions.
- The thesis organization and chapter overview.

The next chapter **(**chapter 2**)** presents a summary and analysis of the relevant publications on these thesis topics about digital forensics framework for early detection and response to internal cybersecurity incidents in the financial environment

Chapter 2

2. Literature Review

2.1 Introduction

This chapter presents a summary and analysis of the relevant publications on these thesis topics about digital forensics framework for early detection and response to internal cybersecurity incidents in the financial environment

2.2 Background

Cybersecurity incident responses and digital forensics and investigations are two related, coherences, and integrated topics. In cybersecurity incident responses and cybercrime methodology, the major concern is looking for evidence, examining what happened, and mitigation of the incident consequences. Digital forensics works to investigate, rebuild the incident, and collect proper evidence to reveal and examine the incident's root causes. [6].

In-depth research was conducted on the digital forensics process, information security incident handling process, and the integration between two process models within the financial sector, as well as in-depth research on several sub-topics related to research to draw a broader perspective on the research topic.

2.3 Digital Forensic Within Financial Sector

2.3.1 The Need for Forensics Investigations Within the Financial Sector

The global financial sector institutions rely drastically and extensively on technology development and information systems for operating business, serving customers as well and protecting internal and external business environments. Such dependence ensures its ability to deliver state-of-the-art digital services as well as preserve its competitive advantages within the financial global market [7].

Because of their growing dependence on information systems and digital technologies as well as moving into financial technologies in delivering their financial services, the financial fraud landscape, and crime scene were moved from the traditional scene into the digital one which is more flexible to exploited and harder to detect. Making the majority of organizations in general, and financial services institutions in particular, more vulnerable to the effects of cybercriminals attacks, disgruntled employees, hacktivists, and government hackers, who attempt to access an organization's computer systems to steal valuable information [8].

Thus the accelerated and sophisticated level of malicious cyber activity against financial organizations, as well as the constant barrage of cyber-attacks, forms unique challenges for organizations' digital investigators and cybersecurity professionals [9].

Cybercriminals, regardless of their relation to the organization (whether they are internal or external), and motivated by financial gains, form the most apparent and the most persistent threat to financial services institutions, as to the "Society for Worldwide Interbank Financial Telecommunications", shortly "SWIFT" recently published assessment report [10].

2.3.2 Digital Forensic Regulations and Legislations Within Financial Sector

Many organizations worldwide have sector-specific regulations and legislation that they are obliged to comply with. Within financial sector organizations, it is usually governed and operates under full strict control and supervision of the central banks and the “International Monetary Fund”, shortly “IMF”, thus the central banks and IMF is the regulatory body for all regulations and laws governing the financial service organization [11]. Due to the nature and criticality of its core business and financial services provided by them. Hence it should be in full compliance with all regulatory requirements posed by the central bank.

One of the most financial industry-related IR and DF models is the "common process model for incident response and digital forensics” [12]. The use of the proposed model was recommended by the IMF, as one of the IMF 2007 annual conference action items agenda. As illustrated in Figure 2.1. This model aims to investigate computer security incidents as well as integrate forensic investigation into computer incident response procedures.

The proposed model consists of the following process:

- Pre-analysis phase
- Analysis phase
- Post analysis phase

In 2008, the “Payment Card Industry Security Standards Council" introduced the “Payment Card Industry - Data Security Standard”, shortly “PCI DSS” as one of the most famous standards related to the security of the payment industry and payment systems.

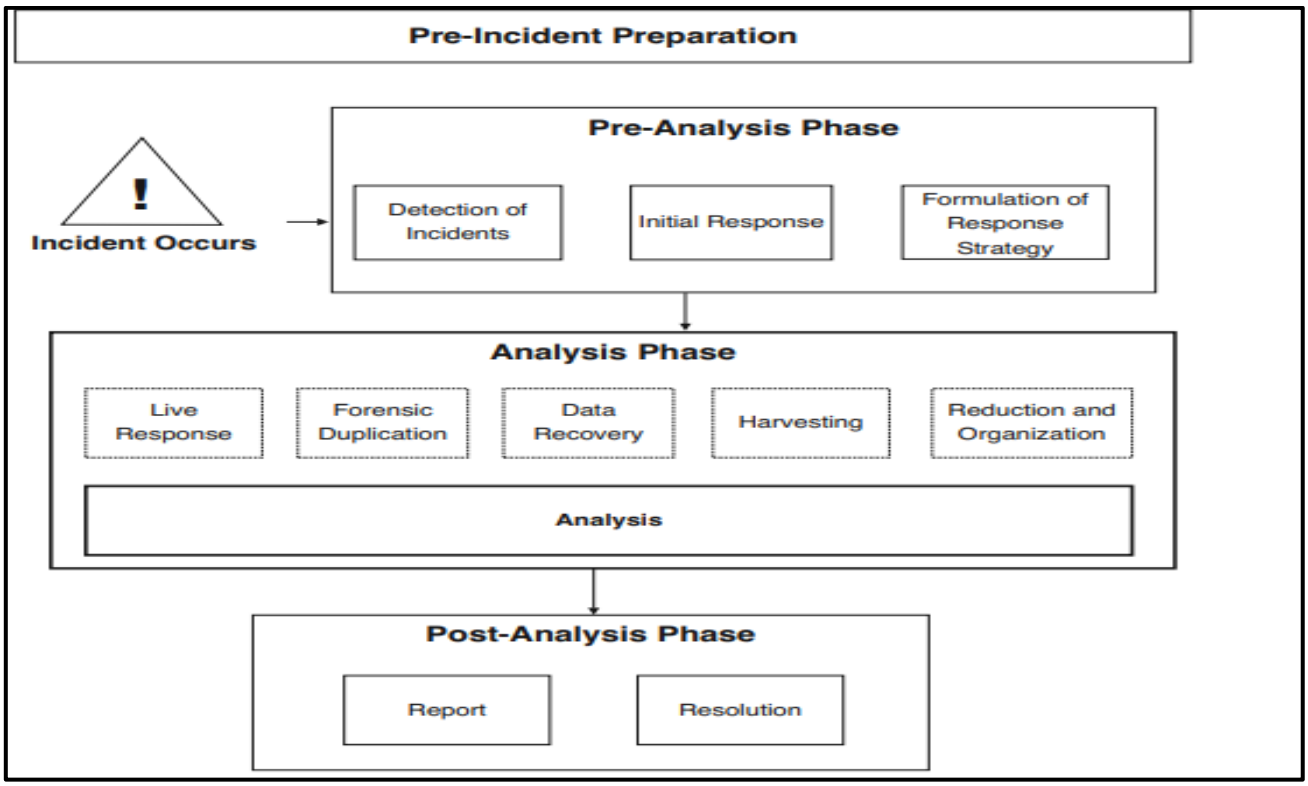


Figure 2.1: Common Process Model for Incident Response and Digital Forensics [12]**.**

The introduced standard provides a group of security controls, technical requirements, and procedures baseline to protect the financial and operational payment data [13]. Within a recent version of the standard introduced in 2022, the standard recommends establishing cybersecurity incident handling and response processes as well as introducing forensics processes in detection and response procedures. The standard was limited to general control recommendations and is not considered a framework or process model.

The SWIFT network, released “SWIFT’s Customer Security Program”, shortly “SWIFT CSP” contains several cyber security mandatory controls to be followed by all financial sector organizations worldwide to help financial service providers protect their financial applications and network as well as keep their defenses up to date against cyberattacks [14].

SWIFT CSP enforces a wide range of security controls and requirements related to digital forensics and incident handling and detection (requirement 6 and requirement 7) for all financial service providers and the banking sector [15]. Such controls as:

- **Detect anomalous activity**: (malware protection, software integrity, database integrity, logging and monitoring, intrusion detection)
- **Plan for incident response and information sharing**: (cyber incident response planning, security training, and awareness, penetration testing)

2.3.3 Digital Forensic Practices and Applications Within Financial Sector

The recent analysis of the cybercrime and digital investigation practice in the banking industry, reveals that it is highly necessary and recommended to develop and introduce a new approach for detecting, investigating, and responding to cybercrime, as the current measures and approaches applied to traditional crimes are no longer effective in this area. Thus new approaches to cybercrime investigation in the banking industry should be developed [16].

Several types of research conducted on digital forensics within the financial sector found that a community of digital forensics practitioners working towards investigating and analyzing technology fraud already exists within the finance industry [17]. The need for such a digital forensics community emerged rapidly especially over the past 10 - 15 years due to the advancement of electronic financial services and associated security threats such as social engineering and phishing attacks, online banking Trojans, and other categories of cyber criminals and threat activity targeting the financial sector and industry, thus the research found that there

is a critical need to directly integrate these existing communities of the practitioner with digital forensics community and practices [18].

In [19], the researchers proposed a digital forensic readiness framework dedicated to Nigerian banks that are categorized as major financial sector organizations. The proposed framework was developed with seven major elements and aims to protect sensitive and critical information from being compromised. As well as to minimize and eliminate attacks targeting such bank information by cyber attackers. Major components of the proposed framework were:

- **Strategy**: ensuring that the financial sector organization has a forensics strategy aligned with the objectives and needs of the organization.
- **Policy and procedures**: to guide the organization's staff on how to conduct their forensic activities within the workplace.
- **People**: are needed to execute and operate forensic activities within the organization.
- **System**: to detect, aggregate, and collect all logs and activity information.
- **Monitor and report**: reporting and communicating digital forensic incidents.
- **Forensic preparation**: ensuring that digital forensic training strategy is well developed and being implemented.
- **Risk assessment**: ensure identifying the value of information systems as well as indicators of compromise.

The gap within this proposed framework is that it is a local study and does not cover international research as well and the proposed framework is limited to the readiness process and does not support early detection and response activities and proactive components.

The research results from [20] found that the majority of financial fraud incidents are reported by either customer-compliant, internal audit function or by any third-party notifications, rather than (and outside) to be reported by internal and dedicated fraud investigation and detection strategy and framework, thus fraud investigations and detection process as well as needed teams and noted to be unfamiliar to most of the banks covered by the study. Thus, the banking sector needs to work towards a more future focus on developing fraud detection and investigations programs and capabilities.

In [21], research proposed a digital fraud and forensics process model that is used to detect and respond to anomaly financial transactions and systems intrusions as well as incidents conducted by malicious users, by analyzing a huge amount of system transactions within the financial system environment. The proposed model maintains incident accountabilities and responsibilities as a basic building block for developing cyber incident policies and investigation frameworks. Major components of the proposed model are the identified indicators of compromises for each financial system in use.

2.3.4 Financial Applications Security and Forensics Requirements

To operate and execute all financial and business processes within financial sector organizations, we need to deploy the appropriate software applications that might be categorized under the financial applications umbrella [22].

Financial applications components are composed into the following categories [23]:

- Physical and information technology infrastructure.
- Operating systems

- Application systems
- Database management systems
- Middleware applications.

The use of such applications as well as the automation of financial services and business processes introduces the overall financial environment and its all components to business risks associated with the use of those application-associated network infrastructure components [24]. To mitigate such risk, organizations need to deploy a series of application security control over each level of business and financial systems components [25], or at minimum, control baseline as a minute required controls need to be deployed to guarantee the security of the financial applications environment [26].

The major components of any security control baseline proposed by [27] are illustrated in Figure 2.2 below:

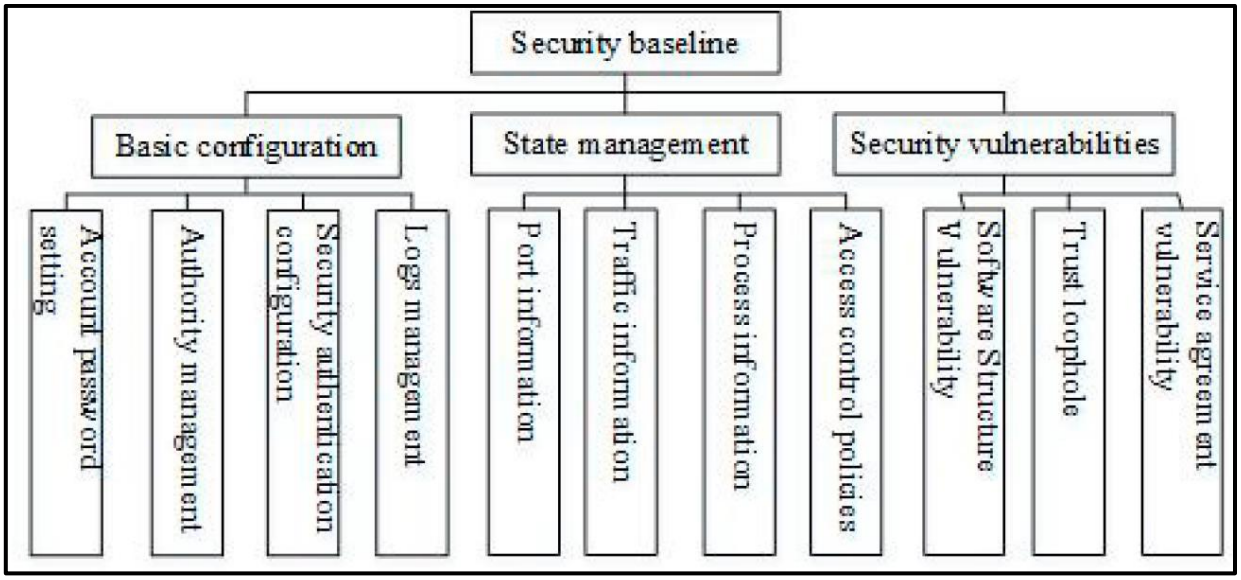


Figure 2.2: Composition of Application Security Controls Baseline [27]**.**

By analyzing the proposed model, it will be very clear that one of the basic requirements for business and financial systems control baseline is log management and activity monitoring controls that are considered core requirements for security investigations, and forensic and incident response processes.

Other approaches to ensure the security and safety of business financial applications are adapting security continuous monitoring over financial applications and supporting infrastructure[28]. The optimal model to guarantee such a level of security might be done by building a security operation center (SOC) to continuously monitor systems and infrastructure [29].

The study in [30], proposed comprehensive security architecture for monitoring information systems and network components, the proposed security architecture is designed based on log collection and management process, the basic components of the proposed architecture are:

- Log generators (log sources)
- Collection servers (log aggregation alerts and attack indicators)
- Storage servers

The proposed model [30] considered valuable resources for the development of a continuous monitoring operation center that would be based on several security alerts and attack indicators.

In [31], NIST identifies and recommends the following computer security log sources to be monitored to build comprehensive log management and incidents detection program:

- **Security software level**: (antimalware, IDS/IPS, remote access software, web proxies, vulnerability management software, authentication servers, routers, firewalls, network quarantine servers)

- **Operating systems level**: (system events, audit records)
- **Applications level**: (client requests and server responses, account information, usage information, significant operational actions)

The proposed model [31] considered valuable resources for the process of developing a continuous monitoring operation center that would be based on several security alerts and attack indicators. Over several network components level.

For information systems and applications security controls at various levels, NIST recommends a group of controls within "NIST special publication 800-53" [32], deploying the recommended controls for the organization's high-value assets like financial and payment system applications, ensuring the security of applications and the overall operating environments supporting those applications, control groups over application levels are:

- Access controls
- Awareness and training
- Audit and accountability
- Configuration management
- Contingency planning
- Identification and authorization
- Incident responses
- Maintenance
- Media protection
- Physical and environmental protection
- Planning

- Program management
- Personal security
- Risk assessment
- System and service acquisition
- System and communication protection
- System and information integrity
- Supply chain risk management

Several controls are considered proactive controls and might be deployed as early detection security controls for early detection of cybersecurity incidents, especially the following controls ad sub controls:

- Audit and accountability
- Configuration management
- Incident responses
- Risk assessment

2.4 Generic Digital Forensics Approaches and Process Models

The accelerated growth and sophisticated techniques and trends used to commit cyber-attacks by perpetrators and international cybercriminal gangs reveal the need to develop multi-purpose digital forensics and international investigation process models to assist investigators during the cyber investigation process they held worldwide. To ensure proper procedures are followed during the process as well as achieving the needed results cited by the investigation team [33].

Several investigative and forensics process models have been developed and implemented over the years since the foundation of forensics sciences. The majority of these models share the characteristics that it is oriented and focus on investigation aspects and the digital evidence collection process rather than the in-depth process model covering the whole forensics process.

Though dozens of investigative models developed and implemented over the years, this section of research will review only a few of them due to the major similarity of components designed as well as the covered scope. This section will cover the generic digital forensics model era through the period of 2000 to 2014 related to our research study.

2.4.1 Digital Forensic Research Workshop (DFRWS)

one of the earliest collaborative and formal interests towards the development of digital forensics science was founded by the "Digital Forensic Research Workshop", shortly "DFRWS" as a result of its first open forensic research workshop (conference) in 2001. and in the form of a technical report titled "a road map for digital forensic research"

With broad participation and collaborations from computer forensic examiners, university researchers, and security experts, the DFRWS conducted its first workshop with the major attendee's objective of forming a community of interest in the field of digital forensics, as well as forming a meaningful dialog and road map for digital forensics research to establish a framework for digital forensic science.

DFRWS defined digital forensic science as: "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources to facilitate or

further the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" [34].

The basic building block of the formal framework for digital forensic science extracted from the DFRWS proposed definition of digital forensics, as a linear investigative process model starting from identification steps into decision steps, from identification to the decision that typically appears to be used in the process of digital forensic analysis as illustrated in Figure 2.3. Which shows the details and sub-phases for each main step. The major categories of the proposed framework are; (identification, preservation, collection, examination, analysis, presentation, and decision process)

Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

Figure 2.3: DFRWS linear investigative process [34]**.**

The limitation of the DFRWS model is that this model is an investigative model only and does not support the whole digital forensics process, especially the response activity to an occurred incident [35].

2.4.2 Abstract Digital Forensic Model (ADFM)

As an enhanced version inspired by the DFRWS model, the proposed "Abstract Digital Forensic Model", shortly "ADFM" [36] was developed based on the common process that is technology and crimes independent. This model suggests 9 key components for the forensics process, as a compatible and flexible standardized process model regardless of the digital technology involved in forensics investigation. The flexibility of this model design facilitates and supports dealing with different digital devices in a backward and forward compatibility manner. The major key components of the proposed model include the following:

- Identification – detecting, determining, and recognizing incidents and incidents types using an indicator of compromise as a proactive and continuous detection approach.
- Preparation – preparing all issues related to the case, such as tool employees, adapted techniques, approved search warrants, authorizations, and organizational support.
- Approach strategy – formulating an investigation approach based on specific technology involved in crime and crime scenes.
- Preservation – securing, isolation, and preserving digital evidence as well as maintaining chain of custody to all evidence related to crime.
- Collection – recording of the crime scene information and baking up the digital evidence by following well-established procedures of evidence duplication and validation.
- Examination – conducting an in-depth search of evidence that is related to the suspected crime.
- Analysis – determination of evidence's significance, and drawing conclusions based on evidence found.

- Presentation – presenting your findings and conclusions as well as explaining the presented conclusions.
- Returning evidence – ensuring the proper procedures are followed to return the evidence to the proper owner.

The limitation of the ADFM model comes with its generality of the categories that might be defined as general for practical and professional uses

2.4.3 The Integrated Digital Investigation Process Model

The "Integrated Digital Investigation Process Model", shortly "IDIP" [37] was developed based on the "crime scene theory for physical investigations" with 17 sub-phases organized into main five groups (readiness, deployment, physical crime scene investigation, digital crime scene investigation, and review phase).

This model treats computers and digital devices as an object or physical evidence (a subject of crime - the computer is itself a crime scene) rather than an investigation crime scene. This adds limitations to the investigation process and the credibility of evidence collected from computer systems. Due to considering the digital crime scene as a secondary one to the physical crime scene. Figure 2.4. Illustrated the five major groups of phases forming the (IDIP) investigation process model.

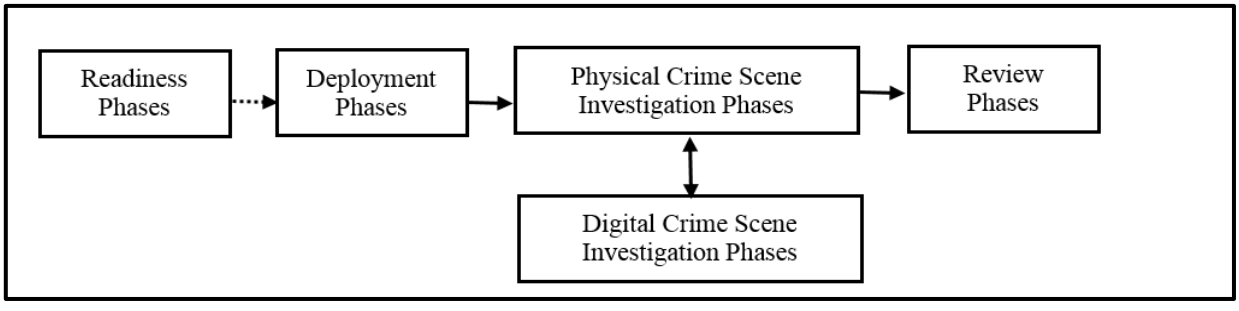


Figure 2.4: Phases of the IDIP Model [37]**.**

2.4.4 The Enhanced Integrated Digital Investigation Process Model

The "Enhanced Integrated Digital Investigation Process Model", shortly "EIDIP" [38] was developed as an enhanced version inspired by (IDIP). As illustrated in Figure 2.5. The proposed model consists of five major phases that modified the original one by adding a new phase (trace back phase) that is designed to trace back to the computer and digital systems that would lead investigators to the point where exactly the crime was committed. Thus (EIDIP) is one of the earliest models that are appropriate for the digital and cyber investigations process.

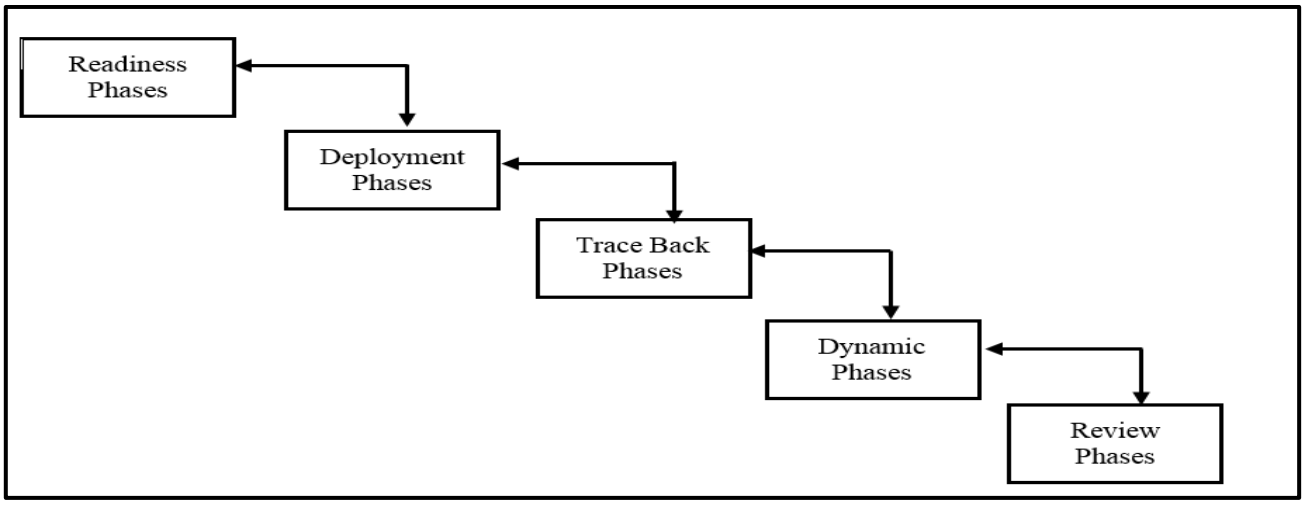


Figure 2.5: Phases of the EIDIP Model [38]**.**

2.4.5 The Extended Model of Cybercrime Investigations (EMCI)

The "Extended Model of Cybercrime Investigations", shortly "EMCI" [39] was developed as a comprehensive generalized cyber investigation reference model focusing in general on information flow issues between model components and processes and activities rather than the procedures for conducting each one. The model consists of 13 major activities as described in the following list and illustrated in Figure 2.6.

- Awareness
- Authorization
- Planning
- Notification
- Search for and identify evidence
- Collection of evidence
- Transport of evidence
- Storage of evidence
- Examination of evidence
- Hypothesis
- Presentation of hypothesis
- Proof/defense of the hypothesis
- Dissemination of information

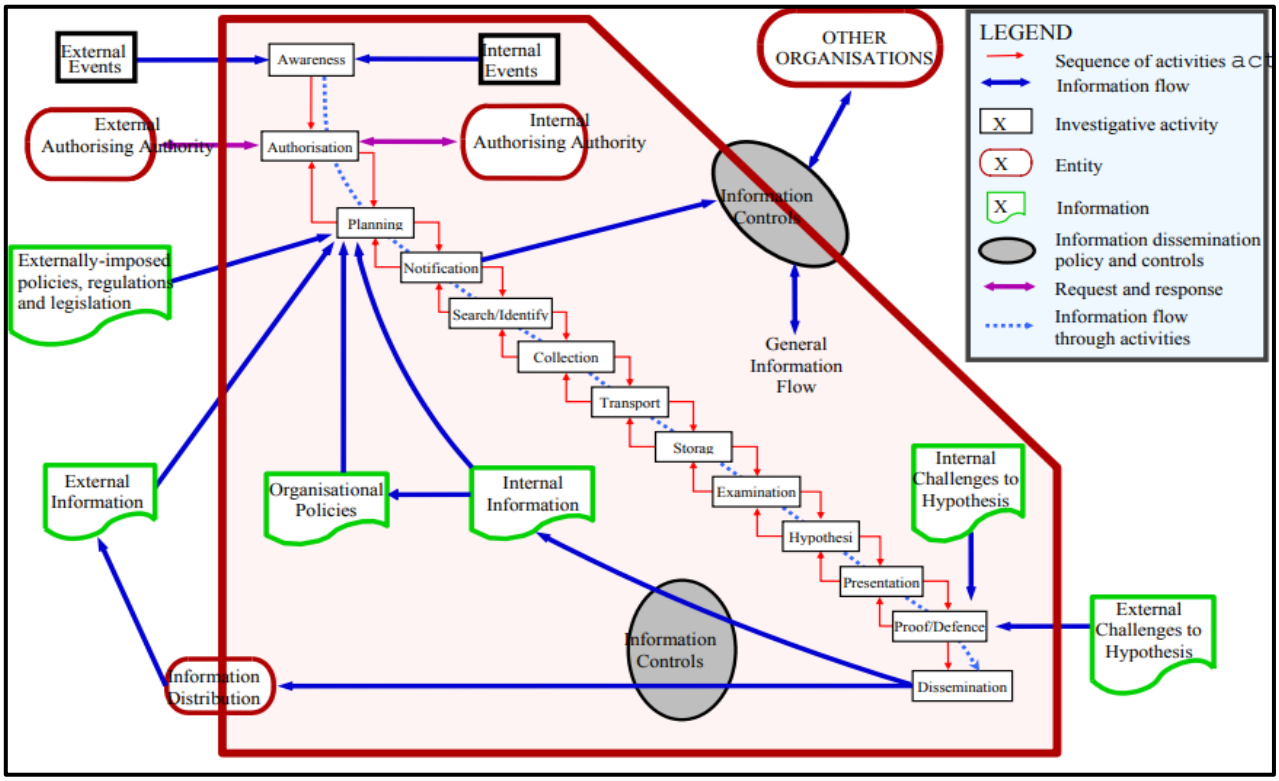


Figure 2.6: The Extended Model of Cybercrime Investigations [39]**.**

For the model to be applicable, it should be tolerated to the specific needs of any organization by developing a detailed procedure to be followed during each investigation process.

2.4.6 The Systematic Digital Forensic Investigation Model (SRDFIM)

The "Systematic Digital Forensic Investigation Model", shortly "SRDFIM" [40] organizes and breaks the digital forensics investigation process into eleven phases as illustrated in Figure 2.7.

This generalized model [40] provides a consistent, systematic, and standardized process model for the majority of the digital investigations process. As well as used for attaching technology and non-technology related issues in the investigation process.

Due to the nature of the phases included, the proposed model [40] is considered one of the most detailed digital forensic investigation models to date, thus it can be implemented elastically for the cyber investigation process as well as investigating cyber and technology-related incidents that might occur at the organizational level.

The model consists of the following process – phases (preparation, securing the scene, survey, and recognition, documenting the scene, communication shielding, evidence collection, preservation, examination, analysis, presentation, result, and review)

2.5 Cyber Security Incident Handling and Response Process

As the importance of being able to detect and identify cyber security incidents, it is very important to handle each level of the incident and respond to the consequences in a systematic, organized, and well-defined manner that ensures proper identification, detection, analysis, contamination, and treatment of incident and taking appropriate activities to deal with [41]. This

section introduces in detail the related literature regarding cyber security incident detection, handling, and responding processes.

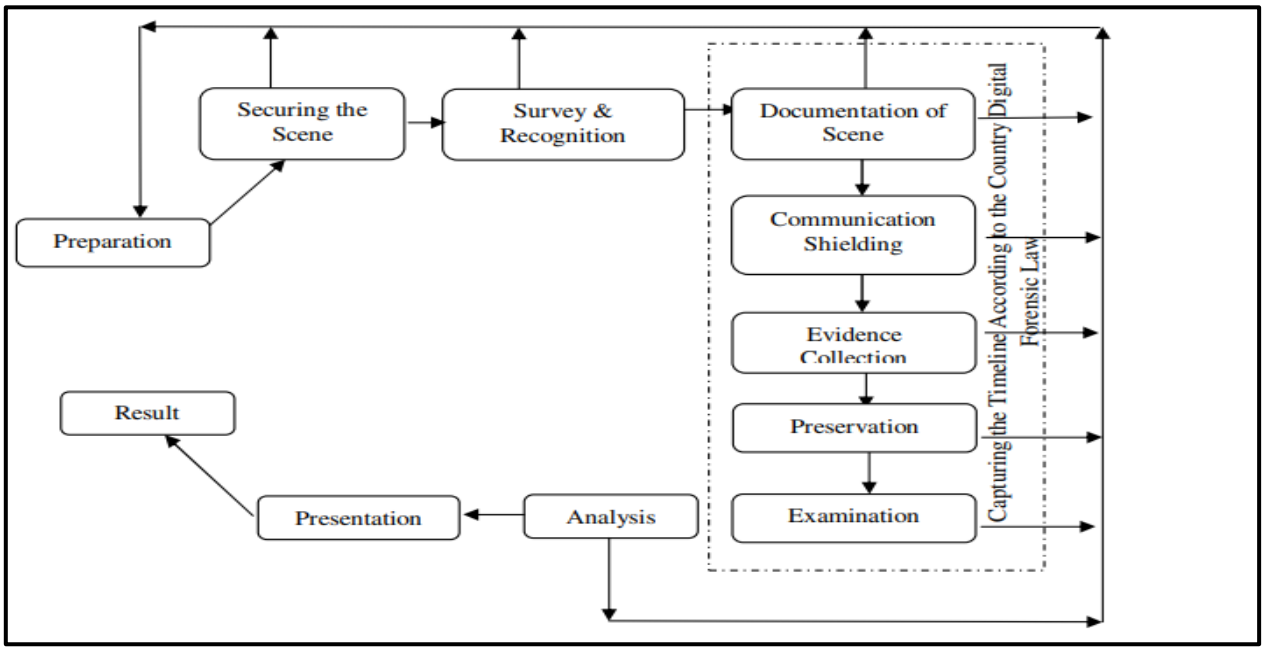


Figure 2.7: Phases of Systematic Digital Forensic Investigation Model (SRDFIM) [40]**.**

2.5.1 Cyber Security Incidents

When it comes to the adverse occurrence and consequences of any technology-related and cybersecurity events that negatively affect the confidentiality, integrity, or availability of information and information systems in the digital environment, regardless of the volume of consequences and frequency of occurrence, then we are describing a real cyber security incident case [42].

Such cases should be effectively detected, addressed, and handled in a timely and quick manner to mitigate the adverse consequences in another area within the organization. Especially when it comes to a very complex and sensitive environment such as the financial sector which is considered one of the most attractive targets to cybercriminals worldwide [43]

One of the earliest and decent definitions of cyber security incidents was proposed by the “United States”, shortly “U.S” software engineering institute, the institute defines security incidents as “some type of unauthorized activity against a computer or network that results in a violation of a security policy. Whether it is an action, an event, a situation, or collection of data relating to an attack” [44].

2.5.2 Cyber Security Incident Impact and Response Process

Cyber security incident has variant impact and consequences on the information within the digital environment, such incidents varying from low impact to catastrophic consequences and depending mainly on the influenced area or information or systems and the value of that information or system to the organization [45].

The cyber security incident response process is defined based on NIST as "a continuous process that enables organizations to detect, analyze, eradicate, and recover from potential cybersecurity incidents in a timely and cost-effective manner” [46].

2.5.3 Cyber Security Incident Categories

Cyber security incidents can occur from different sources, such sources are categorized into two major sources, internal and external sources [47]. The study in [48] proposed a model for categorizing cyber security threats and incidents based on several criteria, one of the proposed criteria is the origin and sources of the threat, and the proposed model [47] defines two major sources for security incidents, internal and external.

One of the most accurate definitions of external threats and incidents proposed defines external incidents committed as "the individuals or organizations working outside of a company and cause

for the external threats with the most external threats to information systems are natural disasters, external attacks occur through the connected network or physical intrusion" [49].

While the researcher focuses on insider threats and incidents, our proposed research will not go beyond the definition the external threat and incidents that are mainly committed or generated by parties or issues that are not directly related to the organization or the operating digital environment (competitor's data theft, data leaks, … etc.).

2.5.4 Insider Cyber Security Incidents

Internal cyber security incidents are mainly committed or conducted by insider actions and issues or by people from inside the organization or who have a direct relation to the internal digital environment (like staff misuse, employee data theft, internal policy violations, intentional damage information …etc.) [50]. The majority of security research reveals that insider threats form the biggest risk when compared to other security incident sources [51].

Several research papers and international security surveys that focus on the impact assessment of security incident, show that the majority of security incident sources was committed by insider threats with a very high impact on the global economy. The financial service organization is the main target of such attacks [52].

The [53] survey mentioned that 60% of the financial losses related to cybersecurity incidents were due to insider threats. The 2022 version of the data breach investigations report [54] shows that 82% of cybersecurity breaches involved the human element. In the form of stolen credentials, phishing attacks, misuse of assets, or simply errors with 27% of total attacks belonging to insider perpetrators in the financial sector.

The formal definition of insider threats proposed by “The Computer Emergency Response Team”, shortly “CERT” of the insider threat center of the U". S software engineering institute as: "a current or former employee, contractor, or business partner who meets the following criteria”:

- The insider who has or had authorized access to an organization’s network, system, or organization’s data.
- The insider who has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, availability, or physical well-being of the organization’s information or information systems or workforce [55].
- Typical examples of insider attacks or threats to information systems proposed by [56], and categorized as the following:
  - ✓ Unauthorized extraction, duplication, or exfiltration of data
  - ✓ Tampering with data (unauthorized changes to data)
  - ✓ Destruction and deletion of data and critical assets
  - ✓ Downloading and installing software or data from unauthorized sources.
  - ✓ Using cracked software that might hold backdoors or malicious code.
  - ✓ Network eavesdropping and packet sniffing.
  - ✓ Identity spoofing and theft of other users
  - ✓ Social engineering attacks.
  - ✓ Unauthorized activities or misuse of resources for non- work-related
  - ✓ Installing malicious software purposefully
  - ✓ Theft or loss of mobile devices or laptops.

2.5.5 Cyber Security Incident Handling and Response Frameworks

One of the globally well-known and typical cyber security incident handling processes was developed in 2012 and revised in 2018 by NIST [57] and has been published within its "special Publication" shortly "SP" 800-61. The proposed process model [57] consists of 4 major steps to effectively handle any cyber-related incidents and covers the process of how organizations should handle and respond to cyber security incidents, as illustrated in Figure 2.8 and the steps described below:

- Preparation: proactively prepare your environment and organization to effectively be able to respond to any potential incidents.
- Detection and analysis: identifying and determining the occurrence of incidents as well as detecting the singe and indicators of an incident. And analyzing all information related to those indicators.
- Containment, eradication, and recovery: mitigating the consequences of an incident as well as restoring the previous operating status of the information environment.
- Post-incident activity: documentation of an incident's details and learning lessons for future incidents as well as applying all prevention control to prevent the reoccurrence of such incidents in the future.

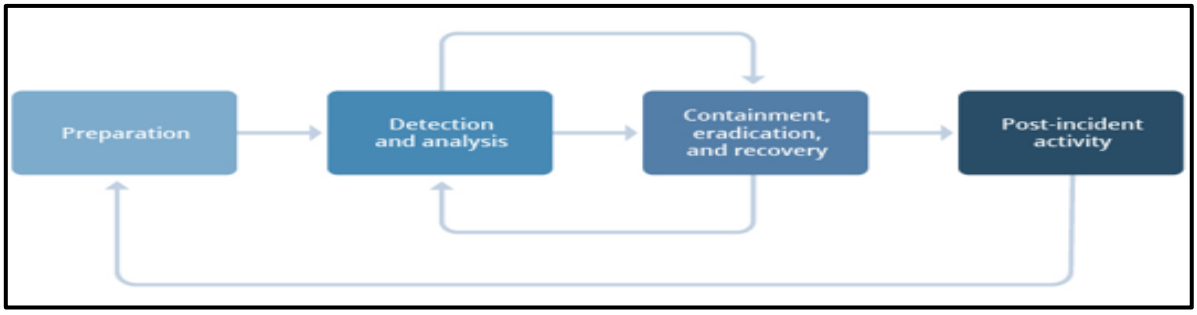


Figure 2.8: NIST (SP) 800-61 Incident Response Process [57]**.**

The flexibility of the framework and the lower procedures level make it one of the best choices for handling information security incidents with all categories and from different sources. As well as the flexibility to integrate the proposed process into a forensics process.

Another global and well-known cyber security incidents handling process was developed by the “SysAdmin, Audit, Network and Security”, shortly the “SANS” Institute in 2011 "the incident handlers Handbook” [58].

The proposed process model [58] consists of 6 major steps to effectively handle any cyber-related incidents and covers the process of how organizations should handle and respond to cybersecurity incidents.

- Preparation—development of security policy, conducting a risk assessment, sensitive assets inventory, and forming of “Cyber Security Incident Response Team” (CSIRT).
- Identification—monitoring of its systems detecting anomalies operations, and declaring security incidents.
- Containment— doing short-term containment, isolating the network segments, doing long-term containment, and fixing restoring systems into production.
- Eradication—remove unwanted suspects from all affected systems, examine the root cause of the incident, and take future actions to prevent similar incidents in the future.
- Recovery—restoring production systems. Verify and monitor targeted systems to make sure they are in normal status.
- Lessons learned—prepare detailed documentation of the incident, investigate the incident deeply, and improve the incident response process.

As well as the NIST incident response process, the SANS incident response process model is considered flexible and one of the preferred choices for handling information security incidents with all categories and from different sources. As well as the flexibility to integrate the proposed process into a forensics process.

2.5.6 Zero Trust Model

One of the modern cybersecurity models that comes to ensure the security of networks and information systems as well as a modern alternative model to the traditional perimeter network security is the zero trust model, introduced by Google's beyondcorp initiative [59]. The base idea behind this model is not to trust any of your network nodes and components and always to verify them [60]. The concept and need for such models come with the advancements and complexity in network design as well as the complexity of requirements needed to be applied to protect a such network [61].

The national institute of Standards and Technology (NIST) defines "Zero Trust", shortly "ZT" as "the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources" [62] as illustrated in Figure 2.9.

One of the biggest advantages of the zero trust model is the capability to increase the traceability for forensics as well as allow practitioners to learn from past incidents due to the logging capabilities and requirements of such a model[63]. The zero trust model is built based on the following pillars [64]:

- The computer network is always supposed to be hostile.

- External and internal network threats exist at all times.
- Network locality placement is not sufficient to decide the level of trust in a network
- Every network device user and all network data traffic flow are authenticated and authorized
- Network components policies should be dynamic and evaluated from as many network sources of data as possible.

As per the capabilities and architecture of the zero-trust model, some components of the model might help in the process of early detection and responses to cyber incidents, especially within the preparation phase that is designed to build incident response capabilities that prevent the potential incident occurrence.

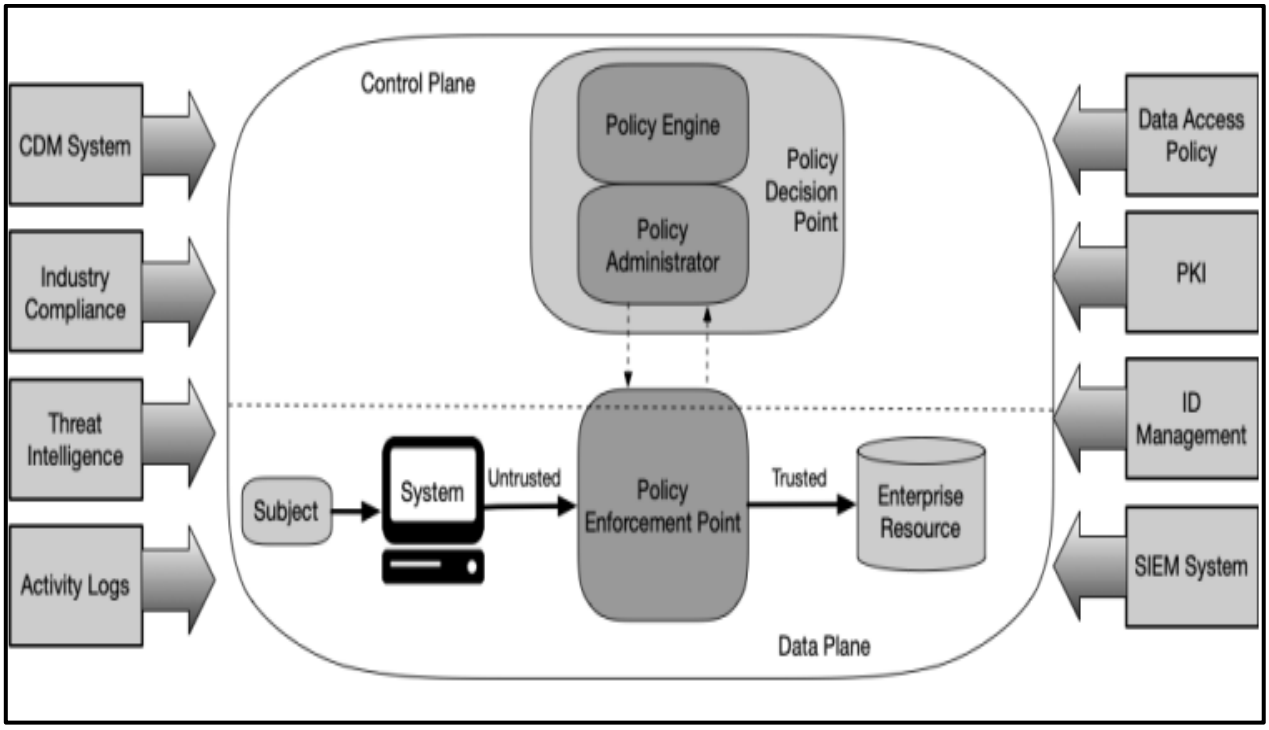


Figure 2.9: NIST (SP) 800- 207 Core Zero Trust Logical Components [62]**.**

2.6 Integrating Forensics Process into Incident Responses

security incident responses and computer forensics are two related, coherences, and integrated topics, within security incident responses and cybercrime methodology, the major concern is looking for evidence on what happened exactly, while computer forensics works to provide and deliver such evidence to reveal the truth [65].

While conducting a literature review and during comprehensive research in digital forensics and its relations to the information security incident handling process, we experienced the following results and gaps in the existing knowledge (organized by dates):

- In the most recent research on digital forensics and incident handling integration conducted in 2020, "Integrated incident response model for database forensic investigation"[66], the researchers proposed an incident response model designed to investigate incidents within a database environment by proposing suitable process and theoretical model of evidence constructing and integrating cyber incident response model (IIRM) to be relied upon in the database incidents forensic and investigation field. This research is limited to database environments for general purposes organizations and does not cover comprehensive digital forensics framework for financial environments.
- In 2019, several researchers covered digital forensics framework and proposed investigations process models,[67] proposed the "standardized digital forensic investigation process model", shortly “SDFIPM”, and the researchers proposed an advanced investigation process model (SDFIPM), for conducting digital forensic investigations, the limitation of this model

is a generic model which might be applied in several fields, such that law enforcement, commerce, and incident response but not covering the financial environment.

- Also in 2019 types of research, [68] proposed comparison and mapping of all previously developed digital forensics frameworks. The proposed mapping and enhanced process results in a well-designed and optimized investigation process, with limitations to the financial environment scope.
- In 2017, [69] proposed a digital forensics framework for cloud computing incidents, the proposed framework was designed to mitigate the forensics process dependency on cloud service providers and suggest a new process model for collecting digital forensic evidence from outside the cloud environment.
- Also in 2017 types of research, [70] proposed an "evidence gathering framework correlates multiple patterns detected" from normal network traffic. These two pieces of research are also limited to cloud computing and network environments and do not cover comprehensive digital forensics frameworks for the financial environment.
- In 2016, [71] proposed a generic digital forensics framework for investigating Internet of Things devices (IoT), the proposed framework is designed to help conduct digital forensics investigation within all related components of the IoT-based environment. With limitations to (IoT) environment scope.
- In 2014, [72] focused on the need for research to be conducted as well as encouraging "further research and advancement in the area of incident response about digital forensics". This research study illustrated the importance of the relationship between digital forensics and incident response.

- In 2013, [73] proposed a digital forensics framework for monitoring cloud computing, the proposed framework developed a novel process model for monitoring user activity within cloud environments using a secure and reliable cloud forensic framework. This proposed research is also limited to cloud computing environments and does not cover comprehensive digital forensics frameworks for financial environments.
- In 2011, [74] proposed a distributed digital forensics and incident response framework, The researchers presented a rapid incidents response framework based on open-source computer tools to investigate an organization's remote devices, disks, and memory units in enterprise environments. With limitations to devices and memory environment scope.
- In 2010, [75] proposed an "advanced framework for digital forensic technologies", the proposed framework employs a top-down approach to the digital forensic process, starting with legal issues, continuing with organizational issues, and ending with a purely technical issue that deeply addresses core forensic principles. The proposed framework does not cover any financial environmental aspects or scope.
- In 2007, [76] proposed a "forensic approach to incident response, network investigation, and system administration using digital evidence bags" The proposed framework presented how the newly proposed digital evidence containers (bags), can collect and analyze evidence from a dynamic environment. The proposed framework does not cover any financial environmental aspects or scope.
- The oldest reviewed research on digital forensics and incident handling integration conducted in 2004, [77] proposed a digital forensics framework based on an event gathering process. The proposed framework includes an investigation process model based on crime scene procedures. In this proposed model, each digital device collected is considered a digital crime

scene, that is included within the physical crime scene where located. The proposed framework does not cover any financial environmental aspects or scope.

As a result of the comprehensive literature review research in digital forensics and its relation to the information security incident handling process, we experienced the current gap in knowledge that needs to be addressed and cannot be filled unless the research project is completed. Table 2.1 illustrates the current literature and the current gap in the field of integrating digital forensics into the incident repose process within the financial sector.

Gap assessment identified using a comparison between the available processes in current forensics models within the literature in the field of digital forensics, against the proposed model that this research aims to develop using the following criteria:

- Whether the available models cover the typical digital forensics processes.
- Whether the available models cover the typical incident response processes.
- Whether the available models cover the integrated digital forensics and incident response processes.
- Whether the available models are considered generic forensics and incident response models.
- Whether the available models are considered technical-specific models.
- Whether the available models developed for the financial sector.
- Whether the available models are developed to cover and support integrated digital forensics and incidents response processes for the industry-specific sector as the financial sector.

Further research on digital forensics and its relations to the information security incident handling process should be conducted to bridge the current gap in this knowledge.

Table 2.1: Summary of Identified Frameworks and Current Gap Within Literature.

Inclusion Criteria	The current gap within current digital forensics and incidents generic process models																			
	CPMIRDF [11]	DFRWS [34]	ADFM [36]	IDIP [37]	EIDIP [38]	EMCI [39]	SRDFIM [40]	NIST [57]	SANS [58]	ZT [62]	IIRM [66]	SDFIPM [67]	DFFCCI [69]	EGFCMPD [70]	GDFFIIOT [71]	DFFMCC [73]	DDFIRF [74]	AFDFT [75]	FAIRNISA [76]	DFFEGP [77]
DF Process	✓	✓	✓	✓	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IR Process								✓	✓		✓		✓				✓		✓	✓
Integrated DF and IR											✓		✓				✓		✓	✓
Generic Model		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓						✓		✓
Specific Technical Model											✓		✓	✓	✓	✓	✓	✓	✓	
Financial Model	✓																			
Financial Integrated DF and IR																				

2.7 Chapter Conclusions and Summary

In this chapter, comprehensive deep research was conducted on several previous studies related to our work through the prior work and literature review task. The current studies considered initial and general-purpose frameworks. Thus, we experienced the current gap in knowledge that needs to be addressed and cannot be filled unless the research project is completed. Below is the major finding extracted from the literature review work:

- There's a high demand for developing a dedicated forensics framework for the financial service sector due to the current gap of knowledge and research in this area, as well as the increase in sophisticated cyber-attacks and the security insiders threat landscape.

- Various information security control baseline models have been developed to ensure the security of high-value information systems like financial and payment applications. The majority of the models required developing formal incident response and forensics processes to ensure early detection and investigation of cyber incidents.
- Several investigative and forensics process models have been developed and implemented over the years. The majority of models focus on investigation aspects and the evidence collection process rather than the in-depth process model covering the whole forensics process.
- Several cyber security incident process models have been developed and implemented over the years. The majority of models are mature enough to manage a whole incident response activity and are subject to be integrated with extracted forensics models.
- Security incident responses and computer forensics are two related topics. The scope of the majority of the studies that correlate such relations is limited to specific and technology-oriented frameworks rather than specific industry-oriented frameworks (i.e. Financial environment). Even though, selected components are subject to be integrated with selected components of both security incidents and the forensics process for developing our proposed framework.

The next chapter (chapter 3) explains the researcher's approach to answering the research questions and explains the most appropriate research strategy and data collection methods for the proposed research.

Chapter 3

3. Research Strategy and Data Collection Methods

3.1 Introduction

This chapter aims to explain the researcher's approach to answering the research questions and explains the most appropriate research strategy and data collection methods for the proposed research.

3.2 Research Strategy

Amongst several approaches and research strategies that might be used for conducting technology-related research studies and appropriate for answering the research questions, especially for an exploratory research study, the grounded theory (as data collection and analysis methods) as well as theory data collection available choices, consider the most appropriate method for information and technology related research [78], especially with research that involves interactions between people using or interacting with information technology [79].

By adapting grounded theory, the researcher might generate or discover a new theory based on the analysis of data systematically obtained through social research to explore complementary social relationships and the behavior of groups [80].

In addition, adopting grounded theory is considered useful for conducting early studies of a new discipline or new systems. Because using grounded theory enables an examination of methods on how people respond to various phenomena [81].

Grounded theory, as a research method, allows the use of different and sometimes several methods for research data collection [82]. The data collection techniques that a researcher may employ under grounded theory includes (interview, direct and participant observation, content or documentary analysis, focus group, and survey) [83].

Since the science of digital forensics is a new field of study and involves direct interactions between people and technology, as well as the nature of this research on developing a new framework for digital forensics, the grounded theory seems the most appropriate method for developing a new framework for digital forensics [84], with the below-selected data collection techniques:

- Content or documentary analysis through literature and related works
- Assessment survey.
- Interview with a focus group.

3.3 Research Instruments and Data Collections Methods

3.3.1 Literature as a Research Instrument and Data Collections Method

To identify the gap in current literature, as well as to understand what others worked in the area of study, a total of (100) literature and related cyber security, incidents responses, and forensics international standards were reviewed and critically analyzed to extract major and common

forensics and incidents response framework elements that apply to the financial sector and to be used as a basic building block in the process of framework development. The following major literature and related work were covered within the literature review chapter in this phase:

- Financial sector overview.
- The drivers for, and the need for digital forensics within the financial sector.
- Digital forensics regulations and standards within the financial sector.
- Financial and payment applications security and forensics requirements.
- Generic digital forensics approaches, frameworks, and process models.
- Cyber security incident handling and response process.
- Cyber security incident categories and insider threats.
- Generic cyber security incident handling and response frameworks.
- Generic cyber security model: zero trust model
- Integrating forensics process into incident responses

Through the prior work and literature review task, we found in open literature very limited studies that directly focused on digital forensics integration into the information security incident handling process within the financial sector. The current studies considered initial and general-purpose frameworks. Thus, we experienced the current gap in knowledge that needs to be addressed and cannot be filled unless the research project is completed. Detailed information and results of this phase as well as the identified gap can be found in section 2.6 of this dissertation (conclusions and summary).

3.3.2 Survey as a Research Instrument and Data Collections Method

To better understand how financial organizations conduct security practices and to gather facts about the current state of cyber security practices and forensics programs, capabilities, and needs, as well as to know how cyber security incidents handling and digital forensics processes and practices are run and handled by the financial sector. In addition, to explore missing data within the literature, the survey's data collection method was selected by samples of financial institutions from different countries (inside and outside Palestine with 21 participant banks and payments companies). An assessment survey was developed covering the below five major areas, and designed based on the maturity and readiness factor of each cybersecurity below domain to introduce possible enhancements on groundwork and extracted processes:

- General cybersecurity capabilities, practices, and governance model.
- Cyber security incidents handling approaches and readiness level.
- Digital forensics capabilities and framework used.
- Major indicators and anomalous events (KRI, IOC, IOA) adapted to detect insider cybersecurity incident
- Good practice security standards and technology tools used.

As the aim of this data collection instrument and phase is to explore the current trends and practices within the area of study, a maximum sample size of 21 participants was used to collect the required exploratory data, and this number was considered valid to gather data for same-purpose research.

According to [85], using a sample size of 10 to 30 samples is considered sufficient and valid in cases of exploratory type research and pilot studies. The sample size is considered large enough to test the hypothesis and considered small enough to bypass any sample obstacles and effects.

3.3.3 Interviews as Research Instrument, Data Collection, and Validation Method

Interviews with a focus group of experts in the field of cyber security and digital forensics professionals were conducted for theoretical validation of the proposed framework, and feedback data on the preliminary developed framework were collated directly from participants' thought-focusing groups, (8 participants) to revise the framework (if needed).

Interviews responses data and expert opinions were collected to acquire theoretical validation and expert opinion of the proposed framework, as well as validate the applicability of framework elements to the financial sector. Expert opinions on the preliminary framework validation (if applicable) revised on the preliminary framework to issue the final version.

Focus groups are considered as a choice to validate the theoretical aspects of the framework, especially for qualitative and exploratory research types. [86] define focus group as “a way of collecting qualitative data, which- essentially- involves engaging a small number of people in an informal group discussion (or discussions), ‘focused’ around a particular topic or set of issues”.

The justification behind choosing such instruments is that qualitative and exploratory research usually uses focus group methods in the process of collecting data from multiple participants in parallel since it is the most economical, efficient, and fast method for such type of research [87].

The structures of well-designed groups usually consist of 6 to 12 participants and usually last between 1 and 2 hours [88].

3.4 Chapter Conclusions and Summary

This chapter explained the researcher's approach to answering the research questions and explained the most appropriate research strategy and data collection methods for the proposed research, as illustrated in Figure 3.1.

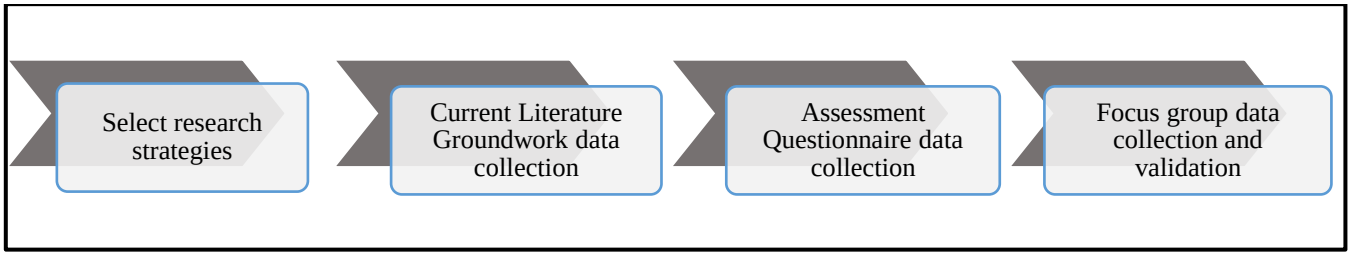


Figure 3.1: Research Strategy, Instrument, and Data Collections Methods

By adapting grounded theory as a systematic qualitative research and data collection methodology, the selected data collection techniques that support the research strategy are identified in the list below and within:

- Content or documentary analysis through literature and related works from a wide range of well-known and reputable scientific journals (i.e. IEEE, Science Direct, Google Scholar).
- Assessment survey.
- Interview with a focus group.

The next chapter (chapter 4), explains the data collection process and how data was collected through multiple data collection approaches. In addition, the next chapter explains how the exploratory data analysis was conducted and how the researcher used grounded theory and technical approaches to analyze the collected data.

Chapter 4

4. Data Collection and Exploratory Data Analysis

4.1 Introduction

This chapter explains the data collection process and how data was collected through multiple data collection approaches. In addition, this chapter explains how the exploratory data analysis was conducted and how the researcher used grounded theory and technical approaches to analyze the collected data.

4.2 Survey Data Collection and Analysis

To better understand how financial organizations conduct security practices and to gather facts about the current state of cyber security practices and forensics programs, capabilities, and needs, as well as to know how cyber security incidents handling and digital forensics processes and practices are run and handled by the financial sector. In addition, to explore missing data within the literature, surveys were sent and completed and data was collected by sample financial institutions from different countries (inside and outside Palestine with 21 participant banks and payments companies). An assessment survey was developed covering the below five major areas, and designed based on the maturity and readiness factor of each cybersecurity below domain to introduce possible enhancements on groundwork and extracted processes:

- General cybersecurity capabilities, practices, and governance model.
- Cyber security incidents handling approaches and readiness level.
- Digital forensics capabilities and framework used.
- Major indicators and anomalous events (KRI, IOC, IOA) adapted to detect insider cybersecurity incident
- Good practice security standards and technology tools used.

4.2.1 Survey High-Level Hypothesis

Hypothesis one (H1). The majority of financial firms have mature cyber security capabilities (the international bank has higher maturity levels).

Hypothesis two (H2). The majority of financial firms have well-defined incident handling and response capabilities and approaches and it is enterprise-level implemented.

Hypothesis three (H3). The majority of financial firms have a basic or no dedicated framework for managing digital forensics issues.

Hypothesis four (H4). The majority of financial firms do forensics investigation as a part of the incident handling and responses process and have third-party arrangements for any specific forensics activities.

Hypothesis five (H5). The majority of financial firms have deployed solid monitoring processes involving forensics practice without a proper and formal framework.

Hypothesis six (H6). The majority of financial firms include several incident responses and forensics processes within their internal practices.

Hypothesis seven (H7). The majority of financial firms have recommended developing a dedicated framework for managing digital forensics issues.

The results of the survey support our research hypothesis and initial proposed framework. In addition, all related responses are considered within the framework development process and embedded as a sub-process within the final version of the proposed framework. The section below contains the major results of the research survey.

4.2.2 Targeted Audience, Community Size, and Survey Distribution Method

The survey asked cyber security professionals within the financial sector to report on major information security program components as well as specific components related to the research aims (security program status, security governance, incident response capabilities, forensics capabilities, risk assessment processes, indicators, and anomalous events).

Linkedin messages and emails were sent to a group of information security leaders within financial firms globally between the period of (01/02/2023 to 31/03/2023), to request their professional participation in the pre-designed web-based survey. LinkedIn messages and email survey requests only went out to 100 security leaders worldwide representing international, regional, and local banks as well as payment processors companies.

Because the type of survey is an exploratory survey, a total of only 21 security leaders responded to the survey for the assigned period. This is considered valid to gather data for the same purpose of research. All of them provided complete responses. There were 14 male respondents and 7 female respondents.

Global commercial banks as of the beginning of 2023 are 10,334 commercial banks worldwide in reference to Ibisworld global industry statistics report [89], and the payment processors companies as of the beginning of 2023 1,300 processors companies worldwide as to merchant cost consulting global industry statistics report [90]. A total of 11,634 financial sector firms are covered by this research and represent the overall community size of financial and payment companies worldwide.

4.2.3 Analysis Method

For this research, exploratory factor analysis was employed for study to ensure study factor validity.

4.2.4 Survey Participant Qualifications, Profile, and General Information

For this research, the targeted survey respondents represent professionals from security management, who are directly responsible for information security program development and information security incident handling and forensics process.

4.2.4.1 Participant’s Profile and Professional Background Information

To assess the qualifications of each respondent, we asked respondents about their level of experience and professionality in the field of cybersecurity responses and what the job titles attached to their knowledge. The majority of respondents' answers reflect directly related jobs to cyber security with the majority of survey respondents’ working experience being more than 16 years (72%). Thus, respondents are considered qualified to fill out the survey, based on the distribution list and responses. As illustrated in Figure 4.1 and Figure 4.2.

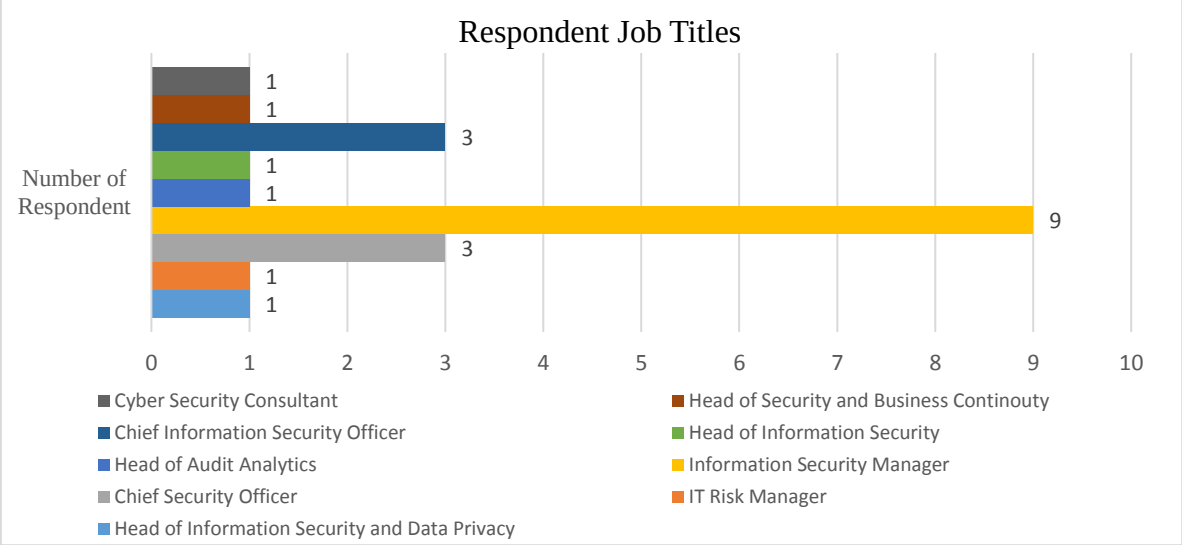


Figure 4.1: Survey Respondent Job Titles.

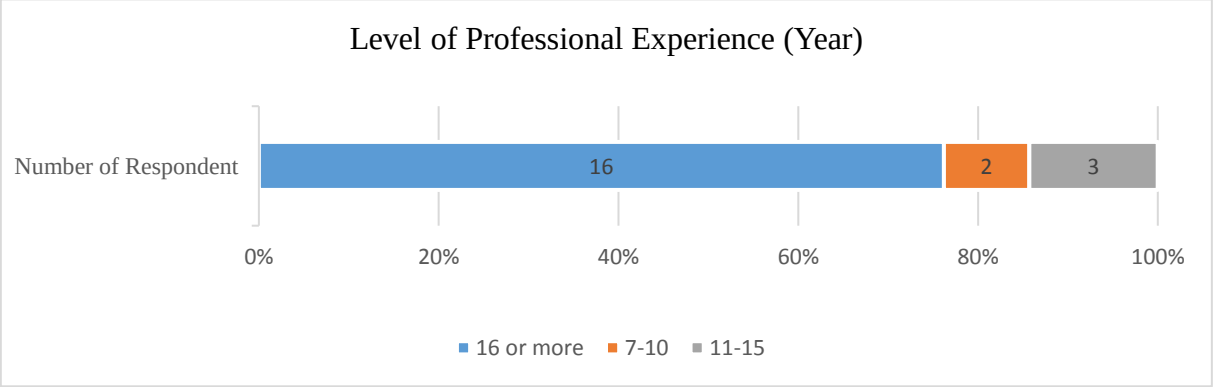


Figure 4.2: Survey Respondent Level of Professional Experience (Year).

4.2.4.2 Participant's Cybersecurity Education and Qualifications

For further assurance to validate respondent qualifications, we asked respondents about their educational and qualifications level. The majority of respondents answer that 86 % consider themselves to have professional cyber security skills with the majority of them (62%) holding advanced academic degrees. In addition, (17 out of 21). Respondents have more than one cyber

security certificate from different certification bodies as illustrated in Figure 4.3, Figure 4.4, and Figure 4.5.

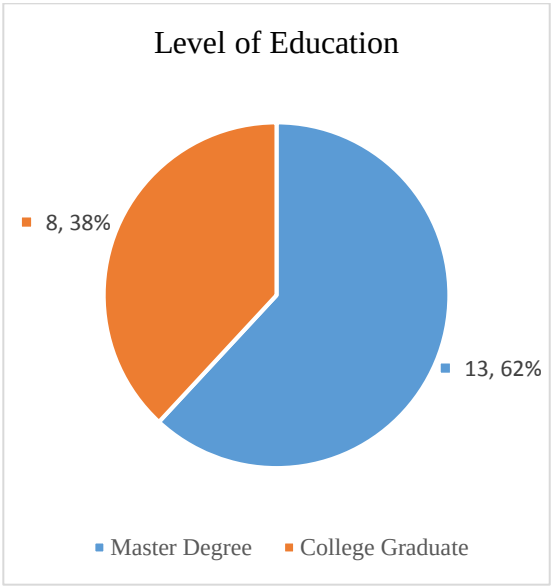


Figure 4.3: Level of Education.

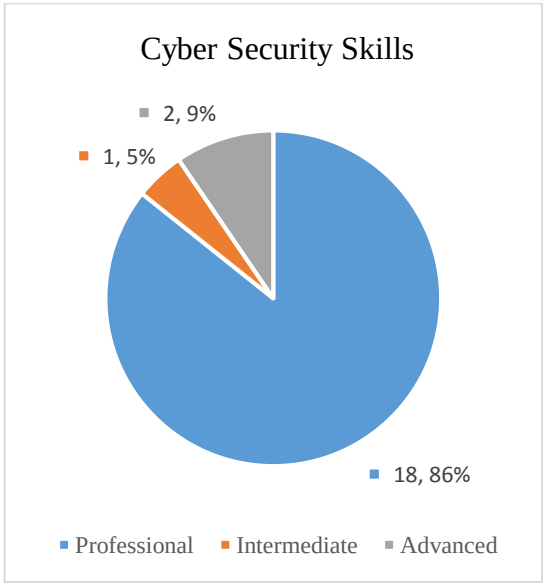


Figure 4.4: Cybersecurity Skills.

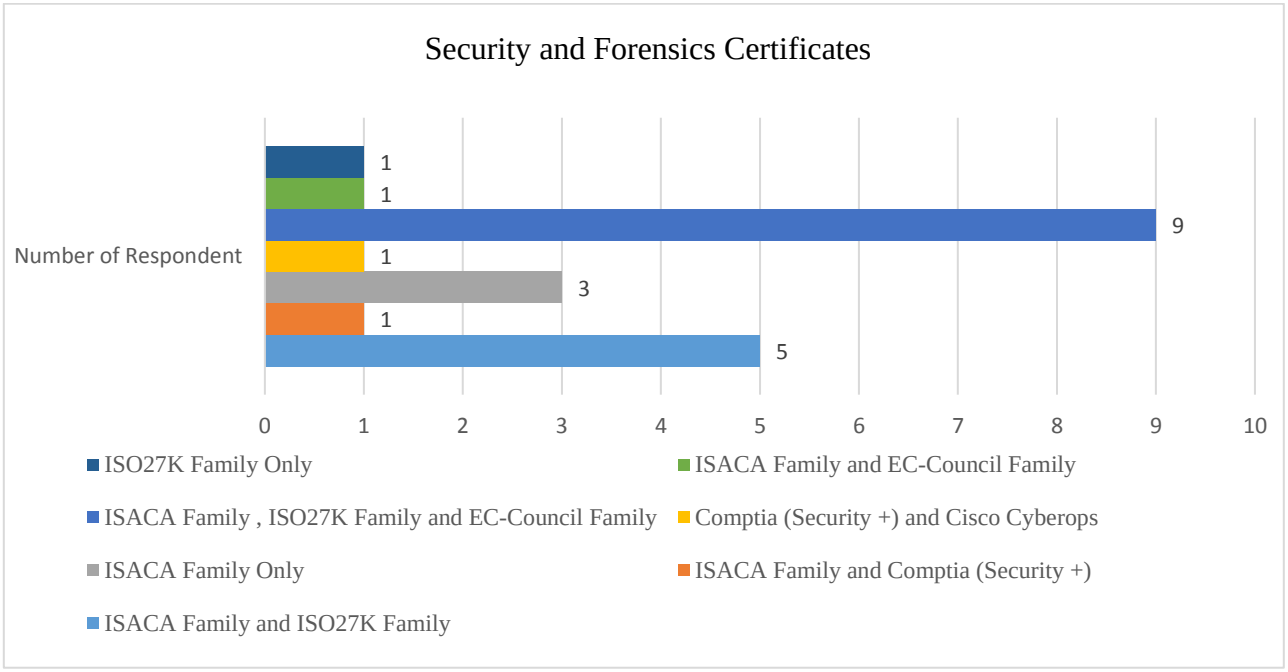


Figure 4.5: Survey Respondent Security and Forensics Certificates.

4.2.4.3 Participant's Work Place Category and Region

For classifying the categories of financial institutes as well as the geographical categorization of each financial institute, we ask respondents to identify the type and nationality of financial institutes, 90% of respondents are working within the banking sector, and only 10% are working in a payment service provider company. This value is justified when comparing the total number of populations in the banking sector and payment service provider firms. As illustrated in Figure 4.6 and Figure 4.7.

Nearly 52 % of respondents are working for international financial institutes, 24 % are working for regional financial institutes, and 24% are working for local financial institutes. Because the survey is internationally distributed, the output of this survey is considered an international output because the majority of respondents are working for international financial institutes.

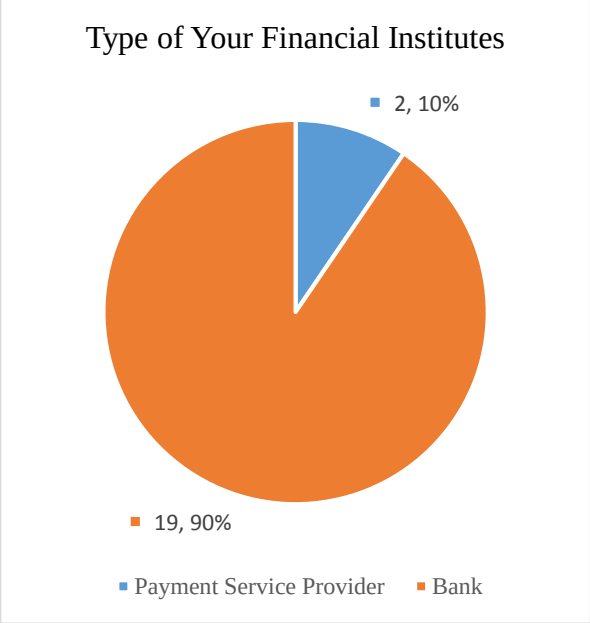


Figure 4.6: Financial Institutes Type.

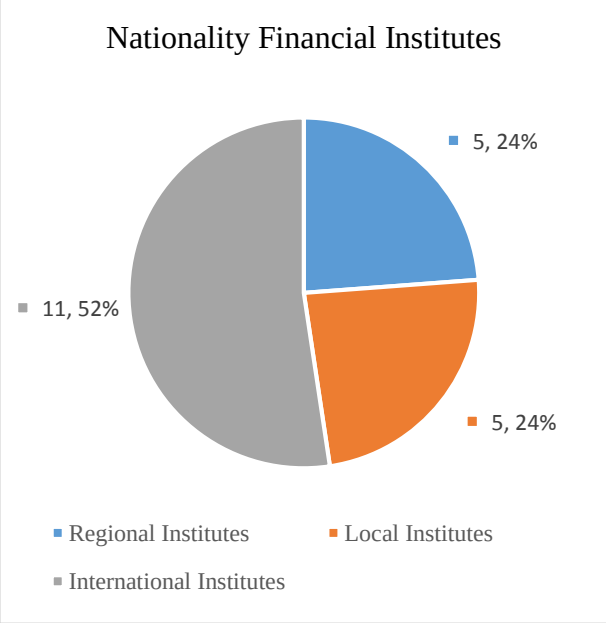


Figure 4.7: Financial Institutes Nationality.

4.2.5 Results Summary

This section presents the summary of research results regarding the survey as a research instrument and data collection method.

4.2.5.1 Information Security General Practices

To assess the maturity of information security practices within financial organizations, we asked respondents about several major components related to information security functions and practices. The majority of respondents said that they have an internal information security department within the organizations they work for. The majority of responses represent that this department has very well-structured and essential components to be considered having a good maturity level of information security within the organization. As illustrated in Figure 4.8.

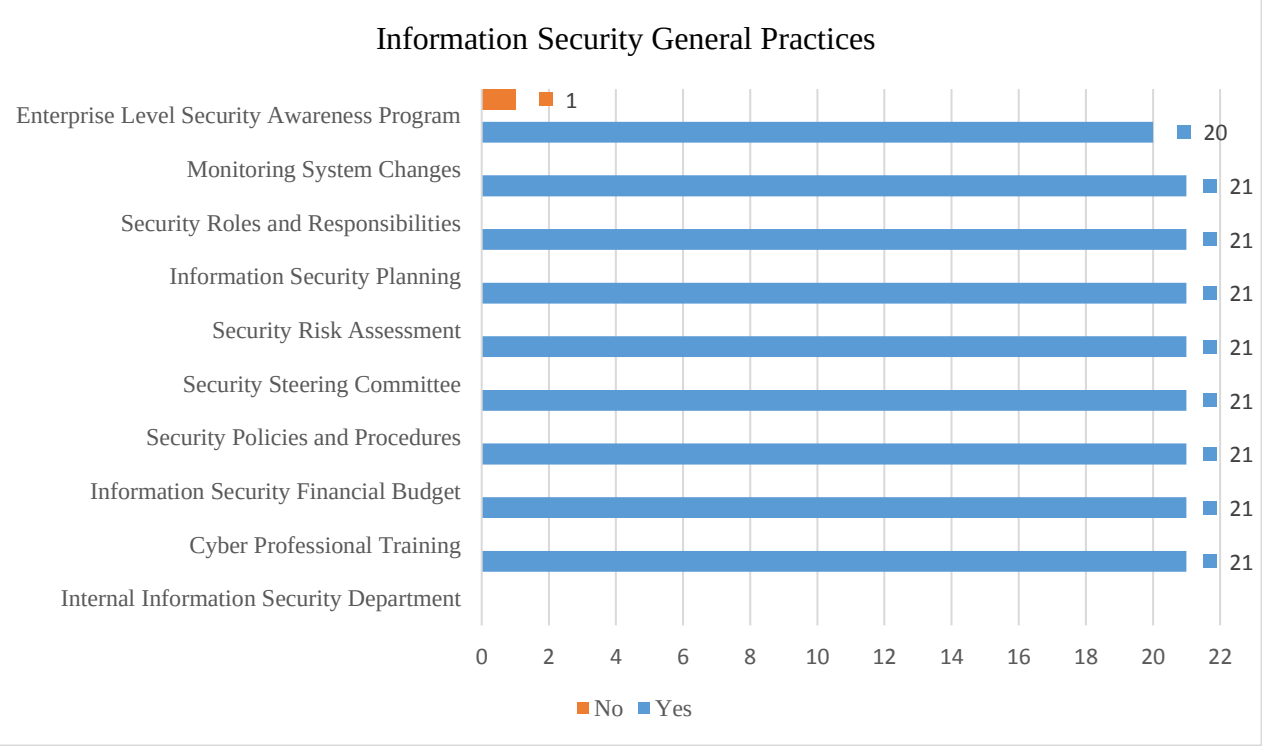


Figure 4.8: Information Security General Practices.

All components practically adapted and practices within the financial organization (collected directly from respondents) should be embedded into the proposed framework design because incident response and digital forensics are essential and core parts of any information security program. components are:

- Information security awareness.
- monitoring processes.
- roles, and responsibilities.
- security planning.
- risk assessment.
- committee.
- Security policies and procedures.
- Financial budget.
- Cyber security training.

4.2.5.2 Cyber Security Incidents Response and Handling Capabilities

To assess the maturity of cyber security incident response and handling capabilities within financial organizations, we asked respondents about several major components related to cyber security incident response and handling capabilities and practices.

The majority of respondents said that they have very well-structured and essential components to be considered having a good maturity level of information security incident handling process within the organization they are working to. As illustrated in Figure 4.9.

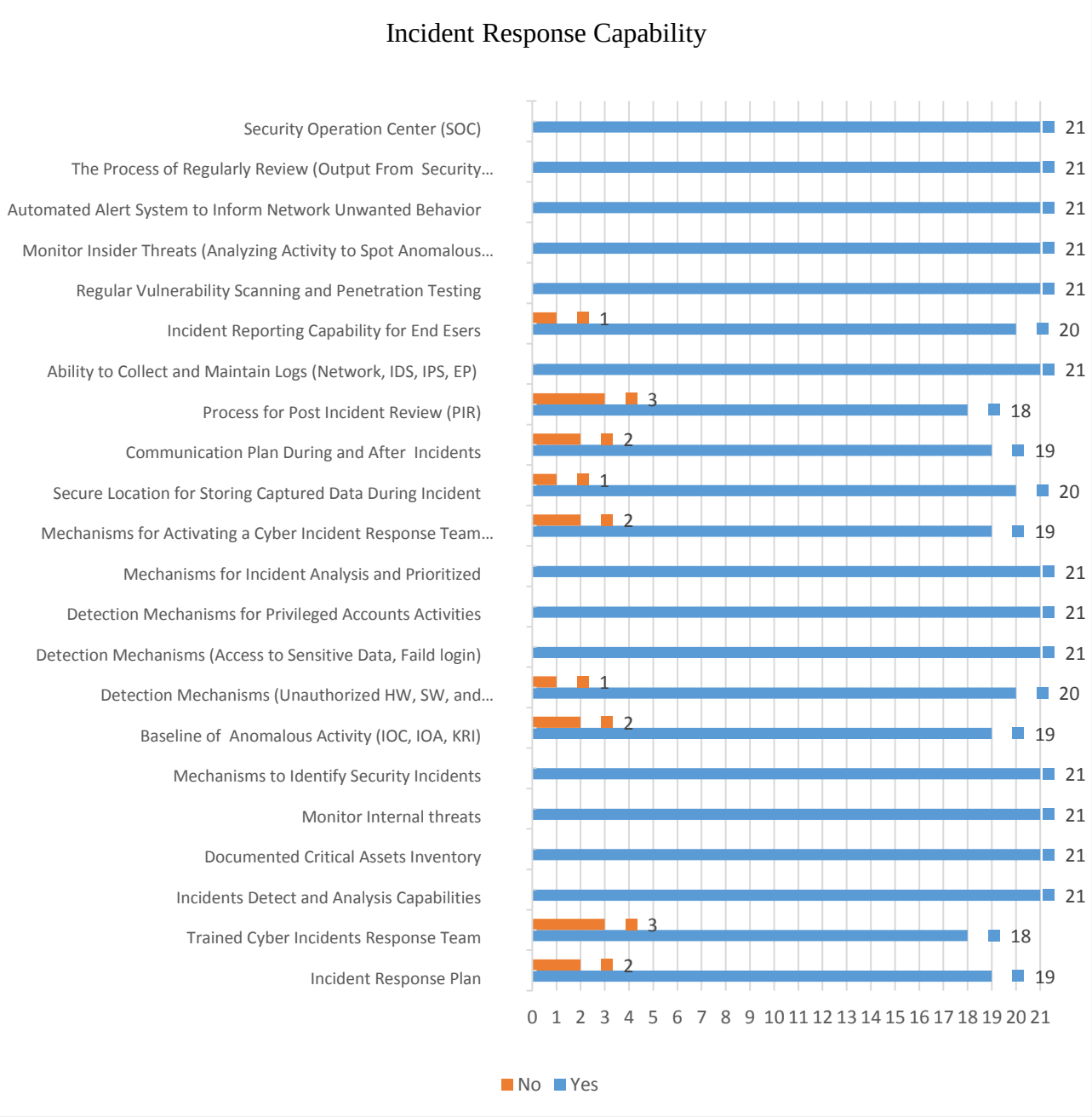


Figure 4.9: Incident Response Capability.

All components practically adapted and practices within the financial organization (collected directly from respondents) should be embedded into the proposed framework design because

incident response and digital forensics are essential and core parts of any information security program. components are listed in Table 4.1:

Table 4.1: Incident Response Components and Process.

No.	Incident response components and processes to be included within the proposed framework
1	Incident response plan
2	Trained cyber incidents response team
3	Incidents detection and analysis capabilities
4	Documented critical assets inventory
5	Monitor internal threats
6	Mechanisms to identify security incidents
7	The baseline of anomalous activity (IOC, IOA, KRI)
8	Detection mechanisms (unauthorized HW, SW, and configuration changes)
9	Detection mechanisms (access to sensitive data, failed login)
10	Detection mechanisms for privileged accounts activities
11	Mechanisms for incident analysis and prioritized
12	Mechanisms for activating a cyber-incident response team (CIRT)
13	Secure location for storing captured data during incident
14	Communication plan during and after incidents
15	Process for post-incident review (PIR)
16	Ability to collect and maintain logs (network, IDS, IPS, EP)
17	Incident reporting capability for end users
18	Regular vulnerability scanning and penetration testing
19	Monitor insider threats (analyzing activity to spot anomalous behavior)
20	Automated alert system to inform the network of unwanted behavior
21	The process of regular review (output from security systems)
22	Security operation center (SOC)

4.2.5.3 Cyber Security Incidents Response, Handling, and Forensics Technologies

Another important factor that needs to be considered within any forensics framework baseline and essential component is the detection and response technologies used and adopted by organizations for executing and operating the process and frameworks, practitioners are asked to report on technologies adapted for detecting and responding to cyber incidents, the majority of respondents report a security detection tools that would support any detection process and activities. That is mainly used for anomalous activity detection and environmental changes. S illustrated in Figure 4.10.

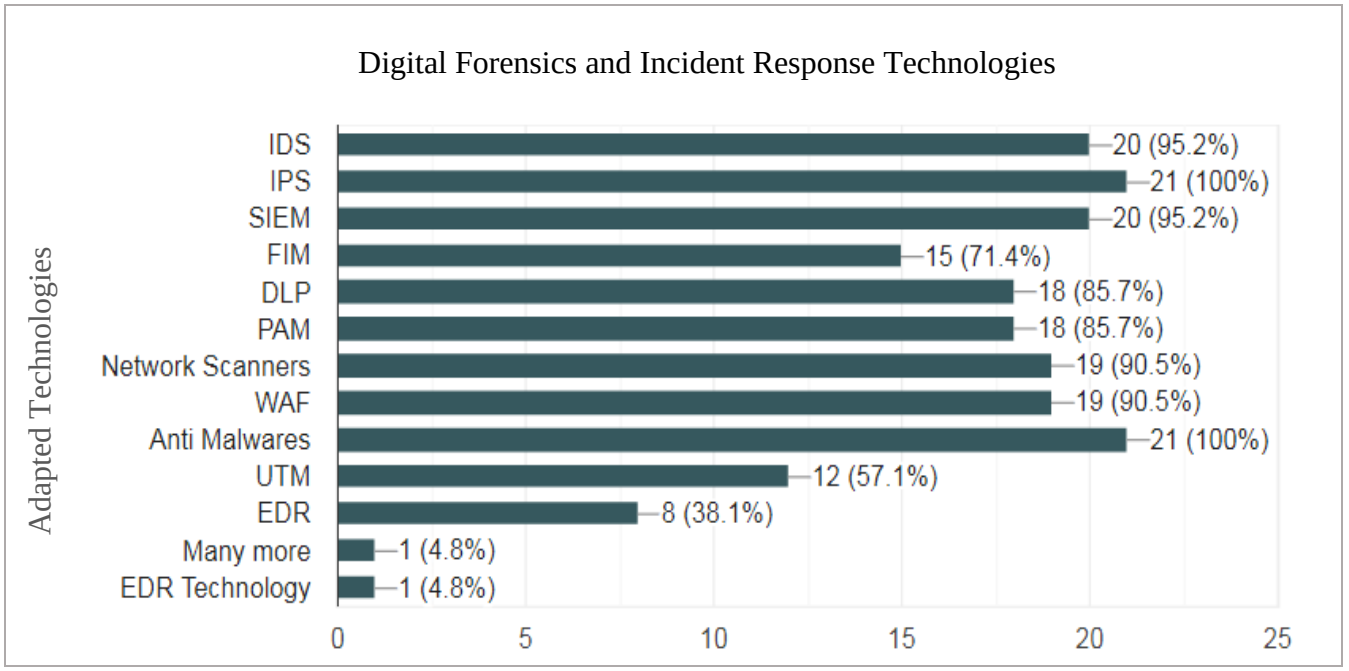


Figure 4.10: Digital Forensics and Incident Response Technologies.

All components practically adapted within the organization should be embedded into the preliminary framework design because incident response and digital forensics are essential and core parts of any information security program. The components are shown in Table 4.2 below:

Table 4.2: Digital Forensics and Incident Response Technologies.

No.	Digital Forensics and Incident Response Technologies To be Included Within Proposed Framework
1	IDS: Intrusion Detection System
2	IPS: Intrusion Prevention System
3	SIEM: Security Information and Event Management
4	FIM: File Integrity Monitoring
5	DLP: Data Loss Prevention
6	EDR: Endpoint Detection and Response
7	PAM: Privileged Access Management
8	Network Scanner
9	WAF: Web Application Firewall
10	Anti-Malware
11	UTM: Unified Threat Management

4.2.5.4 Cyber Security Incidents Response and Handling Frameworks

For establishing the incident handling and response process, the majority of respondents adapt or consider the process of several good practice frameworks, mainly NIST CSF, ISO 27K, CISA, and COBIT), their responses validating grounded work and extracted process within the preliminary framework design because NIST framework considered one of major source framework in the process of designing preliminary framework design because NIST frameworks and models considered one of major source frame, responses are presented within Figure 4.11.

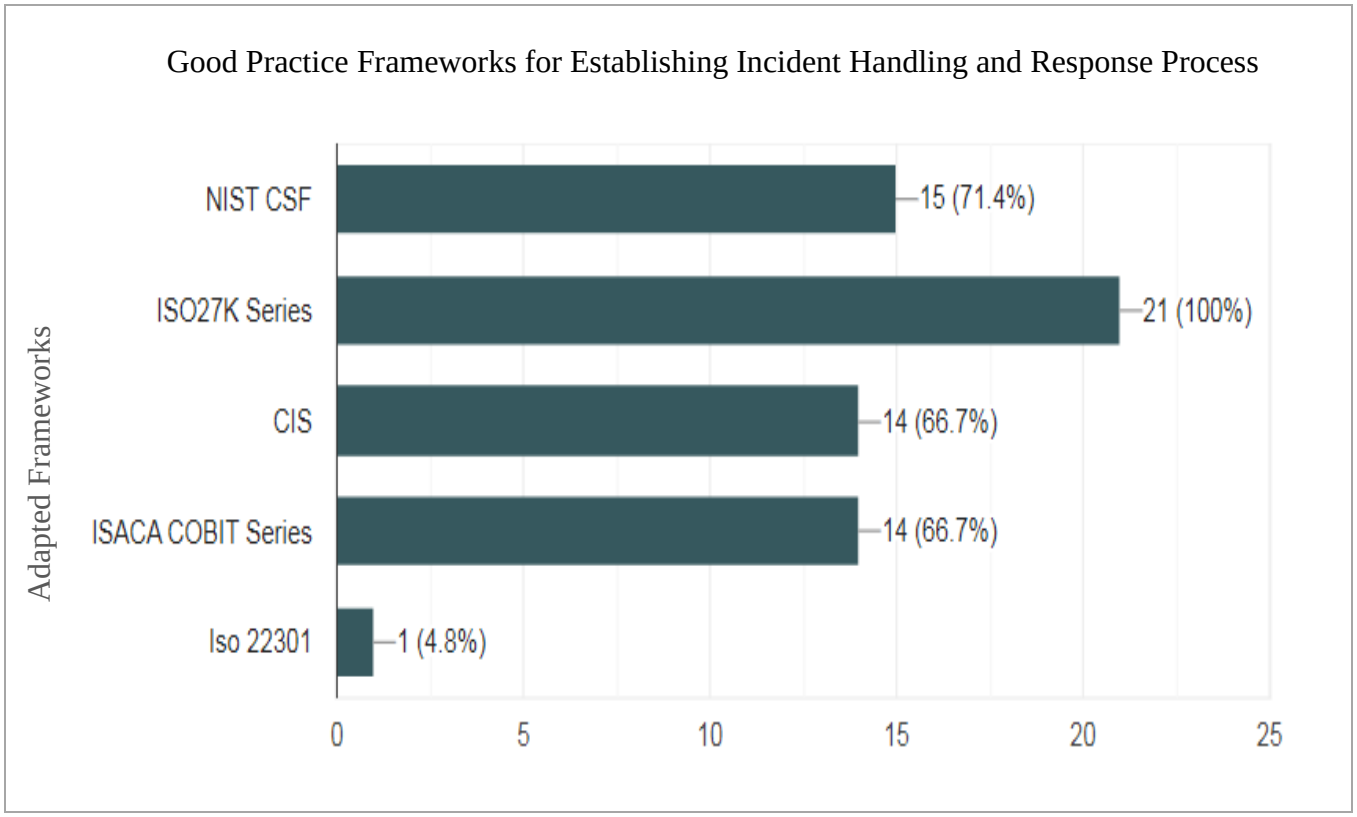


Figure 4.11: Adapted Frameworks for Establishing Incident Handling Process.

4.2.5.5 Cyber Security Threats Indicators, Indicators of Attacks, and Indicators of Compromise

All components practically adapted within an organization should be embedded into the preliminary framework design due detection process of insider threats considered the core purpose of the proposed framework, and all insider threats indicators should be taken into account in revising the preliminary framework design, below major valid responses (6 practitioners did not respond to this question due to confidentiality of the information) major responses are shown in Table 4.3 below.

Table 4.3: Cyber Security Threats Indicators.

No.	Cyber Security Threats Indicators, Indicators of Attacks, and Indicators of Compromise To be Included within the proposed Framework
1	Usage patterns and access to sensitive information and functions for users and privileged users
2	The use of highly privileged systems accounts. Database changes to access secretive data copying of data into external storage. Sending email to personal or web-based email. Use of USB storage devices installation of unauthorized software download of software failed login user management activities
3	Using privileged accounts in daily operations, abnormal process or activities detection by EDR, a large number of files transferred outside the bank, failed access attempts systems or DB's
4	The use of high privilege accounts copying large volumes of data add, delete and user changes configuration change. Security changes ◌network access outside working hours any other indicators based on risk assessment results
5	Superuser activity data copying user provisioning
6	Use of admin accounts, copy classified data, new user change, user delete, users, profile change, configuration changes, database changes, failed login, and user behavior.
7	Excessive firewall denies, scanning, privilege escalation, multiple logins followed by success, huge outbound traffic, shared accounts, unusual patching, unusual high privilege access, unauthorized access
8	Access to sensitive data super user actions use of storage devices copy huge amount of data add user delete user modify user configuration changes un usual logins websites
9	IOC, SHA, hash, IPS
10	Insider threats indicators like access to systems using privileged accounts, user profile changes, user management, access and transfer of sensitive data
11	Admin accounts activities data transfer configuration changes security changes failed login remote access use of mobile codes use of non-original software use of data storage units and sites user provisioning activities
12	Privileged account monitoring, admin access to critical systems, software changes, field login, account management activities, configuration changes, remote access to systems, new software installation, authorization process, use of data storage

4.2.5.6 Digital Forensics and Investigation Capabilities

For further assurance to validate respondent forensics qualifications, (11 out of 21) respondents who represented 52 % of the sample size, consider themselves to have advanced digital forensics and investigation skills in addition, this group is considered qualified to respond to any digital forensics' issues, qualifications of respondents illustrated in Figure 4.12.

These ratios represent a shortage in digital forensics skills when compared to the cyber security skills of practitioners, thus training should be one of the core processes that should be embedded within the preliminary framework design.

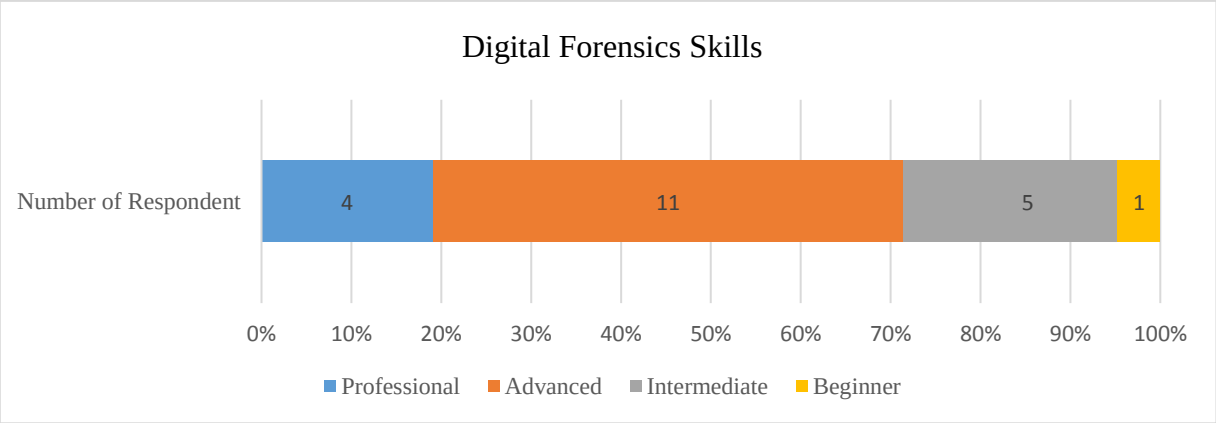


Figure 4.12: Respondent's Digital Forensics Skills.

The majority of the respondents (17 out of 21) said that they do not have an internal digital forensics department within the organizations they work for. The majority of responses represent that there is no process in place for conducting digital forensics, and they do not have any training courses for developing staff for developing team forensics capabilities, Figure 4.13 illustrates DF capabilities based on responses collected.

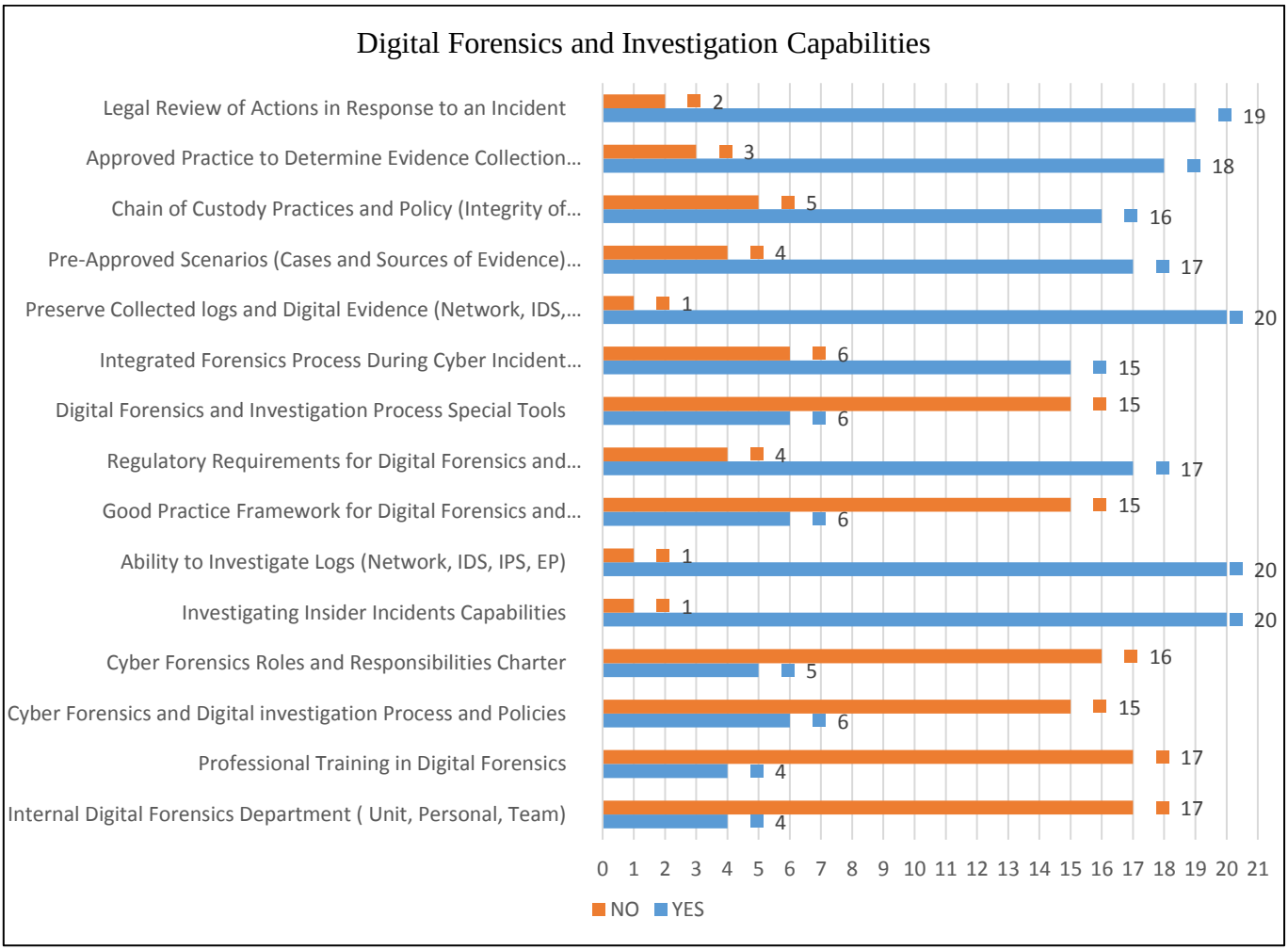


Figure 4.13: Digital Forensics and Investigation Capabilities.

All components practically adapted within the organization should be embedded into the preliminary framework design components as illustrated in Table 4.4 below:

Table 4.4: Digital Forensics Components and Process.

No.	Digital Forensics and Investigation Capabilities To be Included within proposed Framework
1	Internal digital forensics department (unit, personal, team)
2	Cyber forensics and digital investigation process and policies

3	Professional training in digital forensics
4	Cyber forensics roles and responsibilities charter
5	Investigating insider incidents capabilities
6	Ability to investigate logs (network, IDS, IPS, EP)
7	Good practice framework for digital forensics and investigation process
8	Regulatory requirements for digital forensics and investigation process
9	Digital forensics and investigation process special tools
10	Integrated forensics process during the cyber incident response process
11	Preserve collected logs and digital evidence (network, IDS, IPS, EP)
12	Pre-approved scenarios (cases and sources of evidence) that need digital forensics actions.
13	Chain of custody practices and policy (the integrity of collected evidence)
14	Approved practice to determine evidence-collection requirements
15	Legal review of actions in response to an incident

4.2.5.7 Current Incidents Response, Investigations, and Forensics Process

To collect data on the current incident response, investigations, and forensics process within financial organizations, we asked respondents about the actual practices conducted within the work environment. Table 4.5 below lists all valid responses (7 practitioners did not respond to this question due to the confidentiality of the information). All components practically adapted within the organization should be considered within the framework design phases.

Table 4.5: Incident Response, Investigations, and Forensics Process.

No.	Incidents Response, Investigations and Forensics Process To be Included within proposed Framework
1	Framework for banks to handle cyber security incidents, client data disclosure, and thresholds with associated practices for cyber frauds including disclosure to regulators.
2	Incidents identification, detection, analysis, investigation, forensics, containment, reporting
3	Detection, collection, analysis, preserving, presenting
4	Prepare; identify; contain; eradicate; restore; lessons learned
5	We follow the NIST process model
6	Identify a list of internal threats, threat events, detect events, analyze events, investigate and forensics, examine, mitigate or authorize, reporting
7	Incidents identification, detection, analysis, investigation, forensics, containment, reporting
8	NIST typical process: preparation, detection and analysis, containment, eradication, and recovery, post-incident activities, and reporting
9	There are no clear procedures or process
10	Incidents indicators identification, activity detection, incident analysis, investigation and forensics, treatment and responses, recovery and reporting
11	Detection then analysis then escalation then forensics then treatment then mitigation then reporting

4.2.5.8 Recommended Enhancements to Current Incident Response, Investigations, and Forensics Processes.

To collect suggestions for enhancements to current practices, we asked respondents in open-ended questions, to suggest any enhancements on current practices. The majority of respondents say that the current process needs to be enhanced and that they recommend establishing a forensics

process for detecting insider threats. All components practically adapted within an organization should be embedded into the preliminary framework design because the incident response process is considered the core purpose of the proposed framework, below is major valid responses (6 practitioners did not respond to this question due to the confidentiality of the information) are as illustrated in Table 4.6 below:

Table 4.6: Proposes Enhancement of current practices.

No.	Digital Forensics and Investigation Proposes Enhancement on current practices To be Included within proposed Framework
1	A dedicated and trained forensics team.
2	Incident response and handling simulation.
3	The forensics process should be included in the incident response process.
4	Soar automation.
5	Building integrated incident response and forensics process as an early warning system.
6	Establish a well-defined process model during incident response activities.
7	Enhance forensics capabilities to ensure proper investigation of all incidents by establishing forensics formal and documented forensics process.
8	Forensics process (following detection & analysis phase).
9	Incident management procedure built on best practice.
10	Standard and solid forensics process.
11	Establish solid forensics processes that ensure proper training and preparation for all stakeholders.

4.2.6 Proof of Survey Hypothesis

- **Hypothesis one (H1)**. The majority of financial firms have matured cyber security capabilities. Proofed by section (4.2.5.1, 4.2.5.2)
- **Hypothesis two (H2)**. The majority of financial firms have well-defined incident handling and response capabilities and approaches and it is enterprise-level implemented. Proofed by section (4.2.5.2, 4.2.5.3)
- **Hypothesis three (H3)**. The majority of financial firms have basic or no dedicated frameworks for managing digital forensics issues. Proofed by section (4.2.5.6, 4.2.5.7)
- **Hypothesis four (H4)**. The majority of financial firms do forensics investigation as a part of the incident handling and responses process and have third-party arrangements for any specific forensics activities. Proofed by section (4.2.5.6, 4.2.5.7)
- **Hypothesis five (H5)**. The majority of financial firms have deployed solid monitoring processes involving forensics practice without a proper and formal framework. Proofed by section (4.2.5.6, 4.2.5.7)
- **Hypothesis six (H6)**. The majority of financial firms include several incident responses and forensics processes within their internal practices. Proofed by section (4.2.5.6, 4.2.5.7)
- **Hypothesis seven (H7)**. The majority of financial firms have recommended developing dedicated frameworks for managing digital forensics issues. Proofed by section (4.2.5.8)

The majority of results of the survey support our research hypothesis, in addition, all related responses are considered within the framework development process and embedded as a sub-process within the final version of the proposed framework. As illustrated in the next chapter.

4.3 Literature Data Collection and Analysis (Grounded Work)

4.3.1 Identifying and Selecting Source Frameworks and Source Processes

To collect data and extract the relevant forensics and incident response process from the literature and current forensics and incident response models, the source digital forensics, and incident response models were identified and selected amongst several current models that were discussed and analyzed within the literature review section. Source models are considered the reference models for all extracted processes, and form the basic building block of the proposed model to be developed as a result of this research.

Source model selection for this study was designed based on the extracted processes from models covered and identified within previous literature and current forensics and models in the field of forensics process and incident response models.

Wide coverage of digital forensic investigation and incident response processes that are broadly applicable to this research study, and is required to fulfill the aim of the proposed forensics investigation and incident response model.

By adapting and using a coverage metric approach for model verification [91], the researcher quickly identifies and indicates the sourced model's applicability. The source forensics model is said to have good and high coverage value only if the selected source model is a generic forensics and incident response model, and has at least two major investigation processes that support framework major requirements (pillars) and sub-requirements. The model has considered a reduced amount of coverage value if the selected model is not a generic forensics and incident response model, and only describes one forensic and incident response process [66].

The output of the literature data collection and analysis method is identifying and selecting nine (9) common and generic digital forensics models with a total of forty – five (45) identical extracted processes (after removing duplicates) as shown in Table 4.7.

Table 4.7: Source Frameworks and Extracted Processes (Groundwork).

Extracted processes	Source frameworks: digital forensics and incidents generic process models								
	DFRWS	ADFM	IDIP	EIDIP	EMCI	SRDFIM	NIST	SANS	CPMIRDF
Identification	✓	✓						✓	
Preservation	✓	✓				✓			
Collection	✓	✓				✓			
Examination	✓	✓			✓	✓			
Analysis	✓	✓				✓	✓		✓
Presentation	✓	✓				✓			
Decision process	✓								
Preparation		✓				✓	✓	✓	✓
Approach strategy		✓							
Returning evidence		✓							
Readiness			✓	✓					
Physical crime scene investigation			✓						
Digital crime scene investigation			✓						
Review			✓	✓		✓			
Deployment				✓					
Traceback				✓					
Dynamic									
Awareness				✓	✓				
Authorization					✓				

Planning					✓				
Notification					✓				
Search for and identify evidence					✓				
Transport of evidence					✓				
Storage of evidence					✓				
Hypothesis					✓				
Presentation of hypothesis					✓				
Proof/defense of the hypothesis					✓				
Dissemination of information					✓				
Securing the scene						✓			
Survey						✓			
Recognition						✓			
Documenting the scene						✓			
Communication shielding						✓			
Result						✓			✓
Detection							✓		✓
Containment							✓	✓	
Eradication							✓	✓	
Recovery							✓	✓	✓
Post incidents activity and lessons learned							✓	✓	✓
Response									✓
Response strategy									✓
Harvesting									✓
Reduction and organization									✓
Report									✓
Resolution									✓

4.4 Interviews Data Collection and Analysis (Focus Group)

Data collected during the framework validation phase does not require any changes to the framework design. Thus, the interview response is considered the theoretical framework validation.

4.5 Chapter Conclusions and Summary

This chapter explained the data collection process and how data was collected through multiple data collection approaches. In addition, this chapter explained how the exploratory data analysis was conducted and how the researcher used grounded theory and technical approaches to analyze the collected data.

The next chapter (chapter 5), explains and describes the methodology conducted for the framework development process. As well as presenting a comprehensive framework model.

Chapter 5

5. The Methodology and Framework Development

5.1 Introduction

This chapter explains and describes the methodology conducted for the framework development process. As well as presenting a comprehensive framework model.

5.2 High-Level Methodology

In this research, and to develop the proposed DF framework, the following methodology was followed: (the framework development process as illustrated in Figure 5.1)

- Firstly, we have gathered information on digital forensic and incident response models that are grounded in our proposed model. To understand the current trends and needs for DF in the financial sector, as well as understand the current approaches used for integrating DF into IR. This step was completed by collecting and analyzing the literature and related international standards on digital forensics framework and IR and extracting relevant processes from identified source models.
- Secondly, an exploratory assessment questionnaire was developed and sent, and responses were collected from sample financial institutions from different countries (inside and outside Palestine with 21 participant banks and payments companies). This step was done to

understand and explore actual practice, capabilities, and real needs in the area of incident response and digital forensics to explore missing data within the literature and to extract and enhance all relevant processes and practices from a practical and professional perspective.

- Thirdly, a full design for the proposed forensics framework was developed. framework development was conducted by groundwork the extracted core processes, sub-processes, framework major functionalities from the literature, baseline requirements, and source frameworks. As well as introduces enhancements conducted by extraction of actual practices collected by financial institutions through exploratory surveys to enhance the extracted process.
- Fourthly, interviews with a group of experts in the field of cyber security and digital forensics were conducted to validate the theoretical part of the proposed framework. Feedback collected directly from participants' thought-focusing group of (8 participants)
- Finally, the framework was technically validated by testing the ability of framework implementation to detect, investigate, and respond to major insider threats incidents by designing several technical incidents scenarios that simulated real insider threat activities

5.3 Data Analysis Approach

- Comprehensive data analysis was conducted over gathered data (literature groundwork and survey data) to shape the common model elements of generic forensics framework components and to extract applicable components to the financial sector.
- The analysis includes analyzing common elements of related forensics frameworks as well as combining and mapping those elements with the actual practices extracted from survey results to extract final model components applicable to the financial sector.

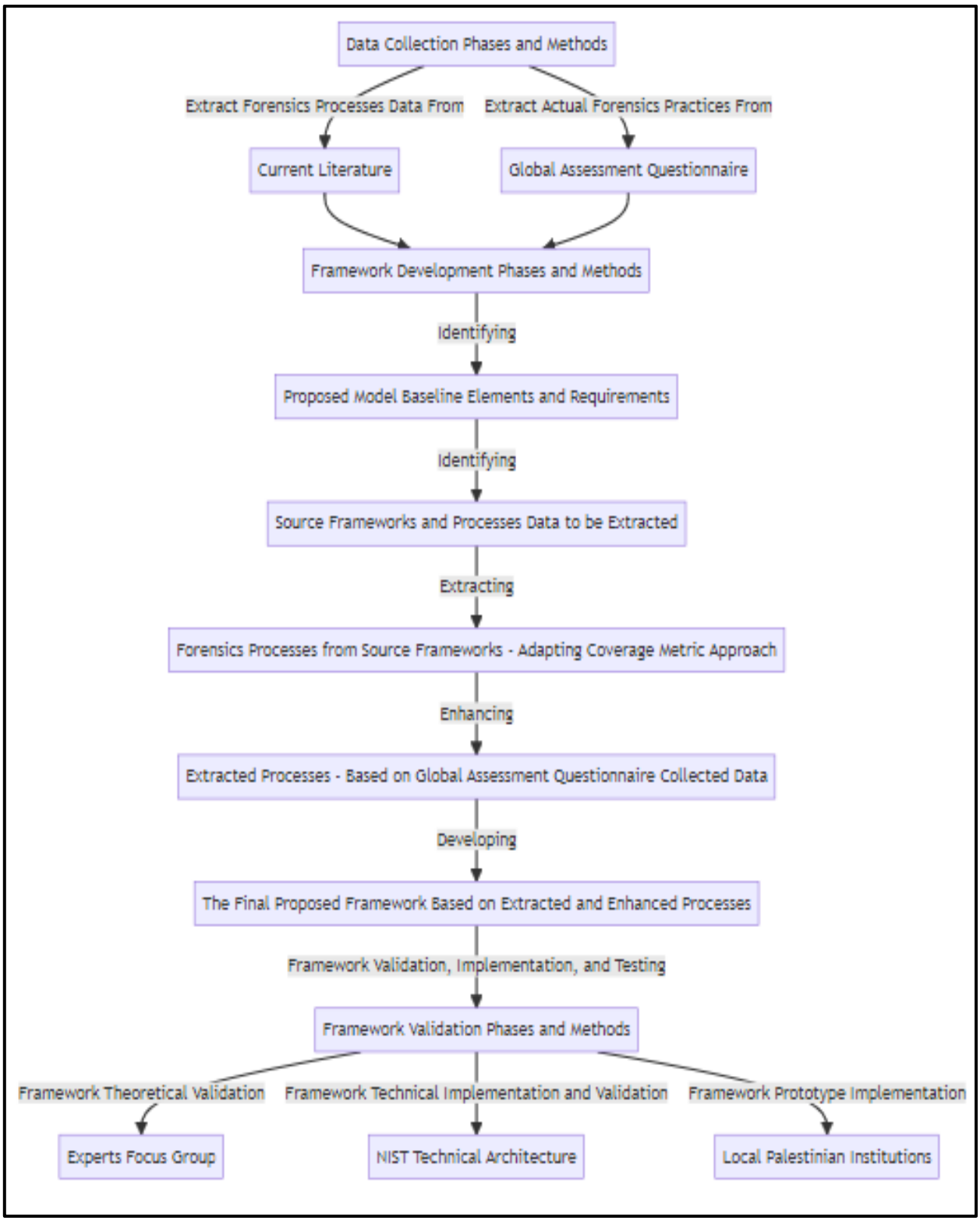


Figure 5.1: Research Methodology and Framework Development Process.

5.4 Framework Design and Development

After completing all steps related to data collection and analysis, the framework preliminary design process is accomplished by analyzing common elements of related generic forensics frameworks that apply to the financial sector and combining those elements with the actual practices extracted from survey results, to select and extract the core components of the research proposed model applicable for the financial sector.

5.4.1 Identifying Baseline Requirements and Readiness Factors of Proposed Framework

As digital forensics readiness elements and factors are considered the core and essential components to assess the maturity and efficiency of any forensics frameworks that enable security professionals to be equipped for digital forensic investigations, the forensics readiness elements can be used as baseline elements of any development process of general forensics framework and process models assessment [92]. Thus, the author utilizes a benchmark baseline component extracted from a combination of two major digital forensics readiness frameworks, one for the general organizational level framework, and the other for the financial sector framework. The utilized baseline components would then be mapped into data extracted from groundwork and survey results to develop our proposed model.

Amongst several digital forensics readiness frameworks developed to assess digital forensics readiness levels, [93] proposed an organizational digital forensics readiness framework as an enterprise-level theoretical framework comprised of two assessment categories, forensic capabilities, and readiness elements. The goal of the proposed framework as mentioned by the author is to “describe a comprehensive approach to identifying the factors that contribute to

digital forensic readiness and how these factors work together to achieve forensic readiness in an organization".

The elements of the selected baseline models are mature and qualified (and tested) to be used as a general baseline framework for organizational digital forensics readiness and assessment process. To be mapped into current generic and specific digital forensics frameworks covered through the literature review section, the extracted forensic readiness organizational factors are listed below:

- Strategy
- Non-technical stakeholders
- Technical stakeholders
- Technology
- System monitoring
- System architecture
- Policy
- Training
- Culture
- Top management support
- Governance

In addition, and to ensure dual sources of framework baseline requirements and assessment factors, [94] proposed a holistic-based framework of digital forensic readiness for the use of the banking sector and financial institutions. The proposed framework consists of eight interrelated

components as basic core components in digital forensic readiness that should be available within any forensics framework and practices. The proposed components are:

- Strategy
- Policy and procedure
- People
- Forensic preparation
- System and events
- Monitor and report
- Risk assessment
- Legal Requirements

After analyzing the forensics baseline elements and eliminating the duplicates between the two chosen forensics baseline and readiness frameworks components, 14 baseline components for the digital forensics readiness framework were extracted to shape the common model elements of generic forensics frameworks requirements and baseline components.as illustrated in Table 5.1 below.

Table 5.1: Forensics Frameworks Requirements and Baseline Components.

DF frameworks baseline requirements (elements)	Organizational digital forensics readiness framework	Holistic-based framework (financial)
Strategy	✓	✓
Non-technical stakeholders	✓	
Technical stakeholders	✓	
Technology	✓	

System monitoring	✓	✓
System architecture	✓	
Policy	✓	✓
Training	✓	
Culture	✓	
Top management support	✓	
Governance	✓	
Policy and procedure	✓	✓
People		✓
Forensic preparation		✓
System and events	✓	✓
Monitor and report	✓	✓
Risk assessment		✓
Legal requirement		✓

To the best of the author's knowledge, and to organize the structure of the proposed framework, digital forensics framework baseline requirements are subject to be arranged and grouped into 5 major requirements (pillars) with 14 sub-requirements (pillars enablers) that support pillars implementation as illustrated in Table 5.2. Below are the major pillars elements:

- **Governance requirements**: direction, management, and execution guidelines.
- **People requirement**: people preparation and human capital training.
- **Infrastructure and technology requirement**: technology and solutions
- **Monitoring requirement**: monitoring process and scope development.

- **Reporting requirement**: pre, during, and post-incident documentation.

Table 5.2: Proposed Framework (Pillars) and Sub-Requirements (Pillars Enablers).

Proposed framework (pillars)	Proposed framework sub-requirements (pillars enablers)
Governance	Strategy
	Policy and procedure
	Culture
	Top management support
	Risk assessment
	Legal requirement
People	Non-technical stakeholders
	Technical stakeholders
	Training
Infrastructure	Technology
	System architecture
Monitoring	System monitoring
	Forensic preparation
Reporting	Reporting

5.4.2 Mapping Source Framework's Extracted Processes into Proposed Framework Pillars Supported by Extracted Process. (Proposed Process Selection)

Mapping source framework's process models that contain a related forensics and response process, into the corresponding proposed frameworks pillars and sub-requirements (pillars

enablers). So that each extracted and grounded process supports the achievements of proposed framework pillars and pillar enablers.

The result of the mapping process shows that all processes extracted from source models (9 source models) are directly or directly, supporting the pillars and sub-requirements of the proposed framework (pillars enablers). Thus, all applicable extracted processes of those models should be selected and included within the design of the proposed model. As illustrated in Table 5.3 and Table 5.4 below.

Table 5.3 Mapping Source Framework's Extracted Processes into Proposed Framework Pillars Supported by Extracted Process.

Extracted processes (grounded)	Proposed framework pillars supported by extracted process	Source frameworks: digital forensics and incidents generic process models								
		DFRWS	ADFM	IDIP	EIDIP	EMCI	SRDFIM	NIST	SANS	CPMIRD
Identification	Monitoring and forensics	✓	✓						✓	
Preservation	Monitoring and forensics	✓	✓				✓			
Collection	Monitoring and forensics	✓	✓				✓			
Examination	Monitoring and forensics	✓	✓			✓	✓			
Analysis	Monitoring and forensics	✓	✓				✓	✓		✓
Presentation	Reporting	✓	✓				✓			
Decision process	Monitoring and forensics	✓								
Preparation	Governance		✓				✓	✓	✓	✓
Approach strategy	Governance		✓							
Returning evidence	Monitoring and forensics		✓							
Readiness	Infrastructure			✓	✓					
Physical crime scene investigation	Monitoring and forensics			✓						

Digital crime scene investigation	Monitoring and forensics			✓						
Review	Reporting			✓	✓		✓			
Deployment	Infrastructure				✓					
Traceback	Monitoring and forensics				✓					
Dynamic	Monitoring and forensics									
Awareness	Governance				✓	✓				
Authorization	Governance					✓				
Planning	Governance					✓				
Notification	Monitoring and forensics					✓				
Search for and identify evidence	Monitoring and forensics					✓				
Transport of evidence	Monitoring and forensics					✓				
Storage of evidence	Monitoring and forensics					✓				
Hypothesis	Governance					✓				
Presentation of hypothesis	Governance					✓				
Proof/defense of the hypothesis	Governance					✓				
Dissemination of information	Monitoring and forensics					✓				
Securing the scene	Monitoring and forensics						✓			
Survey	People						✓			
Recognition	Monitoring and forensics						✓			
Documenting the scene	Reporting						✓			
Communication shielding	Infrastructure						✓			
Result	Reporting						✓			✓
Detection	Monitoring and forensics							✓		✓
Containment	Monitoring and forensics							✓	✓	
Eradication	Monitoring and forensics							✓	✓	

Recovery	Monitoring and forensics							✓	✓	✓
Post incidents activity and lessons learned	Reporting							✓	✓	✓
Response	Monitoring and forensics									✓
Response strategy	Governance									✓
Harvesting	Monitoring and forensics									✓
Reduction and organization	Reporting									✓
Report	Reporting									✓
Resolution	Reporting									✓

Table 5.4 below illustrates a high-level mapping of the source framework's process models into proposed framework pillars and pillar enablers.

Table 5.4: High-Level Mapping of Source Framework's Processes Models into Proposed Framework Pillars and Pillars Enablers.

Proposed framework (pillars)	Proposed framework (pillars enablers)	Forensics and incident respaces models related to proposed framework pillars and sub-requirement								
		DFRWS	ADFM	IDIP	EIDIP	EMCI	SRDFIM	NIST	SANS	CPMIRD
Governance	Strategy		✓			✓				✓
	Policy and procedure	✓	✓							
	Culture					✓				
	Top management support		✓			✓				
	Risk assessment	✓	✓			✓				
	Legal requirement	✓	✓				✓			
People	Non-technical stakeholders					✓				

	Technical stakeholders		✓			✓				
	Training		✓			✓				
Infrastructure	Technology	✓	✓	✓	✓		✓			✓
	System architecture	✓	✓			✓				✓
Monitoring	System & events monitoring	✓	✓			✓	✓	✓	✓	✓
	Forensic preparation	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reporting	Reporting	✓	✓	✓	✓	✓	✓	✓	✓	✓

5.4.3 Model Development and Enhancements of Relevant Processes

After identifying all processes that support achieving the framework pillars, enablers, and baseline requirements, the author starts building the proposed framework based on the results of prior steps. (groundwork data collection and survey data collection)

Major enhancements introduced to the grounded work (to the extracted process from the literature data collection method), enhancements include current process expansion, clarification, and additional sub-processes inclusion to support framework pillars implementation and to foster and strengthen the implementation of (pillars enablers).

The results from prior sections, as well as the current resource on the research topic, are considered a great resource for developing this section as well as the proposed forensics framework, especially when getting all components together and tolerating results into the financial sector. Table 5.5 below illustrates extracted source processes (grounded process) mapped into each source model and the inclusivity and enhancements status of these processes within the proposed model (grounded source process into proposed framework).

Table 5.5: Grounded Source Process into Proposed Framework.

Extracted processes (grounded)	Source frameworks: digital forensics and incidents process models									Process inclusivity and enhancements within the proposed framework (enhanced based on survey data results)
	DFRWS	ADFM	IDIP	EIDIP	EMCI	SRDFIM	NIST	SANS	CPMIRDF	
Identification	✓	✓						✓		Included and enhanced (detection process)
Preservation	✓	✓				✓				Included and enhanced (technology)
Collection	✓	✓				✓				Included and enhanced (technology)
Examination	✓	✓			✓	✓				Included and enhanced (analysis)
Analysis	✓	✓				✓	✓		✓	Included and enhanced (analysis)
Presentation	✓	✓				✓				Included and enhanced (reporting)
Decision process	✓									Included (analysis)
Preparation		✓				✓	✓	✓	✓	Included and enhanced (governance)
Approach strategy		✓								Included and enhanced (governance)
Returning evidence		✓								Not applicable
Readiness			✓	✓						Included and enhanced (governance)
Physical crime scene investigation			✓							Not applicable
Digital crime scene investigation			✓							Included and enhanced (forensics)
Review			✓	✓		✓				Included and enhanced (reporting)
Deployment				✓						Included and enhanced (technology)
Traceback				✓						Included and enhanced (forensics)
Dynamic										Included and enhanced
Awareness				✓	✓					Included and enhanced (governance)
Authorization					✓					Replaced by approved policy and procedures (governance)
Planning					✓					Included and enhanced (governance)

Notification					✓					Included and enhanced (technology)
Search for and identify evidence					✓					Included and enhanced (analysis)
Transport of evidence					✓					Included and enhanced (technology)
Storage of evidence					✓					Included and enhanced (technology)
Hypothesis					✓					Replaced by the risk assessment process
Presentation of hypothesis					✓					Replaced by risk assessment reporting
Proof/defense of the hypothesis					✓					Replaced by risk assessment reporting
Dissemination of information					✓					Replaced by incidents reporting
Securing the scene						✓				Included and enhanced (technology)
Survey						✓				Included and enhanced (analysis)
Recognition						✓				Included and enhanced (forensics)
Documenting the scene						✓				Replaced by evidence preservation, storing
Communication shielding						✓				Not applicable
Result						✓			✓	Replaced by incidents reporting
Detection							✓		✓	Included and enhanced (detection)
Containment							✓	✓		Included and enhanced (contained)
Eradication							✓	✓		Included and enhanced (contained)
Recovery							✓	✓	✓	Included and enhanced (contained)
Post incidents activity and lessons learned							✓	✓	✓	Included and enhanced (reporting)
Response									✓	Included and enhanced (contained)
Response strategy									✓	Included and enhanced (governance)
Harvesting									✓	Replaced by collection
Reduction and organization									✓	Replaced by containment (contained)
Report									✓	Included and enhanced (reporting)
Resolution									✓	Replaced by containment

5.4.4 The Proposed Model and Detailed Enhancements

As the core objective of our proposed model is to be able to support early detection and response process, the three major process categories that need to be enhanced are detection, forensics, and response process as well as incident responses process with flow integration between two other processes.

The early detection process means that we need to work proactively and early before even security incidents occur. Table 5.6 illustrates the proposed framework considering (the extracted process and extracted survey responses) as well as the description of the introduced enhancement.

Due to the lack of detailed information related to the governance and management of cybersecurity and IT process within selected source models, ISACA COBIT 2019 [95], the latest IT governance framework used as a baseline process model for all enhancements introduced and needed for sub-processes related to governance, people, and all other non-technical pillars and enablers of the proposed framework. (mapping framework's governance pillars into COBIT 2019 process)

In addition to table Table 5.6 below, The proposed framework model is illustrated as a process flow diagram in Figure 5.2. The proposed diagram shows the major framework pillars and elements, and how the different framework pillar elements interact and communicate with each other.

Table 5.6: The Detailed Proposed Framework.

Proposed framework (pillars) and baseline requirements (pillars enablers)		Enhanced extracted process for achieving framework (pillars) and baseline requirements (pillars enablers)	Enhancements description
Governance	**G1. Strategy:** The following extracted processes are grouped under strategy enabler and enhanced: ▪ Approach strategy process ▪ Planning Process ▪ Response strategy process	Gs1. Identify and approve value and long-term business goals for the digital forensics and incidents responses program to your organization.	As the strategy is an essential governance enabler and process, it is enhanced by adding multiple strategy and plan development processes [96] [97] [95], as per ISACA COBIT 2019 its governance and process framework. Enhancements include identifying (value, SWOT, gap, roadmap, and resources) for the forensics process.
		Gs2. Conduct a SWOT analysis to match current forensics and IR capabilities and opportunities.	
		Gs3. Assess the current state of the digital forensics and incidents responses program to identify current gaps and challenges through achieving program goals.	
		Gs4. Define the program strategic plan and assign a road map including program initiatives and action items.	
		Gs5. Identify the resources and budget required for achieving approved goals and mitigating identified gaps.	
		Gs6. Include digital forensics and incidents responses strategy into enterprise-level cybersecurity strategy.	
	G2. Policy and procedure The authorization process gives the overall authority and directions for conducting forensics practices, the extracted process is grouped under policy & procedures enabler and replaced by policy and procedure process.	Gp1. Identify digital forensics and incident response services to be delivered to achieve assigned strategic plan initiatives and action items.	As policy and procedure are essential governance enablers, it is enhanced by adding multiple policy and procedure processes [95], as per ISACA COBIT 2019 governance and process framework. Enhancements include identifying (services, programs, enforcement, and updates) for the forensics process.
		Gp2. Create a set of policies to drive digital forensics and incidents responses program expectations and services.	
		Gp3. Develop and continuously maintain operational procedures and all related activities to support the delivered services.	
		Gp4. Roll out and enforce all policies and procedures for all relevant staff so they are built into, and become integral parts of, enterprise digital forensics and incident response operations.	

		Gp5. Periodically evaluate, monitor, and update the policies and procedures to accommodate changes in business environments.	
	G3. Culture The awareness-extracted processes are grouped under culture enabler and enhanced.	Gc1. Identify the level of security maturity of the organization and set up a comprehensive awareness program.	As culture is an essential governance enabler, it is enhanced by adding multiple culture-supporting processes in addition to awareness [96] including identifying (maturity levels, programs, reports, escalating privacy, and evaluating) for the forensics process.
		Gc2. Develop tailored security awareness programs according to the different maturity levels of organizations, and identify the need for continuous training.	
		Gc3. Promote digital forensics and incident responses - aware culture at all levels within the organization and empower the organization proactively to identify, report, and escalate cyber incidents.	
		Gc4. Create a culture of awareness regarding employees' responsibility to maintain security and privacy practices.	
		Gc4. Continuously evaluate the impact of security awareness programs and refine further training when needed.	
	G4. Top management support The top management support extracted survey processes are grouped under the top management enabler and enhanced. This process is practically performed due to the majority of survey responses.	Gt1. Identify the benefits of digital forensics and incident response programs and communicate those benefits to leaders to obtain their support, buy-in, and commitment.	As top management support is an essential governance enabler, it is enhanced by adding multiple management support processes [97][98] including identifying (communicating, finance, and involvement) for the forensics process.
		Gt2. Acquire management commitment to finance the program and ensure proper budget allocation of required resources to the implementation effort.	
		Gt3. Acquire management active involvement in managing and coordinating the program implementation efforts.	

		Gt4. Enforce the implementation of related policies and procedures through management directions.	
	G5. Risk assessment The hypothesis analyzed the asset status (considered part of the risk assessment) The following extracted processes are replaced by and grouped under risk assessment enabler and enhanced: ▪ Hypothesis ▪ Presentation of hypothesis ▪ Proof/defense of the hypothesis	Gr1. Identify and record current assets and their value to the business	As the hypothesis is replaced by risk to enhance the current process, risk assessment is an essential governance enabler, it is enhanced by adding support processes including (records, identity, and events) for the forensics process.
		Gr2. Identify and analyze risk to identified assets.	
		Gr3. Record data on risk events that have caused or may cause business impacts as per the impact categories defined in the risk taxonomy	
		Gr4. Identify and categorize risk events (key risk indicators) that need to be continuously monitored.	
		Gr5. Perform periodic event and risk factor analysis to identify new or emerging risk issues.	
	G6. Legal requirement No extracted process directly supports the enabler. Supporting processes established based on actual practices and survey responses	Gl1. Identify and log external central bank and industry standards compliance requirements.	As legal requirements are an essential governance enabler, it is enhanced by adding support processes including (regulatory requirements) for the forensics process.
		Gl2. Regularly review and adjust digital forensics and incident response policies and procedures for their effectiveness in ensuring proper and necessary compliance with legal and regulatory requirements.	
		Gl3. Continuously obtain regular assurance on the level of external compliance from all related business units.	
People	**P1. Non-technical stakeholders** No extracted process directly supports the enabler. Supporting processes established based on	Pn1. Identify all business stakeholders, their interests, and their areas of responsibility regarding digital forensics.	As non-technical stakeholders are essential people enablers as per ISACA COBIT 2019 its governance and process framework. [95], It is enhanced by adding support processes
		Pn2. Involve all stakeholders who are critical to the decision-making process.	

	actual practices and survey responses	Pn3. Maintain and communicate an awareness of digital forensics processes and associated activities.	including (interests, clarifying involvement, and communication) for the forensics process.
		Pn4. Clarify and communicate business expectations for digital forensics services and solutions.	
		Pn5. Work with all relevant digital forensics stakeholders and coordinate the end-to-end delivery of digital forensics services and solutions provided to the business.	
	P2. Technical stakeholders No extracted process directly supports the enabler. Supporting processes established based on actual practices and survey responses	Pt1. Establish, agree on, and communicate digital forensics-related roles and responsibilities for all personnel within the enterprise.	Technical stakeholders are essential people enablers. [95], It is enhanced by adding support processes including (roles, teams, train) for the forensics process.
		Pt2. Form the appropriate team to carry on the forensics and IR process	
		Pt3. Acquire and maintain adequate and appropriate staffing	
		Pt4. Identify key personnel.	
		Pt5. Maintain the skills and competencies of personnel.	
	P3. Training No extracted process directly supports the enabler. Supporting processes established based on actual practices and survey responses	Ptr1. Identify all required skills and competencies to achieve selected program objectives.	Technical stakeholders are essential people enablers. [95], It is enhanced by adding support processes including (roles, teams, train) for the forensics process.
		Ptr2. Analyze and identify the gap between target skills and capabilities and current skills of the workforce.	
		Ptr3. Develop action plans, to address the identified gaps in skills on an individual level and collective basis.	
		Ptr4. Continuously review training materials and related skill development programs to ensure the adequacy of training concerning the changing enterprise requirements.	

		Ptr5. Provide all staff with access to cyber knowledge repositories to support the development of required skills and competencies	
Infrastructure	**I1. Technology** The following extracted processes are grouped under technology enabler. Processes are replaced and enhanced based on survey responses: ▪ Preservation ▪ Collection ▪ Deployment ▪ Notification ▪ Transport of evidence ▪ Storage of evidence ▪ Securing the scene ▪ Documenting the scene ▪ Harvesting	It1. Acquire and deploy security information and event management solutions (SIEM)	As technology is an essential infrastructure enabler to support the forensics process [99]. It is enhanced by adding supporting technologies that are practically adopted and deployed based on survey data and responses. These technologies include (SIEM, pam, network tools, EDR, forensics platforms, IDS, IPS, FIM, and DLP)
		It2. Acquire and deploy privilege and access management tools (PAM)	
		It3. Acquire and deploy appropriate incidents monitoring and detection solution at the networks level	
		It4. Acquire and deploy appropriate incidents monitoring detection solutions at the application level	
		It5. Acquire and deploy appropriate incidents monitoring detection solutions at endpoint level EDR	
		It6. Acquire and deploy appropriate forensics platform	
		It7. Acquire and deploy appropriate IDS / IPS	
		It8. Acquire and deploy appropriate file integrity and database integrity (FIM)	
		It8. Acquire and deploy appropriate data leakage prevention solutions (DLP)	
		It10. Integrate monitoring solutions into one platform through the SOC architecture	
	I2. System architecture No extracted process directly supports the enabler. Supporting processes established based on actual practices and survey responses	Is1. Enable all logging features within all layers of the system environment.	As system architecture essential infrastructure enablers[25]. It is enhanced by adding support processes including (logging HW, SW, O.S, and hyper).
		Is2. Enable logging at the hardware level.	
		Is3. Enable logging at the operating system level.	
		Is4. Enable logging on the hypervisor level.	
		Is5. Enable logging on the application and database level.	

Monitoring and forensics	**M1. System monitoring – environment preparation** The preparation and notification extracted processes are grouped under environment preparation Enabler. Processes are enhanced based on survey responses	Ms1. Identify log sources and log events. Identify the level of information to be recorded, based on a consideration of risk and performance	As environment preparation is essential monitoring and forensics enablers support the forensics process. It is enhanced by adding supporting preparation processes that are practically adopted and deployed based on survey data and responses. These processes include (log sources, critical assets, notifications, threshold, and threat documented)
		Ms2. Identify and maintain a list of critical infrastructure and business assets that need to be monitored, based on service criticality and the relationship between configuration items and services that depend on them	
		Ms3. Define and implement monitoring and notification rules that identify and record threshold breach indicators (IOA, IOC) and event conditions.	
		Ms4. Continuously produce event logs and retain all logs for an appropriate period to assist in any future investigations process.	
		Ms5. Configure your incident tickets to be created when the monitoring process and notifications identify deviations from pre-defined recorded thresholds.	
		Ms6. Establish process and operations procedures for monitoring event logs from all identified log sources.	
		Ms7. Threats, both from internal and external sources need to be identified, mitigated, and documented	
		Ms8. A baseline network operation and expected data flows for users and systems are established and managed	
	M2. System monitoring – insider events detection The detection extracted process is grouped under the insider events detection enabler. Processes are expanded and enhanced based on	Msi1. Detect, monitor, and control the use of privileged accounts	As insider events detection is core essential monitoring and forensics enablers to support the forensics process for early insider threats detection. It is enhanced by expanding the current process and adding (51)
		Msi2. Log all data that are collected and correlated from multiple sources and sensors.	
		Msi3. Established incident alert thresholds	
		Msi4. Detect, monitor, and control the network is identified potential cybersecurity events	

	both literature and survey responses:	Msi5. Detect, monitor, and control personnel activity to identify potential cybersecurity events	supporting detection processes and exact events of interest. Enhancement sources are extracted from both literature [100] [101] [102] and Practically adopted and deployed processes based on survey data and responses. These events include (Ms.13 to Ms. 51)
		Msi6. Detect, monitor, and control malicious code.	
		Msi7. Detect, monitor, and control unauthorized mobile codes.	
		Msi8. Detect, monitor, and control unauthorized personnel, connections, devices, and software.	
		Msi9. Revoke the response plan during or after an incident	
		Msi10. Detect, monitor, and control mass emailing of sensitive company data to suspicious locations (personal email or cloud-based storage)	
		Msi11. Detect, monitor, and control web browsing history, network crawling, data hoarding, and copying from internal repositories.	
		Msi12. Detect, monitor, and control access to the organization's network, assets, or applications outside of normal office hours or termination notice.	
		Msi13. Detect, monitor, and control emailing company files to personal or web-based email.	
		Msi14. Detect, monitor, and control the use of USB storage devices.	
		Msi15. Detect, monitor, and control the use of cloud-based storage.	
		Msi16. Detect, monitor, and control printing critical data in bulk.	
		Msi17. Detect, monitor, and control sending scanned files to personal or web-based email (from copy machine).	
		Msi18. Detect, monitor, and control the installation of unauthorized software on work computers.	

		Msi19. Detect, monitor, and control remote access to the network at odd times (while on vacation or during sick leave).	
		Msi20. Detect, monitor, and control access to restricted websites.	
		Msi21. Detect, monitor, and control access to sensitive data after termination notice.	
		Msi22. Detect, monitor, and control unnecessary copies of client lists.	
		Msi23. Detect, monitor, and control excessive or unexplained use of data copy equipment (fax, copy, camera).	
		Msi24. Detect, monitor, and control e-mail messages with abnormally large amounts of data.	
		Msi25. Detect, monitor, and control the use of suspicious protocols (e.g. IRC).	
		Msi26. Detect, monitor, and control the use of suspicious services (e.g. VPN, TOR) or personal software on organizational assets to hide activity.	
		Msi27. Detect, monitor, and control the execution of offensive tools.	
		Msi28. Detect, monitor, and control anomalous peaks in outgoing connection count.	
		Msi28. Detect, monitor, and control the download of blacklisted software.	
		Msi28. Detect, monitor, and control attempts to bypass organizational security procedures and technology (disabling anti-malware tools).	
		Msi29. Detect, monitor, and control attempted escalation of privileges.	
		Msi30. Detect, monitor, and control unidentified devices attached (USB, CD-ROM).	

		Msi31. Detect, monitor, and control failed login attempts and authentication failures.	
		Msi32. Detect, monitor, and control different users (attempting to) log in from the same workstation.	
		Msi33. Detect, monitor, and control user logs into a desktop workstation outside working hours.	
		Msi34. Detect, monitor, and control modification of centrally stored log files/modification or destruction of stored log data or files.	
		Msi35. Detect, monitor, and control the user copies a large number of documents to a local disk.	
		Msi36. Detect, monitor, and control configuration file changes.	
		Msi37. Detect, monitor, and control permission changes.	
		Msi38. Detect, monitor, and control database content changes.	
		Msi39. Detect, monitor, and control user accounts used from multiple devices	
		Msi40. Detect, monitor, and control multiple accounts per user.	
		Msi41. Detect, monitor, and control sending emails with usually large amounts of attachments/data outside of organizational networks	
		Msi42. Detect, monitor, and control CMD command execution	
		Msi43. Detect, monitor, and control local FTP scanners containing data transfer.	
		Msi44. Detect, monitor, and control when a user account is disabled, enabled, or deleted.	
		Msi45. Detect, monitor, and control login failure to an expired account.	

		Msi46. Detect, monitor, and control accounts, groups, or privileges change (added or modified) preceded by multiple login failures.	
		Msi46. Detect, monitor, and control new service discovered on the existing host containing new open port found.	
		Msi47. Detect, monitor, and control members added to domain admins or super user groups.	
		Msi48. Detect, monitor, and control successful login with administrative, root, or any special privileges account login.	
		Msi49. Detect, monitor, and control account login alerts on access to SSH, telnet, and RDP either from inside or outside.	
		Msi50. Detect, monitor, and control database user activity such as table and database creation, and procedures executed.	
		Msi51. Detect, monitor, and control created and altered user profiles, roles, and security settings.	
	M3. System monitoring –analysis The following extracted processes are grouped under analysis enabler. Processes are replaced and enhanced based on survey responses: ▪ Examination ▪ Analysis ▪ Search for and identify evidence ▪ Survey	Msa1. Analyze detected events to understand the nature of the event and whether it false positive or a real attack.	As analysis is an essential process for monitoring and forensics enablers. It is enhanced by replacing extracted analysis processes with those that are practically adopted and deployed based on survey data and responses.
		Msa2. Analyze detected events to understand the attack. Targets and methods.	
		Msa3. Asses potential damage to and theft of resources	
		Msa4. Classify events based on potential damage to identify recovery scope. Activate IR team for classified critical incidents	

	M4. System monitoring –forensics The following extracted processes are grouped under the forensics enabler. Processes are replaced and enhanced based on survey responses: ▪ Digital crime scene investigation ▪ Traceback ▪ Recognition	Msf1. Investigate detected events and all notifications from detection systems.	As forensics is an essential process for monitoring and forensics enablers. It is enhanced by replacing extracted forensics processes with those that are practically adopted and deployed based on survey data and responses.
		Msf2. Traceback detected events and all notifications from detection systems into the source to identify the initiation scenarios of events and root causes.	
		Msf3. Identifying the attacking hosts.	
		Msf4. Gather and handle all evidence information from multiple sources.	
		Msf5. Secure documents and preserve evidence.	
	M5. System monitoring –incidents contained and recovery The following extracted processes are grouped under incidents contained and recovery enabler. Processes are replaced and enhanced: ▪ Containment ▪ Eradication ▪ Recovery ▪ Response ▪ Reduction and organization ▪ Resolution	Msc1. Choose and follow a containment strategy based on incident type to mitigate incidents and isolate affected hosts.	As incidents are contained recovery is an essential process for monitoring and forensics enablers. It is enhanced by clarifying extracted processes and reformatting titles to match the form of a do list and action items
		Msc2. Revoke the recovery plan and ensure it is executed during or after a cybersecurity incident.	
		Msc3. Switch over to alternate clean hosts.	
		Msc4. Clean environment and switch back to the original clean environment. (restore systems to normal operation)	
	M6. Forensic preparation (continuous) The dynamic processes are grouped under preparation enabler. Processes are replaced by updating the framework	Mf1. Continuously monitor and evaluate (g1, g2, g3, g4, g5, g6, p1, p2, p3) before closing of incidents.	Continuous preparation is an essential process for monitoring and forensics enablers and review of activities. It is enhanced by continuously monitoring and updating a framework
		Mf1. Continuously update the (m2) list of insider threat indicators before the closing of incidents.	

Reporting	**R1. Reporting** The following extracted processes are grouped under the reporting enabler. Processes are replaced and enhanced based on survey responses: ▪ Presentation ▪ Review ▪ Dissemination of information ▪ Result ▪ Report	Rr1. Report on incidents with collected evidence and established criteria and escalation mechanisms.	Continuous preparation is an essential process for monitoring and forensics enablers and review of activities. It is enhanced by clarifying extracted processes and reformatting titles to match the form of a do list and action items
		Rr2. Document the root cause of incidents and lessons learned to enhance early detection and response approach.	
		Rr3. Examine the current and future mandatory reporting requirements relating to security incidents for all internal and external parties.	

5.5 Chapter Conclusions and Summary

This chapter explained and described the methodology conducted for the framework development process. As well as presenting a comprehensive framework model. The next chapter (chapter 6), presents and discusses a summary of the research results, as well as the framework validation, implementation, and testing process (theoretical and technical validation).

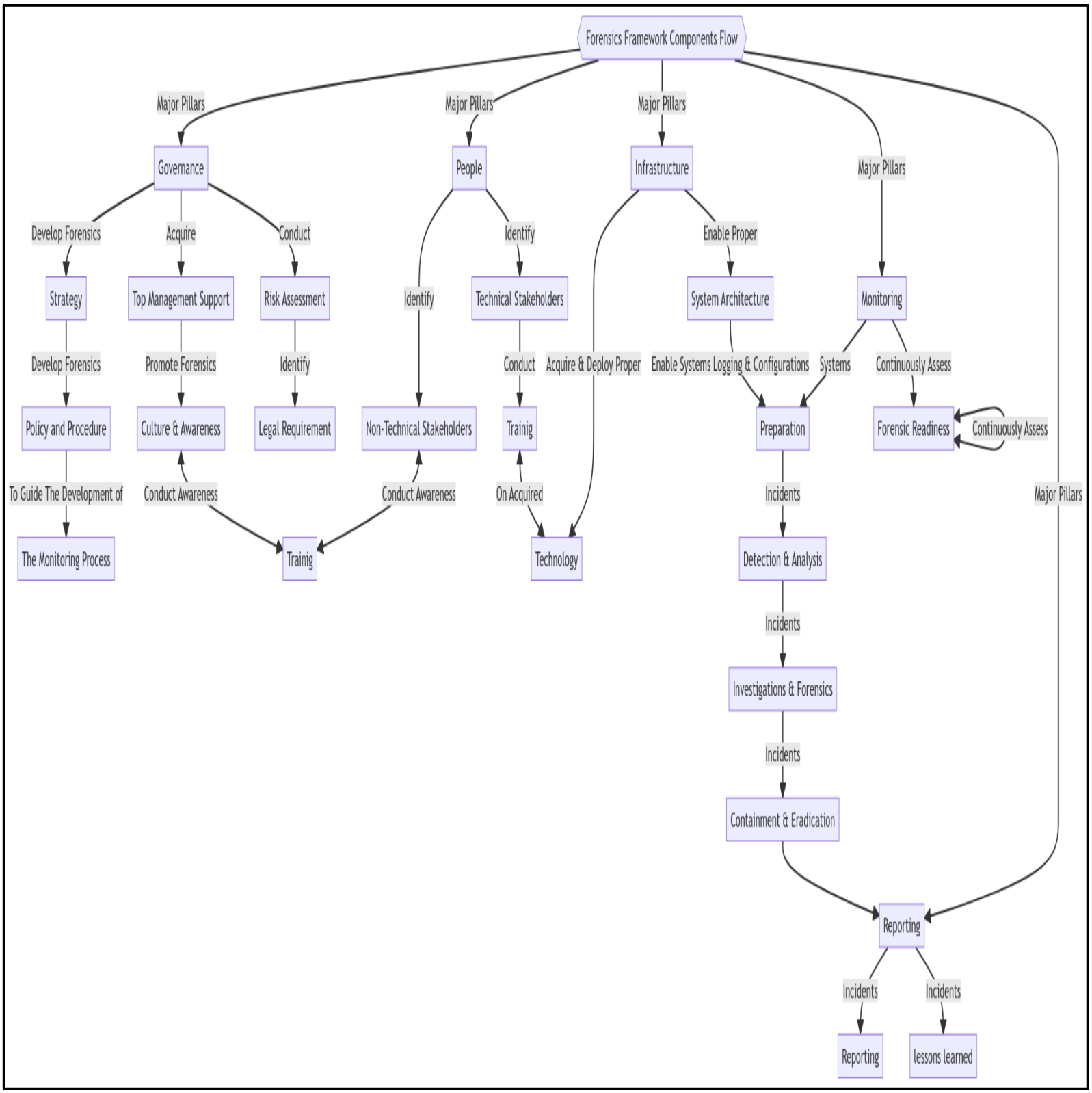


Figure 5.2: The Proposed Framework Model - Process Flow Diagram

Chapter 6

6. Results, Discussion, and Framework Validation

6.1 Introduction

This chapter mainly aims to present and discuss a summary of research and thesis results as well as the following goals:

- Present the summary results of the research.
- Discuss the proposed framework and comparison between the proposed model and existing models.
- Conducting theoretical framework validation.
- Conducting technical framework validation and testing using real insider cyber security incident cases.

6.2 Results Summary

This thesis proposed a novel integrated DF and IR framework, which is further termed (FFEDRICI). The proposed framework would serve as an insider threats incidents management program and security incidents early warning model within the critical financial digital environment.

The proposed model is an integrated and hybrid model that is considered the first ever DF and IR model developed and directed for financial environments. With major aims to:

- Provide the organization's cyber security professionals, forensics investigators, and incident handling teams, with a digital forensics framework and process model to assist them during the cyber investigation process followed by internal cyber incidents.
- Provide financial organizations with well-designed and mature digital forensics and incident response capability model, to ensure early detection and effective responses to internal cybersecurity incidents, as well as reduce and mitigate the potential impact and consequences of incidents on time

The proposed model is supported by five essential pillar requirements and consists of (14) sub-requirements (pillars enablers) and (134) processes and a to-do- list, as illustrated in Table 6.1.

These identified pillars are essential for a digital forensic investigation to be conducted properly and efficiently, ensuring food preparation for implementation.

Table 6.1: The Proposed Framework Summary.

Proposed framework (pillars)	Proposed framework (pillars enablers)	Number of processes
Governance	G1. Strategy	(gs1 – gs6): 6
	G2. Policy and procedure	(gp1 – gp5): 5
	G3. Culture	(gc1 – gc4): 4
	G4. Top management support	(gt1 – gt4): 4
	G.5 Risk assessment	(gr1 – gr5): 5
	G.6 Legal requirement	(gl1 – gl3): 3
People	P1. Non-technical stakeholders	(pn1 – pn5): 5
	P2. Technical stakeholders	(pt1 – pt5): 5
	P3. Training	(ptr1 – ptr5): 5

Infrastructure	I1. Technology	(it1 – it10): 10
	I2. System architecture	(is1 – is5): 5
Monitoring	M1. System monitoring - preparation	(msp1 – msp8): 8
	M2. System monitoring - detection	(msi1 – msi51): 51
	M3. System monitoring - analysis	(msa1 – msa4): 4
	M4. System monitoring - forensics	(msf1 – msf5): 5
	M5. System monitoring - contained	(msc1 – msc4): 4
	M6. Forensic preparation	(mf1 – mf2): 2
Reporting	R1. Reporting	(rr1 – rr3): 3

6.3 Discussion and Comparison between the proposed model and existing models

In this section, the current DF and IR models are compared with the proposed one concerning their respective efficiency, and major capabilities based on several comparison criteria presented within the below sub-section and Table 6.2.

6.3.1 Models Purpose and Applicability as Comparison Criteria

Comparison to the existing DF and IR models, which considered high-level general-purpose frameworks that do not focus on a specific industry or digital environment. The proposed framework is an integrated and hybrid model that is considered the first ever DF and IR model developed that applies to and is directed for internal use of the financial environment.

6.3.2 Data Collection and Incident Detection as Comparison Criteria

As the core objective of our proposed model is to be able to support the early detection and response process, special attention should be given to the process of data collection and incident

detection within the framework to enhance the overall monitoring process to ensure early and proactive capabilities to detect and identified incidents before even the incidents occur.

Compared to the majority of existing DF and IR models that do not determine what kind of user activities should be collected, logged, and monitored. The existing frameworks might fail to collect enough information as well as fail to detect actual incidents promptly which is essential data to analyze the insider's activities.

The proposed framework has given special attention to the process of data collection and incident detection within the framework process to enhance the overall monitoring process. Enhancements introduced into the proposed framework by deeply identifying which kind of user activities need to be collected, logged, and monitored, as well as proactively determining which activities and threats indicators are necessary to carry out an investigation and analysis process.

6.3.3 Infrastructure and Technology as Comparison Criteria

As infrastructure and technology deployment is considered one of the core forensics capabilities and readiness drivers, as well as the critical importance of infrastructure and technology as essential DF and IR models implementation drivers., special attention should be given to the process of infrastructure and technology selection and implementation. To enhance the capabilities of detecting and analyzing the insider's activities.

Compared to the majority of existing DF and IR models that do not determine what kind of IT infrastructure and technology deployment need for an efficient forensics process, the existing

frameworks might fail to select and deploy the infrastructure and technology required to detect and analyze the insider's activities.

The proposed framework has given special attention to the process of infrastructure and technology selection and implementation within the framework process to enhance overall infrastructure and technology environments. Enhancements introduced into the proposed framework by deeply identifying which kind of infrastructure and technology solutions should be selected, acquired, and deployed to ensure proper data collection, incident detection, analysis, and investigation of insider threats incidents

6.3.4 Process Design Inclusivity as Comparison Criteria

Compared to the majority of existing DF and IR models, which focused purely on stand-alone forensics investigations and cyber incidents response processes, such as incident detection, data collection, evidence preserving and reconstruction, data analysis, and documentation, the proposed framework is an integrated and hybrid model that considered the first ever integrated DF and IR model have developed and directed for financial environments.

The proposed model is an enhanced comprehensive model consisting of the majority of extracted processes from current DF and IR models, with introduced enhancements to the majority of them. Table 6.2 lists extracted processes from various current digital forensics and incidents models. As well as an inclusivity comparison between processes included within current models and processes included within the proposed model.

Table 6.2: Process Inclusivity Comparison between current models and the proposed model.

Extracted processes (current DF and IR models)	Current digital forensics and incidents process models (available process per model)									Process status and enhancements within the proposed framework (FFEDRICI).
	DFRWS	ADFM	IDIP	EIDIP	EMCI	SRDFIM	NIST	SANS	CPMIRDF	
Identification	✓	✓						✓		Included and enhanced (detection process)
Preservation	✓	✓				✓				Included and enhanced (technology)
Collection	✓	✓				✓				Included and enhanced (technology)
Examination	✓	✓			✓	✓				Included and enhanced (analysis)
Analysis	✓	✓				✓	✓		✓	Included and enhanced (analysis)
Presentation	✓	✓				✓				Included and enhanced (reporting)
Decision process	✓									Included (analysis)
Preparation		✓				✓	✓	✓	✓	Included and enhanced (governance)
Approach strategy		✓								Included and enhanced (governance)
Returning evidence		✓								Not applicable
Readiness			✓	✓						Included and enhanced (governance)
Physical crime scene investigation			✓							Not applicable
Digital crime scene investigation			✓							Included and enhanced (forensics)
Review			✓	✓		✓				Included and enhanced (reporting)
Deployment				✓						Included and enhanced (technology)
Traceback				✓						Included and enhanced (forensics)
Dynamic										Included and enhanced
Awareness				✓	✓					Included and enhanced (governance)
Authorization					✓					Replaced by approved policy and procedures (governance)
Planning					✓					Included and enhanced (governance)

Notification					✓					Included and enhanced (technology)
Search for and identify evidence					✓					Included and enhanced (analysis)
Transport of evidence					✓					Included and enhanced (technology)
Storage of evidence					✓					Included and enhanced (technology)
Hypothesis					✓					Replaced by the risk assessment process
Presentation of hypothesis					✓					Replaced by risk assessment reporting
Proof/defense of the hypothesis					✓					Replaced by risk assessment reporting
Dissemination of information					✓					Replaced by incidents reporting
Securing the scene						✓				Included and enhanced (technology)
Survey						✓				Included and enhanced (analysis)
Recognition						✓				Included and enhanced (forensics)
Documenting the scene						✓				Replaced by evidence preservation, storing
Communication shielding						✓				Not applicable
Result						✓			✓	Replaced by incidents reporting
Detection							✓		✓	Included and enhanced (detection)
Containment							✓	✓		Included and enhanced (contained)
Eradication							✓	✓		Included and enhanced (contained)
Recovery							✓	✓	✓	Included and enhanced (contained)
Post incidents activity and lessons learned							✓	✓	✓	Included and enhanced (reporting)
Response									✓	Included and enhanced (contained)
Response strategy									✓	Included and enhanced (governance)
Harvesting									✓	Replaced by collection
Reduction and organization									✓	Replaced by containment (contained)
Report									✓	Included and enhanced (reporting)
Resolution									✓	Replaced by containment

6.4 Framework Validation

According to Hammersley, any qualitative research should be judged according to both validity and relevance [103]. Within this context, "relevance relates to whether the study (i) addresses meaningful questions to the population of interest, (ii) adds to the existing knowledge base". Thus, the proposed conceptual framework needs to be judged regarding its validity and relevance to the financial sector by adapting the validation techniques presented within the below sub-sections.

6.4.1 Framework's Theoretical Validation

This section aims to explore the validity and relevance of the proposed conceptual framework - from a theoretical perspective - for the use and applicability of adaption by the financial sector. Validation was conducted by using feedback data collected directly from a focus group of eight experts in the field of cybersecurity and digital forensics within the financial sector. To highlight and identify areas of deviance between the proposed conceptual framework and the discussion generated from the focus groups.

Interviews responses data and expert opinions were collected to acquire theoretical validation of the proposed framework, as well as validate the applicability of framework elements to the financial sector. Expert opinions were documented on the developed framework, with the conclusion of no need to revise the developed framework as explained in the next paragraph.

Our main finding generated from the focus group is that the discussion generated at the group meeting provided robust and sufficient evidence to support the validity of the DF and IR pillars, sub-requirements, and process (to–do process) identified in the proposed DF conceptual

framework to be used and deployed by the financial sector. Thus, this section demonstrated that the proposed DF conceptual framework for early detection and response to internal cyber security incidents is both valid and relevant for use within financial sector practice.

6.4.2 Framework's Technical Implementation and Validation

This section aims to explore the technical implementation and validity of the proposed conceptual framework - from a technical perspective – for the technical efficiencies and capabilities in detecting and investigating insider threats events and incidents based on identified technologies and detection techniques and threats indicators of attack within the proposed framework.

To achieve this objective, two different simulation cases of insider threat activities were used for the technical implementation and validation process. In both cases, the proposed framework procedures that followed, allow real-time detection, analysis, investigation, and response to simulated insider threat activities cases. Thus, this section demonstrated that the proposed DF conceptual framework for early detection and response to insider cyber security incidents is valid, capable, and efficient for early detection and response to insider cyber security incidents.

For technical implementation, detection, and response to insider threats and insider destructive incidents, NIST “special publication 1800-26” proposed a “high-level architecture for the implementation of a DI solution that detects and responds to ransomware and other internal destructive events” [104]. The proposed technical implementation architecture as shown in Figure 6.1 is considered effective and efficient for technical implementation, testing, and

validation of our proposed framework, hence considered technical validation testing of our framework due to the following purposes:

- When selecting specific test scenarios for testing the proposed framework, NIST technical implementation architecture by design and test has proven effective and efficient capabilities in detecting, investigating, and responding to a wide range of insider similar threat scenarios and threat indicators that are covered by our proposed framework. Hence considered technical implementation and technical validation testing of our framework regarding insider threats activities and indicators.
- NIST technical implementation architecture by design and test introduced and adopted a wide range of it infrastructure technologies and security solutions that have proven solid capabilities in detecting, investigating, and responding to a wide range of insider threat scenarios and threat indicators that are similar to its infrastructure technologies and security solutions covered by our proposed framework. Hence considered technical implementation and technical validation testing of our framework regarding adopting its infrastructure technologies and security solutions
- NIST technical implementation architecture by design and test introduced and adopted a wide range of reporting, alerting, and notification capabilities generated from various components of the technical architecture and the security team. The proposed technical architecture allows alerting based on pre-defined events and incidents through email and dashboards. NIST's proposed reporting capabilities are similar to reporting capabilities and requirements covered by our proposed framework. Hence considered technical validation testing of our framework regarding insider threat activities reporting.

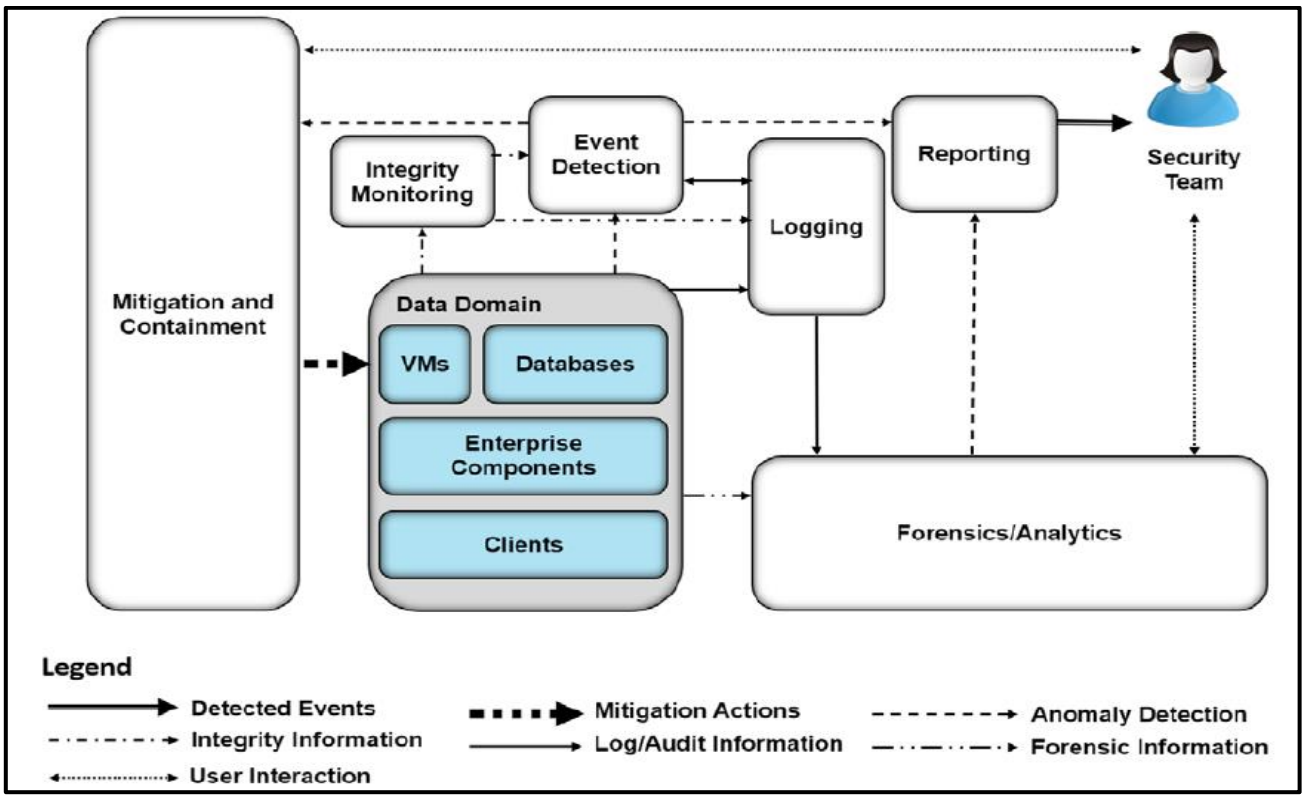


Figure 6.1: NIST Data Integrity Detect & Respond High-Level Architecture [104]**.**

6.4.2.1 NIST Applicable Case 1: Database Modification Via Malicious Insider

Case 1 simulation assumes that a malicious insider threat actor has direct access to an enterprise central database through a web page. The insider threat exploits a vulnerability exposed on the web page to delete a huge volume of the data stored within the database.

Case Identification Detection and Response

The technical implementation architecture by design provides multiple layers of defense against such cases. The architecture integrity monitoring capability is mainly used to detect any changes to the database. These changes in real time, are forwarded to the logging solutions and capability, which also collects all information about web requests. The reporting solutions and capability provide the ability to generate notifications and alerts to inform the security team of anomaly

events. The forensics/analytics solutions and capability are used to investigate and identify malicious access. Below are the details of detection and mitigation steps by adapted solutions:

- The tripwire enterprise (the adapted integrity monitoring solution) successfully monitors the committed changes by malicious insiders to the database configuration.
- The ArcSight ESM (the adapted logging solution) successfully logs all changes to the database and web page requests.
- The ArcSight ESM (the adapted reporting solution) successfully alerts and notifies the security team of all malicious changes to the database.
- Symantec security analytics (the adapted forensics/analytics solution) allows the identification of malicious web page requests that caused the malicious database records deletion

6.4.2.2 NIST Applicable Case 2: File Modification via Malicious Insider

Case 2 simulation assumes that malicious insiders have stolen administrator-level authentication credentials through social engineering and non-technical means. The insider threat actor, using these stolen authentication credentials, has used remote Windows PowerShell sessions to uniformly modify employee stock information to their benefit across several machines. This type of attack will also target the enterprise's data backup system to modify all records of the previously loaded stock information.

Case Identification Detection and Response

The technical implementation architecture by design provides multiple layers of defense against such cases. The architecture integrity monitoring capability detects malicious changes to files

and backups caused by a malicious insider. When incident information is forwarded to the architecture logging and reporting solutions and capabilities, the architecture can report on these changes in real-time. When the security team is notified and alerted to malicious insider activities, they can use the architecture mitigation and containment solutions and capability to disable the malicious insider's access. Below are the details of detection and mitigation steps by adapted solutions:

- The tripwire enterprise (the adapted integrity monitoring solution) successfully detects insider's malicious changes to original files and backups caused by a malicious insider.
- The ArcSight ESM (the adapted reporting solution) successfully reports and alerts security administrators via email on all changes made to original and backup files by a malicious insider.
- The Semperis DSP (the adapted mitigation and containment solution) successfully disables the malicious user accounts that are associated with malicious insider actor activity.

6.5 Framework Implementation Within the Palestinian Financial Sector

Even though the proposed framework is considered an international framework and valid for deployment within the majority of financial institutions worldwide regardless of the geographical location of those institutions, this section discusses the ability to deploy the proposed framework within the Palestinian financial sector, taking into account current cybersecurity regulations related to the implementation of insider threats management approaches.

As mentioned earlier in the literature review section, financial institutions worldwide, are operating under central bank regulations of each country. Such banks are considered the only

authorized bodies for issuing regulations, financial policies, and various standards that need to be implemented within the financial sector of that country. Cybersecurity and IT regulations are some of the most important regulations issued by central banks that should be strictly followed and implemented within financial institutions.

The Palestine Monetary Authority which acts as the central bank of Palestine, recently issued strict cybersecurity regulations named (PMA CyberSecurity Framework) [105]. The issued regulations paid intense attention to the governance of cybersecurity, as well as cybersecurity incidents management and cyber threat detection. These regulations, as well as regulations implementation approaches, form the cornerstone for the implementation and deployment of the proposed framework within the Palestinian financial sector, and in alignment with current cybersecurity regulations.

To achieve proper deployment and implementation of the proposed framework within the Palestinian financial sector, the framework's pillars and its enablers should be mapped to the corresponding regulatory element within PMA cybersecurity regulations. This mapping ensures both proper implementations of the proposed framework, as well as proper compliance with PMA-issued regulations.

Table bellow illustrates The result of the mapping process between framework items and corresponding control articles within PMA regulations, In addition, table present the suggested approach to framework items and comply with regulations.

Table 6.3: Framework Implementation Within the Palestinian Financial Sector

Framework Pillars	Framework's Pillars Enablers	Related PMA CSF Controls [105]	Implementation Activities by Palestinian Financial Institutions
Governance	G1. Strategy	Appendix Article 1 Controls (1 – 4, 1.1)	FI should develop a (3-5) year strategic plan and plan execution roadmap to achieve framework objectives.
	G2. Policy and procedure	Appendix Article 1 Controls (2, 1.3)	FI should develop a Policy and procedure to guide the execution process of framework objectives and processes.
	G3. Culture	Article 2 Controls (2, Appendix 1.2.1, 1.2.5)	FI should Create a culture of awareness regarding the responsibility to maintain security and forensics practices.
	G4. Top management support	Appendix Article 1 Controls (3, Appendix 1.2.5)	FI should acquire management active involvement and support in managing and coordinating the forensics process.
	G.5 Risk assessment	Article 2 Controls (1 – 2, Appendix 1.5)	FI should Identify assets and their value to the business and should Identify and analyze risk to identified assets.
	G.6 Legal requirement	Appendix Article 2 Controls (2.1.6, 2.16.13, 4.2.2)	Fi should Identify and log external central bank and industry standards compliance requirements.
People	P1. Non-technical stakeholders	Appendix Article 1 Controls (1)	FI should Identify and Involve business stakeholders and their responsibility regarding the cyber and forensics process.
	P2. Technical stakeholders	Article 2 Controls (1 - 2)	FI should Form the appropriate team to carry on the forensics process and maintain team skills and competencies.
	P3. Training	Article 2 Controls (1 – 2, Appendix 1.2.6)	FI should Develop plans, to identify and address gaps in skills in cyber and

			forensics knowledge at the individual level
Infrastructure	I1. Technology	Appendix Article 2 Controls (2.2, 2.3, 2.5, 2.6)	FI should Acquire and deploy cyber and forensics-related solutions (SIEM, PAM, DR, IDS, IPS, FIM, and DLP)
	I2. System architecture	Appendix Article 2 Controls (2.13)	FI Should Enable all logging features within all layers of the system and database environment to be monitored.
Monitoring	M1. System monitoring - preparation	Article 3	FI should Identify a list of critical assets that need to be monitored and Identify log sources and events indicators.
	M2. System monitoring - detection	Article 3 Controls (1, Appendix 2.6)	FI should establish strict processes to detect, monitor, and control critical assets' potential cybersecurity events.
	M3. System monitoring - analysis	Article 3 Controls (2 - 4)	FI should classify and analyze detected events to understand the nature of the event and to assess potential damage to and theft of resources
	M4. System monitoring - forensics	Article 3 Controls (7)	FI should Investigate events and trace back evidence to identify initiation scenarios and root causes.
	M5. System monitoring - contained	Article 4	FI should follow a containment strategy based on incident type to mitigate incidents and isolate affected hosts.
	M6. Forensic preparation	Article 1 Controls (1 - 2)	FI should Continuously monitor evaluate, and enhance the monitoring, detection, and forensics process.
Reporting	R1. Reporting	Article 4	FI should report on incidents and Document root causes and lessons learned to enhance the detection process.

6.6 Chapter Conclusions and Summary

This chapter presented and discussed a summary of the research and thesis results.

The next chapter (chapter 7), presents the conclusions, research community contribution, and recommendations of the research. It clarifies the researcher's contributions and suggestions to further future research.

Chapter 7

7. Conclusions and Future Work

7.1 Introduction

This chapter presents the conclusions, research community contribution, and recommendations of the research. It clarifies the researcher's contributions and suggestions to further future research.

7.2 Conclusions

This dissertation focuses on developing a digital forensic framework used in the early detection and response to insider cybersecurity incidents, specifically within the financial sector. The study was conducted by examining a limited number of the generic digital forensic and incidents response frameworks and process models encountered in the current literature, as well as by exploring current and implemented cybersecurity practices and forensics investigation deployed processes within the financial sector.

The study was motivated by the problem of the accelerated growth and sophisticated techniques used to commit cyber-attacks by organizations' insider perpetrators in financial services firms, as well as the current lack of comprehensive forensics and investigations framework that financial services firms can employ for detection and response to internal cybersecurity incidents.

While the primary objective of this dissertation was to investigate existing digital forensic and incidents response frameworks within the known published literature, as well as explore the current state of cyber security and forensics professional practices within the financial sector to develop an integrated single digital forensic process model valid and relevance for the use of financial sector. The resulting framework met the research objectives, solved the identified problem statement, and answered the research questions.

The resulting framework is supported by five essential pillar requirements and consists of (14) sub-requirements (pillars enablers) and (134) processes and a to-do- list. The resulting framework was validated, tested, and found effective and efficient for early detection and response to insider cybersecurity incidents within the financial sector, and effectively able to aid an investigator in the process of early detection and response to insider threats in real-time or near-to-real time and mitigates the risk of insider threat activities.

7.3 Main Research Contribution

The main research contribution of this dissertation is the development of an integrated digital forensic process model that serves as an insider threats incidents management program and security incidents early warning model within the critical financial digital environment. The developed model has made the following contributions:

- Provide the organization's cyber security professionals, forensics investigators, and incident response and handling personnel, with a state-of-the-art digital forensics framework and process model to assist them during the cyber investigation process followed by internal cyber incidents.

- Provide financial organizations with well designed, mature, and a state of art digital forensics and incident response capability model, to ensure the financial sector organization's readiness for early detection and effective responses to internal cybersecurity incidents, as well as reduce and mitigate the potential impact and consequences of incidents in real-time.
- Identified and bridged gaps of knowledge in the literature on the area of digital forensics frameworks for the financial sector, and how to develop integrated digital forensics and incident handling frameworks for the use of the financial sector.

7.4 Future Work

Further work on this research is necessary to extend the scope of testing of the proposed framework with more real case testing scenarios. Furthermore, potential research and future work would be to aim at creating a universally approved standard, for the development of digital forensics frameworks valid and relevant for the use of the financial sector; and to examine the possibility of developing baseline essential requirements for such developed frameworks as the technical qualifications of digital forensics and incidents response professionals.

7.5 Chapter Conclusions and Summary

This chapter presented the conclusions, research community contribution, and recommendations of the research. It clarified the researcher's contributions and suggestions to further future research.

References

[1] K. Kent, S. Chevalier, T. Grance, and H. Dang, *"Guide to Integrating Forensic Techniques into Incident Response,"* 800th–86th ed. Gaithersburg: The National Institute of Standards and Technology, 2006.

[2] Nickson M. Karie, "Taxonomy of Challenges For Digital Forensics," *J. Forensic Sci.*, vol. 60, no. 4, pp. 885–893, 2015, doi: 10.1111/1556-4029.12809.

[3] D. P. Joseph and J. Norman, "An Analysis of Digital Forensics in Cyber Security," in *Bapi, First International Conference on Artificial Intelligence and Cognitive Computing*, 2019, pp. 701–708, doi: 10.1007/978-981-13-1580-0.

[4] Ponemon Institute, "2022 Cost of Insider Threats Global Report," 2022. [Online]. Available: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-uk-tr-the-cost-of-insider-threats-ponemon-report.pdf.

[5] Charles Cresson Wood, "Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature," *Comput. Fraud Secur.*, vol. 2004, no. 1, pp. 16–17, 2004, doi: 10.1016/j.cose.2014.11.006.

[6] C. P. Grobler, C. P. Louwrens, and S. H. Von Solms, "A framework to guide the implementation of Proactive Digital Forensics in organizations," in *2010 International Conference on Availability, Reliability, and Security. Krakow, Poland*, 2010, pp. 677–682, doi: 10.1109/ARES.2010.62.

[7] S. Varga, J. Brynielsson, and U. Franke, "Cyber-threat perception and risk management in the Swedish financial sector," *Comput. Secur.*, vol. 105, no. 102239, pp. 1–18, 2021, doi: 10.1016/j.cose.2021.102239.

[8] A. Panou, C. Ntantogian, and C. Xenakis, "RiSKi: A framework for modeling cyber threats to estimate risk for data breach insurance," in *Proceedings of the 21st Pan-Hellenic Conference on Informatics*, 2017, vol. Part F1325, pp. 1–6, doi: 10.1145/3139367.3139426.

[9] B. Dupont, "The cyber-resilience of financial institutions: Significance and applicability," *J. Cybersecurity*, vol. 5, no. 1, pp. 1–17, 2019, doi: 10.1093/cybsec/tyz013.

[10] William A. Carter, "Forces Shaping the Cyber Threat Landscape for Financial Institutions," *SSRN*, vol. 4, no. 2016–004, pp. 1–40, 2017.

[11] B. Paper, "Financing Global Development : The Role of Central Banks," *SSRN*, vol. 8, no. 8/2015, pp. 1–4, 2016.

[12] F. C. Freiling and B. Schwittay, "A Common Process Model for Incident Response and Computer Forensics," in *IMF 3rd International Conference on IT-Incident Management & IT-Forensics. Stuttgart, Germany*, 2007, vol. 7, no. 2007, pp. 19–40.

[13] Security Standards Council, *Payment Card Industry Data Security Standard*, 4.0., no. 4. London: Security Standards Council, 2022.

[14] J. M. Adrian Nish, Saher Naumaan, *Enduring Cyber Threats and Emerging Challenges to the Financial Sector*, 8th ed., no. 8. Washington, DC: Carnegie Endowment for International Peace, 2020.

[15] Amazon. WS, *SWIFT Customer Security Controls Framework*, 2022nd ed. Seattle: Amazon, 2022.

[16] S. S. Vitvitskiy, O. N. Kurakin, P. S. Pokataev, O. M. Skriabin, and D. B. Sanakoiev,

"Peculiarities of cybercrime investigation in the banking sector of Ukraine: Review and analysis," *Banks Bank Syst.*, vol. 16, no. 1, pp. 69–80, 2021, doi: 10.21511/bbs.16(1).2021.07.

[17] V. Ravi, "Big Data Analytics Enabled Smart Financial Services : Opportunities and Challenges," in *Proceedings of the 10th International Conference on Molten Slags, Fluxes, and Salts*, 2016, vol. 1, pp. 15–39, doi: 10.1007/978-3-319-72413-3.

[18] B. Nikkel, "Fintech forensics: Criminal investigation and digital evidence in financial technologies," *Forensic Sci. Int. Digit. Investig.*, vol. 33, no. 14, pp. 55–73, 2020, doi: 10.1016/j.fsidi.2020.200908.

[19] A. A. G. and A. Musa, "A Recommended Digital Forensic Readiness Framework for Nigerian Banks," *Int. J. Dev. Res.*, vol. 09, no. 08, pp. 28920–28928, 2019.

[20] S. Dzomira, "Digital Forensic Technologies as e-fraud Risk Mitigation Tools in the Banking Industry: Evidence from Zimbabwe," *Risk Gov. Control Financ. Mark. Institutions*, vol. 4, no. 2, pp. 116–124, 2014, doi: 10.22495/rgcv4i2c1art4.

[21] A. C. Kim, S. Kim, W. H. Park, and D. H. Lee, "Fraud and Financial Crime Detection Model Using Malware Forensics," *Multimed. Tools Appl.*, vol. 68, no. 2, pp. 479–496, 2014, doi: 10.1007/s11042-013-1410-3.

[22] R. Syed *et al.*, "Computers in Industry Robotic Process Automation : Contemporary themes and challenges," *Comput. Ind.*, vol. 115, no. 1, p. 103162, 2020, doi: 10.1016/j.compind.2019.103162.

[23] D R Aryawibawa and D A W Syaroni, "Information System Components for Designing Financial Applications in Small and Medium Enterprises," *Int. J. Educ. Inf. Technol. Others*, vol. 3, no. 2, pp. 286–291, 2020, doi: 10.5281/zenodo.3975527.

[24] I. Agur, S. M. Peria, and C. Rochon, *Digital Financial Services and the Pandemic : Opportunities and Risks for Emerging and Developing Economies*, 1st ed. Washington, D.C: The International Monetary Fund Research Center, 2020.

[25] A. Ismail and S. Abdulrahman, "The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector," *J. Xidian Univ.*, vol. 14, no. 7, pp. 1523–1536, 2020.

[26] C. Calliess and A. Baumgarten, "Cybersecurity in the EU The Example of the Financial Sector : A Legal Perspective," *Ger. Law J.*, vol. 21, no. 6, pp. 1149–1179, 2020, doi 10.1017/glj.2020.67.

[27] Y. Ding and Z. Wu, "Research and Application of Security Baseline in Business Information System," *Procedia Comput. Sci.*, vol. 183, no. 2021, pp. 630–635, 2021, doi: 10.1016/j.procs.2021.02.107.

[28] C. Onwubiko, "Cyber Security Operations Centre Security Monitoring for protecting Business and supporting Cyber Defense Strategy," in *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). London, UK*, 2015, pp. 1–10.

[29] K. Dempsey, K. Dempsey, C. Baer, and R. Niemeyer, *Assessing Information Security Continuous Monitoring (ISCM) Programs : Developing an ISCM Program Assessment*, 800th–137A ed. Wilbur: National Institute of Standards and Technology, 2020.

[30] A. Madani, S. Rezayi, and H. Gharaee, "Log Management comprehensive architecture in Security Operation Center (SOC)," in *2011 International Conference on Computational Aspects of Social Networks (CASoN). Salamanca, Spain.*, 2011, pp. 284–

289.
[31] K. Kent and M. Souppaya, *Guide to Computer Security Log Management*, 800th–92nd ed. Gaithersburg: National Institute of Standards and Technology, 2006.
[32] J. T. Force, *Security and Privacy Controls for Information Systems and Organizations Security and Privacy Controls for Information Systems and Organizations*, 800th–53rd ed. Gaithersburg: National Institute of Standards and Technology, 2017.
[33] M. Spremić and A. Šimunic, "Cyber security challenges in digital economy," in *Proceedings of the World Congress on Engineering. London, U.K.*, 2018, vol. 1, pp. 2–7.
[34] Palmer G. A, "A Road Map for Digital Forensic Research," in *First Digital Forensic Research Workshop Conference. Utica, New York*, 2001, pp. 27–30.
[35] K. Kyei, P. Zavarsky, D. Lindskog, and R. Ruhl, "A Review and Comparative Study of Digital Forensic Investigation Models," in *Digital Forensics and Cyber Crime: 4th International Conference. Berlin, Heidelberg*, 2013, vol. 114, pp. 314–327, doi: 10.1007/978-3-642-39891-9_20.
[36] Reith, C. Carr, and G. Gregg, "An Examination of Digital Forensic Models by Mark Reith," *Int. J. Digit. Evid. Fall*, vol. 1, no. 3, pp. 1–12, 2002, [Online]. Available: www.ijde.org.
[37] B. Carrier and E. H. Spafford, "Getting physical with the digital investigation process," *Int. J. Digit. Evid.*, vol. 2, no. 2, pp. 1–20, 2003, doi: 10.1.1.156.9541.
[38] V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process Model," in *Proceedings of the Digital Forensic Research Conference, DFRWS. Baltimore, USA.*, 2004, pp. 1–9.
[39] S. Ciardhuáin, "An extended model of cybercrime investigations," *Int. J. Digit. Evid.*, vol. 3, no. 1, pp. 1–22, 2004.
[40] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model," *Int. J. Comput. Sci. Secur.*, vol. 5, no. 1, pp. 118–131, 2011.
[41] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information Security Incident Management: Current Practice as Reported in the Literature," *Comput. Secur.*, vol. 45, no. 2014, pp. 42–57, 2014, doi: 10.1016/j.cose.2014.05.003.
[42] N. Sun, J. Zhang, P. Rimba, S. Gao, L. Y. Zhang, and Y. Xiang, "Data-Driven Cybersecurity Incident Prediction: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1744–1772, 2019, doi: 10.1109/COMST.2018.2885561.
[43] F. E. Catota, M. Granger Morgan, and D. C. Sicker, "Cybersecurity incident response capabilities in the Ecuadorian financial sector," *J. Cybersecurity*, vol. 4, no. 1, pp. 1–20, 2018, doi: 10.1093/cybsec/tyy002.
[44] G. Killcrece, *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*, 2003rd–001 ed. Pittsburgh: Carnegie Mellon Software Engineering Institute State, 2003.
[45] M. A. Kuypers, T. Maillart, and E. Paté-Cornell, "An Empirical Analysis of Cyber Security Incidents at a Large Organization," 2016. [Online]. Available: https://fsi.stanford.edu/sites/default/files/kuypersweis_v7.pdf.
[46] H. Naseer, S. B. Maynard, and K. C. Desouza, "Demystifying analytical information processing capability: The case of cybersecurity incident response," *Decis. Support Syst.*, vol. 143, no. 2021, p. 113476, 2021, doi: 10.1016/j.dss.2020.113476.

[47] M. Kjaerland, “A Classification of Computer Security Incidents Based on Reported Attack Data,” *J. Investig. Psychol. Offender Profiling*, vol. 2, no. 2, pp. 105–120, 2005.
[48] M. Jouini, L. B. A. Rabai, and A. Ben Aissa, “Classification of security threats in information systems,” *Procedia Comput. Sci.*, vol. 32, no. 1, pp. 489–496, 2014, doi: 10.1016/j.procs.2014.05.452.
[49] S. Hettiarachchi and S. Wickramasinghe, “Study to identify threats to Information Systems in Organizations and possible countermeasures through policy decisions and awareness programs to ensure the information security.,” *Inf. Secur. Methods-Modern Res. Dir.*, vol. 11, no. 2, pp. 1–13, 2016.
[50] I. Homoliak, F. Toffalini, J. Guarnizo, and Y. Elovici, “Insight Into Insiders and IT : A Survey of Insider Threat Taxonomies , Analysis , Modeling , and Countermeasures,” in *ACM Computing Surveys*, 2019, vol. 52, no. 2, pp. 1–40.
[51] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, “Analysis of unintentional insider threats deriving from social engineering exploits,” in *2014 IEEE Security and Privacy Workshops. San Jose, CA, USA*, 2014, vol. 2014, pp. 236–250, doi: 10.1109/SPW.2014.39.
[52] J. Eggenschwiler, I. Agrafiotis, and J. R. Nurse, “Insider threat response and recovery strategies in financial services firms,” *Comput. Fraud Secur.*, vol. 2016, no. 11, pp. 12–19, 2016, doi: 10.1016/S1361-3723(16)30091-4.
[53] K. Roy Sarkar, “Assessing insider threats to information security using technical, behavioural and organisational measures,” *Inf. Secur. Tech. Rep.*, vol. 15, no. 3, pp. 112–133, 2010, doi: 10.1016/j.istr.2010.11.002.
[54] Verizon Business, “Verizon: Data Breach Investigations Report (2008 - 2022),” *Comput. Fraud Secur.*, vol. 6, no. 2022, pp. 1–108, 2022.
[55] Software Engineering Institute Carnegie University, *Common Sense Guide to Mitigating Insider Threats, Fifth Edition*, no. 2016. Hanscom: Software Engineering Institute Carnegie Mellon University, 2016.
[56] M. Ben Salem, S. Hershkop, and S. J. Stolfo, “A Survey of Insider Attack Detection Research,” *Insid. Attack Cyber Security.*, vol. 39, no. 2008, pp. 69–90, 2008, doi: 10.1007/978-0-387-77322-3_5.
[57] K. S. Paul Cichonski, Tom Millar, Tim Grance, *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*, 800th–61st ed. Gaithersburg: The National Institute of Standards and Technology, 2012.
[58] P. Kral, *Incident Handler’s Handbook*, 1st ed. Bethesda: The SANS Institute, 2021.
[59] Iftekhar Ahmed and Tahmin Nahar, “Protection of Sensitive Data in Zero Trust Model,” in *Proceedings of the International Conference on Computing Advancements. New York, USA.*, 2020, pp. 1–5.
[60] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, “Review Article A Survey on Zero Trust Architecture : Challenges and Future Trends,” *Wirel. Commun. Mob. Comput. J.*, vol. 2022, no. 1, pp. 1–13, 2022.
[61] C. Cordeiro and H. Barbosa, “Digital Privacy and Security,” in *Proceedings of the Digital Privacy and Security Conference. Porto, Portugal*, 2019, no. January, pp. 1–69.
[62] C. S. Rose S, Borchert O, Mitchell S, *Zero Trust Architecture*, 800th–207th ed. Gaithersburg: National Institute of Standards and Technology, 2020.
[63] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, “Never trust, always

verify: A multivocal literature review on current knowledge and research gaps of zero-trust," *Int. J. Comput. Sci. Netw. Secur.*, vol. 8, no. 10, p. 102436, 2008, doi: 10.1016/j.cose.2021.102436.

[64] J. Flanigan, "Zero Trust Network Model," Medford, USA, 1, 2018. [Online]. Available: https://www.cs.tufts.edu/comp/116/archive/fall2018/jflanigan.pdf.

[65] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping Process of Digital Forensic Investigation Framework," *Int. J. Comput. Sci. Netw. Secur.*, vol. 8, no. 10, pp. 163–169, 2008.

[66] A. Al-Dhaqm, S. A. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, "Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field," *IEEE Access*, vol. 8, no. 4, pp. 145018–145032, 2020, doi: 10.1109/ACCESS.2020.3008696.

[67] R. Montasari, R. Hill, V. Carpenter, and A. Hosseinian-Far, "The standardised digital forensic investigation process model (SDFIPM)," *Blockchain Clin. Trial*, vol. 1, no. 1, pp. 169–209, 2019, doi 10.1007/978-3-030-11289-9_8.

[68] K. S. Singh, A. Irfan, and N. Dayal, "Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks," in *2019 4th International Conference on Information Systems and Computer Networks (ISCON). Mathura, India*, 2019, pp. 584–590, doi: 10.1109/ISCON47742.2019.9036214.

[69] M. E. Alex and R. Kishore, "Forensics framework for cloud computing," *Comput. Electr. Eng.*, vol. 60, no. 1, pp. 193–205, 2017, doi: 10.1016/j.compeleceng.2017.02.006.

[70] D. M. Divakaran, K. W. Fok, I. Nevat, and V. L. L. Thing, "Evidence gathering for network security and forensics," in *DFRWS 2017 Europe — Proceedings of the Fourth Annual DFRWS Europe. Lake Constance, Germany*, 2017, vol. 20, pp. S56–S65, doi: 10.1016/j.diin.2017.02.001.

[71] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). Vienna, Austria*, 2016, pp. 356–362, doi: 10.1109/FiCloud.2016.57.

[72] B. J. Nikkel, "Fostering incident response and digital forensics research," *Digit. Investig.*, vol. 11, no. 4, pp. 249–251, 2014, doi: 10.1016/j.diin.2014.09.004.

[73] A. Patrascu and V. V. Patriciu, "Beyond digital forensics. A cloud computing perspective over incident response and reporting," in *2013 IEEE 8th International Symposium on Applied Computational Intelligence and Informatics (SACI). Timisoara, Romania*, 2013, pp. 455–460, doi: 10.1109/SACI.2013.6609018.

[74] M. I. Cohen, D. Bilby, and G. Caronni, "Distributed forensics and incident response in the enterprise," *Digit. Investig.*, vol. 8, no. 2, pp. S101–S110, 2011, doi: 10.1016/j.diin.2011.05.012.

[75] D. Trček, H. Abie, Å. Skomedal, and I. Starc, "Advanced framework for digital forensic technologies and procedures," *J. Forensic Sci.*, vol. 55, no. 6, pp. 1471–1480, 2010, doi: 10.1111/j.1556-4029.2010.01528.x.

[76] P. Turner, "Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags," *Digit. Investig.*, vol. 4, no. 1, pp. 30–35, 2007, doi: 10.1016/j.diin.2007.01.002.

[77] B. Carrier and E. Spafford, “An Event-Based Digital Forensic Investigation Framework,” in *Proceedings of The Digital Forensic Research Conference DFRWS 2004. Baltimore, USA .*, 2004, pp. 1–12.
[78] W. J. Orlikowski and J. J. Baroudi, “Studying Information Technology in Organizations : Research Approaches and Assumptions,” *Inf. Syst. Res.*, vol. 2, no. 1, pp. 1–29, 1991.
[79] W. D. Fernández, “The grounded theory method and case study data in IS research: issues and design,” *Inf. Syst. Found. Work. Constr. Crit.*, vol. 1, no. 22, pp. 43–59, 2004.
[80] S. E. Glaser BG, Strauss AL, “The Discovery of Grounded Theory; Strategies for Qualitative Research,” *Nurs. Res.*, vol. 17, no. 4, p. 364, 1968.
[81] Charmaz K., *Constructing grounded theory: A practical guide through qualitative analysis*, 1st ed. London, U.K.: SAGE Publications, 2006.
[82] M. J. Birks M, *Grounded theory: A practical guide*, 3rd ed. London, U.K: SAGE Publications, 2011.
[83] M. R. Oates BJ, Griffiths M, *Researching Information Systems and Computing*, 2nd ed. London, U.K: SAGE Publications, 2022.
[84] G. H. Carlton, “A protocol for the forensic data acquisition of personal computer workstations,” University of Hawai’i, 2006.
[85] W. B. Isaac, S. & Michael, *Handbook in research and evaluation: A collection of principles, methods, and strategies useful in the planning, design, and evaluation of studies in education and the behavioral sciences*, 3rd ed. Washington, D.C: EdITS Publishers, 1995.
[86] Wilkinson, *Focus group research. Qualitative research: Theory, method, and practice*, 2nd ed. London, U.K: PsycINFO Database Record, 2004.
[87] A. J. Onwuegbuzie, “A Qualitative Framework for Collecting and Analyzing Data in Focus Group Research,” *Int. J. Qual. methods*, vol. 8, no. 3, pp. 1–21, 2009.
[88] T. O. Nyumba, K. Wilson, C. J. Derrick, and N. Mukherjee, “The use of focus group discussion methodology : Insights from two decades of application in conservation,” *Methods Ecol. Evol.*, vol. 9, no. 1, pp. 20–32, 2018, doi: 10.1111/2041-210X.12860.
[89] IBIS World, “Global Commercial Banks - Number of Businesses 2005–2028,” *2023*, 2023. https://www.ibisworld.com/global/number-of-businesses/global-commercial-banks/1750/#:~:text=There are 10%2C334 Global Commercial,over the past 5 years%3F (accessed May 10, 2023).
[90] Merchant Costconsulting, “List of Credit Card Processing Companies 2023,” *2023*, 2023. https://merchantcostconsulting.com/lower-credit-card-processing-fees/list-of-credit-card-processing-companies-2023/ (accessed May 15, 2023).
[91] Y. Hoskote, T. Kam, P. H. Ho, and X. Zhao, “Coverage estimation for symbolic model checking,” in *Proceedings of the 36th annual ACM/IEEE Design Automation Conference. New Orleans Louisiana, USA.*, 1999, pp. 300–305, doi: 10.1145/309847.309936.
[92] N. M. Zainudin, N. A. Hasbullah, M. Wook, and S. Ramli, “Digital Forensic Readiness for Cyber Security Practitioners : An Integrated Model,” *J. Posit. Sch. Psychol.*, vol. 6, no. 3, pp. 8423–8433, 2022.
[93] M. Elyas *et al.*, “Towards A Systemic Framework for Digital Forensic Readiness,” *J. Comput. Inf. Syst.*, vol. 54, no. 3, pp. 87–105, 2016, doi:

10.1080/08874417.2014.11645708.
[94] S. M. Garba AA, “A Holistic–Based Digital Forensic Readiness Framework For Zenith Bank, Nigeria,” in *ICCSS 2015 - Proceedings: 2015 International Conference on Informative and Cybernetics for Computational Social Systems. Mardan, Pakistan.*, 2015, no. 2015, pp. 551–560.
[95] ISACA, *Governance and Management Objectives*, 2019th ed. Schaumburg: ISACA Publications, 2019.
[96] I. Corradini, *Building a Cybersecurity Culture in Organizations. How to Bridge the Gap Between People and Digital Technology*. Rome, Italy: Springer Nature Switzerland, 2020.
[97] A. Elbanna, “Top management support in multiple-project environments: An in-practice view,” *Eur. J. Inf. Syst.*, vol. 22, no. 3, pp. 278–294, 2013, doi: 10.1057/ejis.2012.16.
[98] M. I. Štemberger, A. Manfreda, and A. Kovačič, “Achieving top management support with business knowledge and role of IT/IS personnel,” *Int. J. Inf. Manage.*, vol. 31, no. 5, pp. 428–436, 2011, doi: 10.1016/j.ijinfomgt.2011.01.001.
[99] J. Memole-doodson, *Privileged Account Management for the Financial Services Sector*, 1800th–18th ed. McLean, VA: The National Institute of Standards and Technology, 2018.
[100] C. Petrie, Elizabeth, and Evans, “Sharing Insider Threat Indicators: Examining The Potential Use of Swift’s Messaging Platform To Combat Cyber Fraud,” La Hulpe, Belgium, 2016–003, 2017.
[101] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. Shimeall, and L. Flynn, “Common Sense Guide to Mitigating Insider Threats, Sixth Edition,” Carnegie Mellon, DM18-1336, 2018.
[102] M. Kont, M. Pihelgas, J. Wojtkowiak, L. Trinberg, and A.-M. Osula, “Insider threat detection study,” Tallinn, 1, 2015. [Online]. Available: www.ccdcoe.org.
[103] V. Bird *et al.*, “Research Fit for Purpose? Validation of a conceptual framework for personal recovery with current mental health consumers,” *Aust. N. Z. J. Psychiatry*, vol. 48, no. 7, pp. 644–653, 2014, doi: 10.1177/0004867413520046.
[104] J. Cawthra, M. Ekstrom, L. Lusty, J. Sexton, J. Sweetnam, and A. Townsend, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*, 1800th–26th ed. McLean, Virginia: National Institute of Standards and Technology, 2020.
[105] The Palestine Monetary Authority, *PMA CyberSecurity Framework.pdf*, 11th–2022nd ed. Ramallah: PMA, 2022.

Appendix 1: Electronic Survey Sample Distribution List – Email Messages

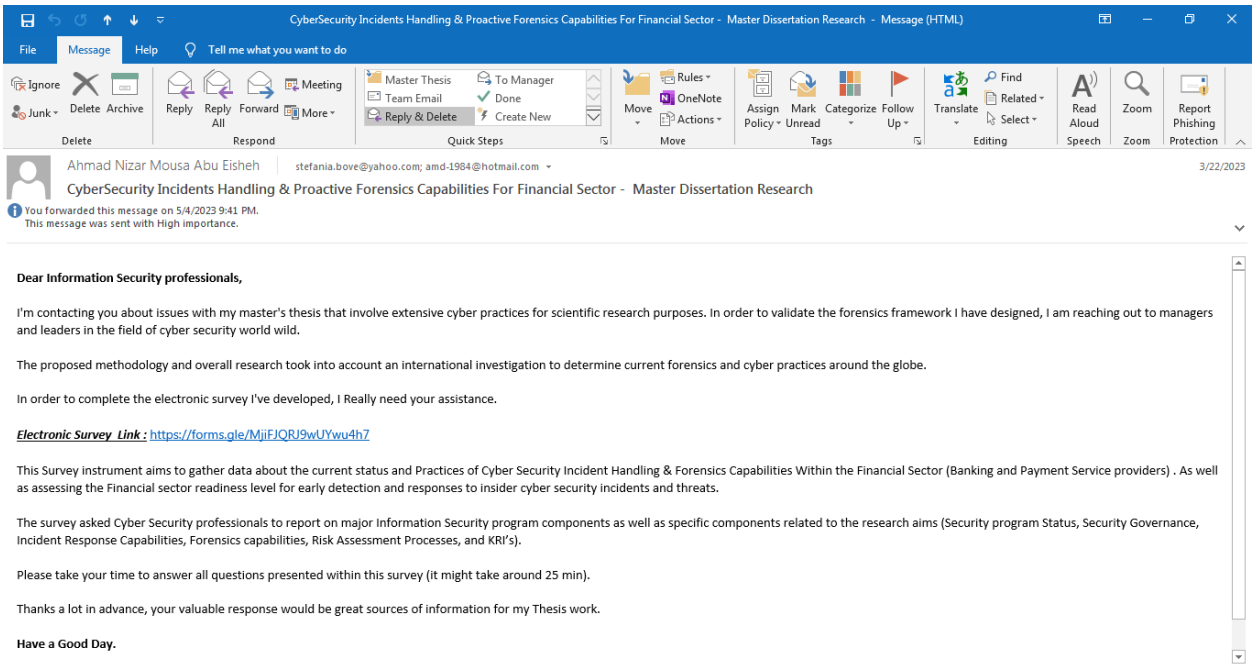


Figure A1.1: Electronic Survey Sample Distribution List – Email Messages – 1.

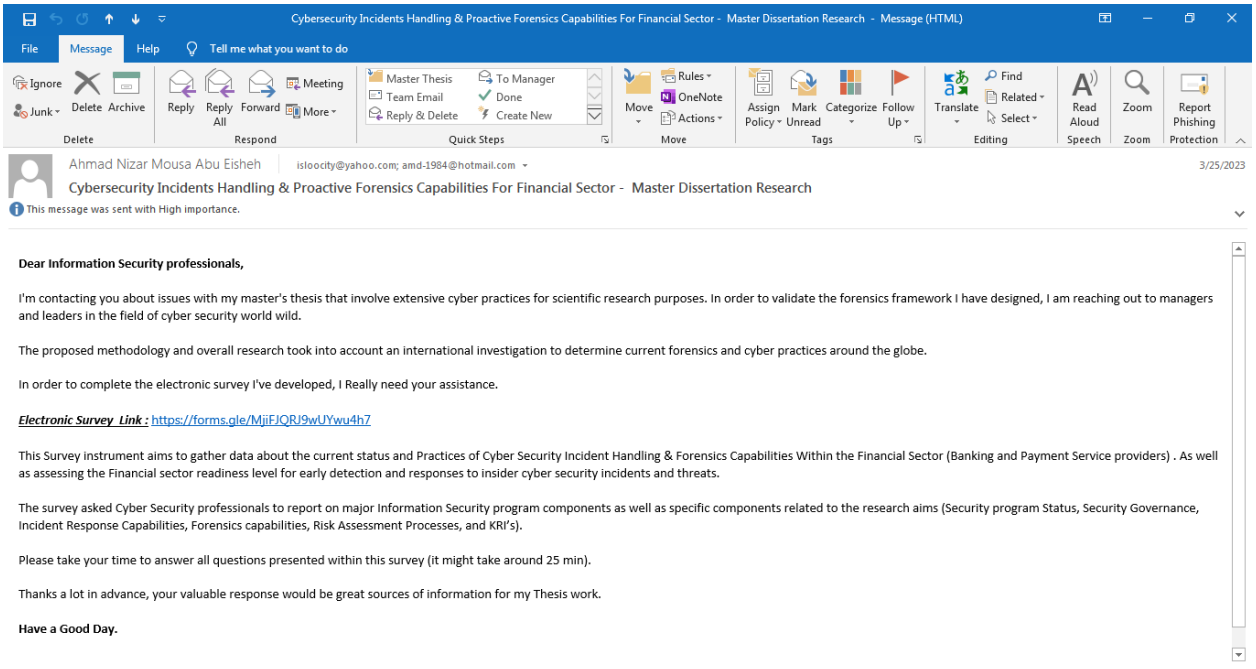


Figure A1.2: Electronic Survey Sample Distribution List – Email Messages – 2.

Appendix 2: Electronic Survey Sample Distribution List – Linkedin Messages

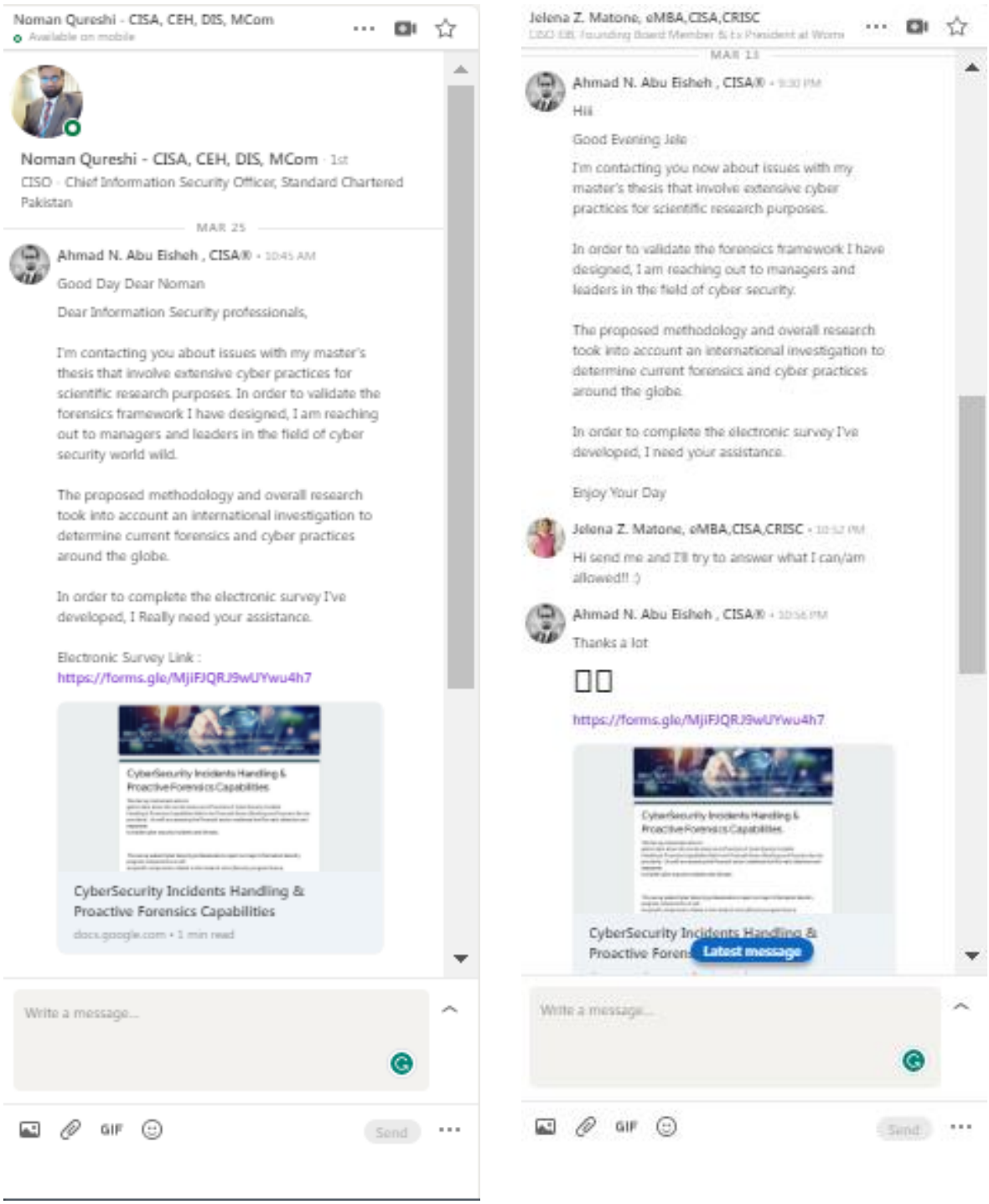
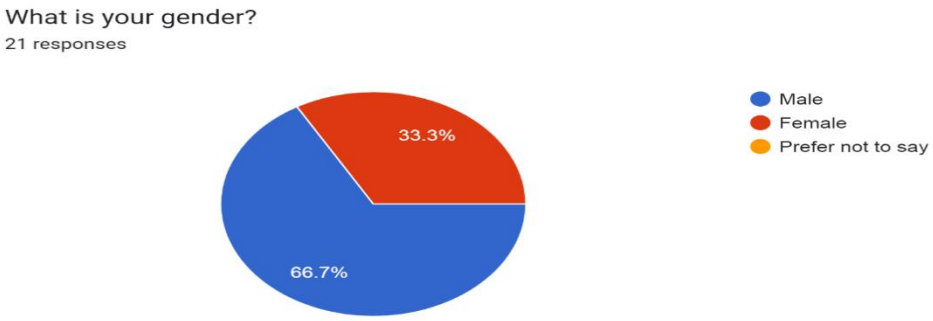


Figure A2.1: Electronic Survey Sample Distribution List – Linkedin Messages.

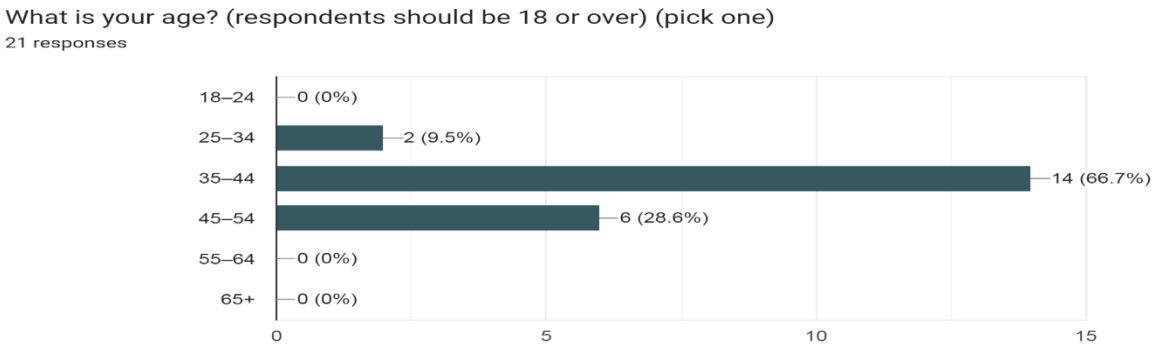
Appendix 3: Electronic Survey Questions and Full Responses Statistics

Demographic Questions Section

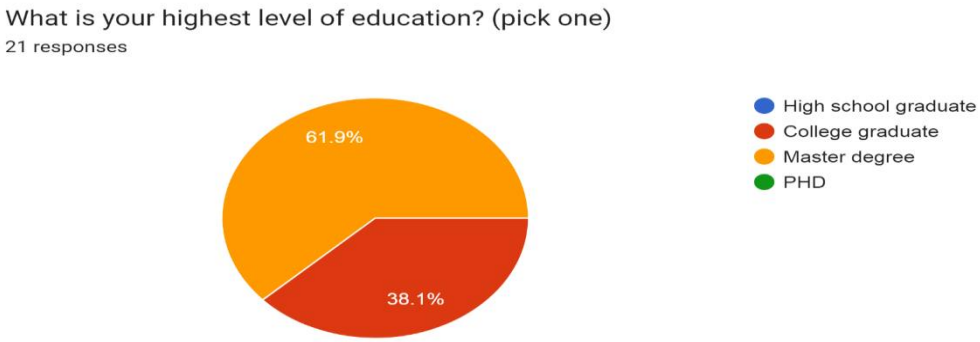
Q1.



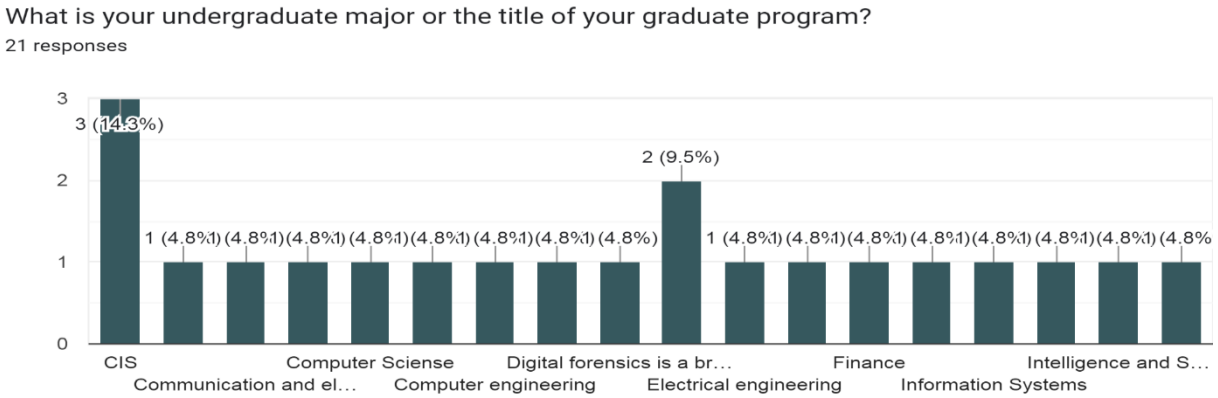
Q2.



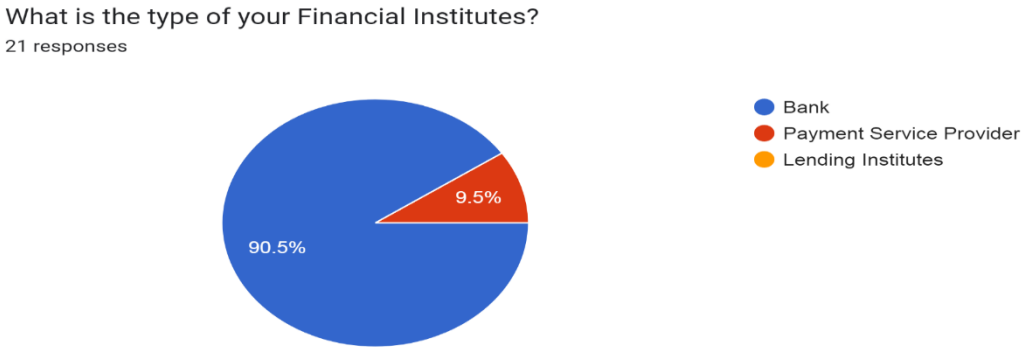
Q3.



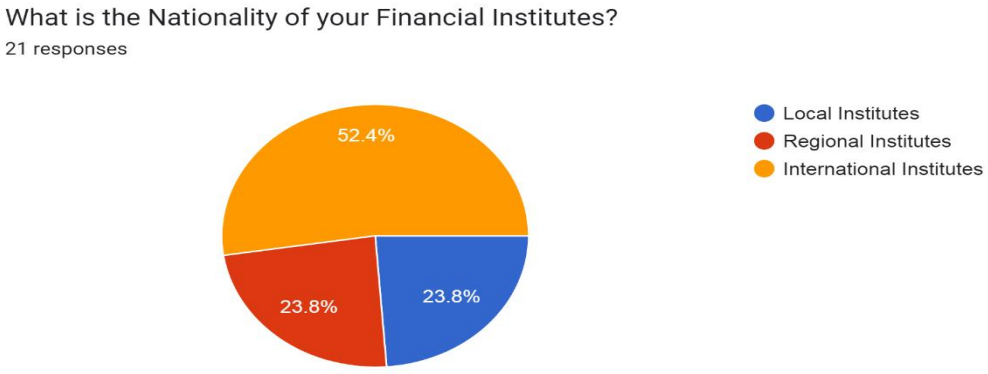
Q4.


What is your undergraduate major or the title of your graduate program?
21 responses
3
2
1
0
3 (14.3%)
1 (4.8%)
2 (9.5%)
CIS
Communication and el...
Computer Sciense
Computer engineering
Digital forensics is a br...
Electrical engineering
Finance
Information Systems
Intelligence and S...

Q5.

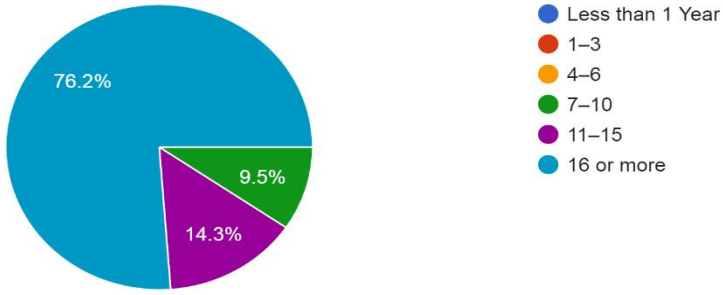

What is the type of your Financial Institutes?
21 responses
9.5%
90.5%
Bank
Payment Service Provider
Lending Institutes

Q6.


What is the Nationality of your Financial Institutes?
21 responses
52.4%
23.8%
23.8%
Local Institutes
Regional Institutes
International Institutes

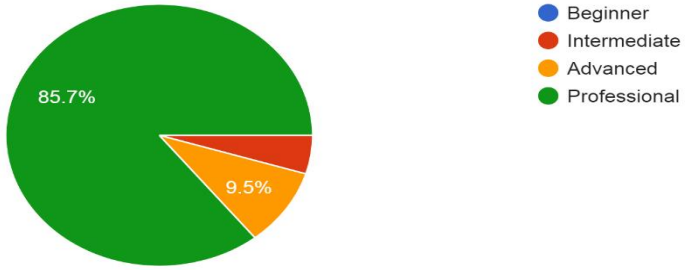
Q7.

How many years of working experience do you have?
21 responses



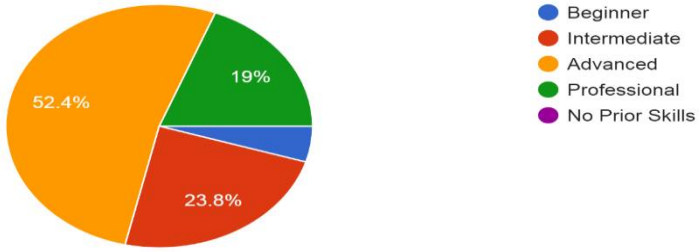
Q8.

How well do you rate your cyber security skills? (pick one)
21 responses



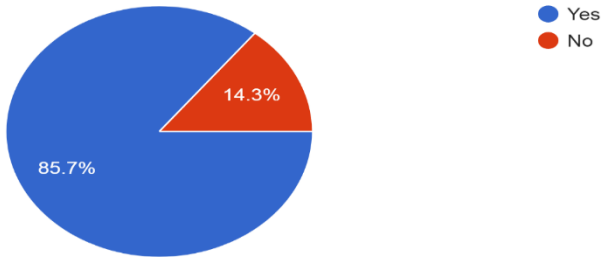
Q9.

How well do you rate your Digital Forensics skills? (pick one)
21 responses



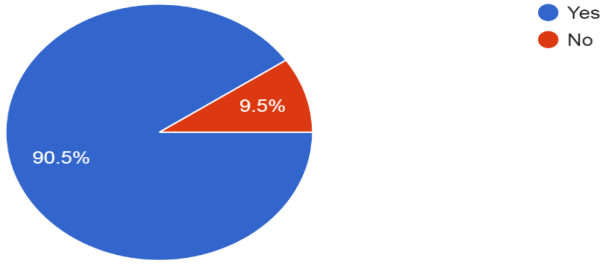
Q10.

Are you directly responsible or a key practitioner in incident response and digital forensics process)
21 responses



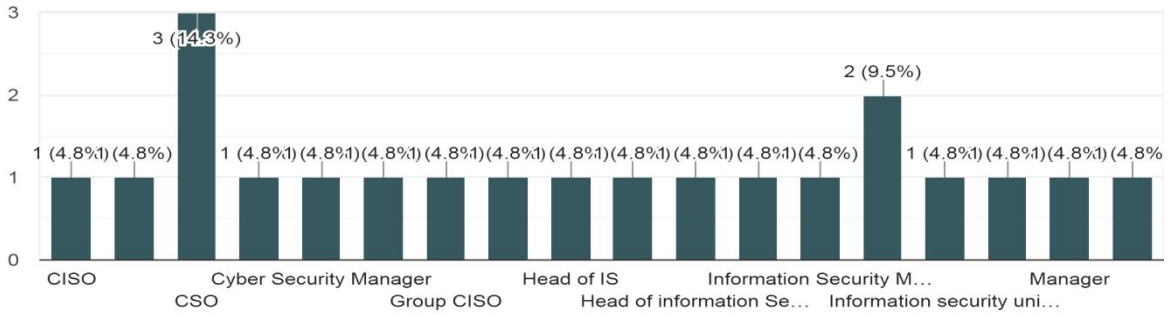
Q11.

Are you a Member of your Organization's cyber security incident response team?
21 responses

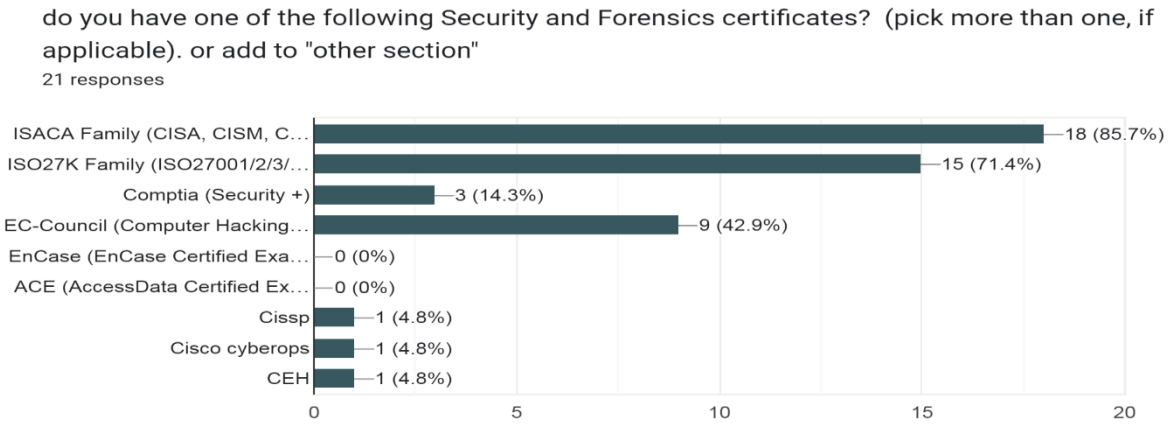


Q12.

What is you Job title
21 responses



Q13.



Q14.

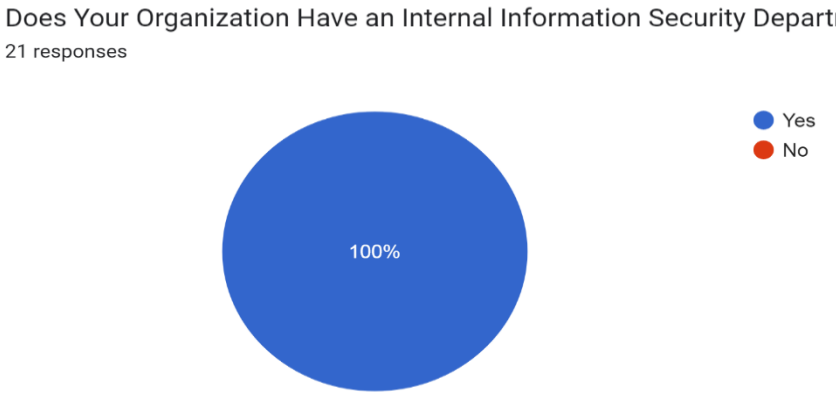
Using your own words, define what digital forensics is.

- The way you investigate logs to learn about incidents
- Mainly collecting the pieces of evidence and identifying the root causes
- The act of harvesting evidence to decide to pursue legal means and root cause analysis to further improve our security posture
- Na
- It is the collection of electronic evidence, preserving it, and analyzing it to investigate cybercrime.
- The science to find out digital evidence in potential legal crimes
- The process of collection, analysis, and presentation of digital evidence to reveal cyber incidents' root causes.
- It is a digital investigation process by
- Extracting digital evidence from the digital medial
- Investigating the digital world to find the root cause of events
- Searching and analyzing evidence in the digital world to identify incident causes
- In my own words, digital forensics is the process of investigation to collect, analyze, and preserve evidence during an investigation of any digital crime. Whereas, as per the book, this process includes analyzing, retrieving, and preserving electronic data that may be useful in an investigation.
- The process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law
- Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting data stored electronically.
- Investigating digital systems to extract proper evidence on incidents

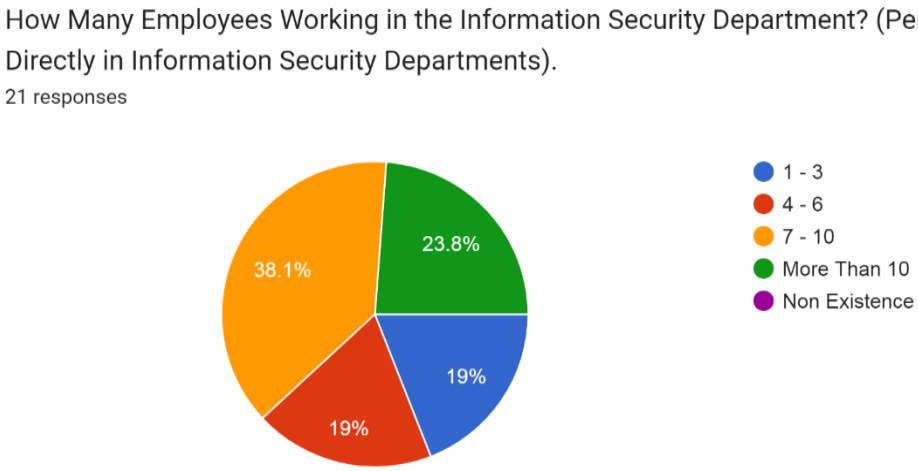
- Digital forensics is the process of storing, analyzing, retrieving, and preserving electronic data that may be useful in an investigation either in case of an incident or analysis of an anomaly inflow of data communication
- The process of identifying the root cause of digital evidence
- By looking inside digital evidence to solve e crimes
- Investigating digital systems to extract evidence
- Analyzing logs and digital evidence to extract the root cause of security incidents

Information Security General Practices

Q15.

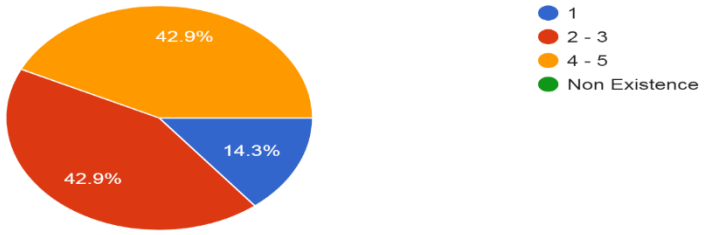


Q16.



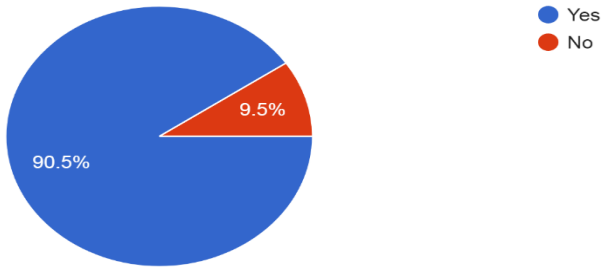
Q17.

How Many Employees Have Specialized Certificates in the Information Security Field?
21 responses



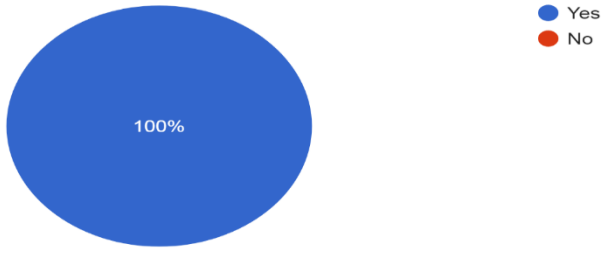
Q18.

Does your organization carry out legal background verification for information security candidates periodically?
21 responses



Q19.

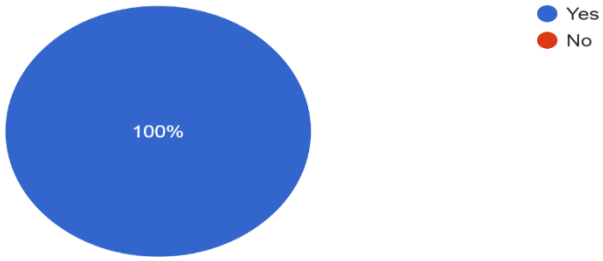
Does your organization develop or support any professional training courses in cyber security for the information security team?
21 responses



Q20.

Is there any dedicated financial budget for the development of information security management systems?

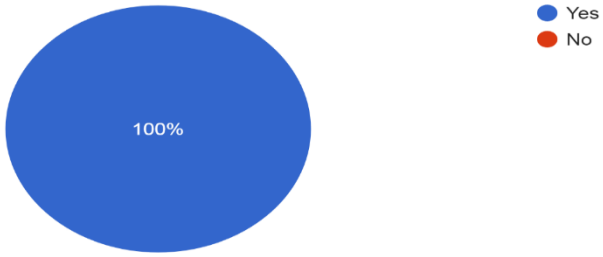
21 responses



Q21.

Does your organization has cyber security policies, procedures, or standards?

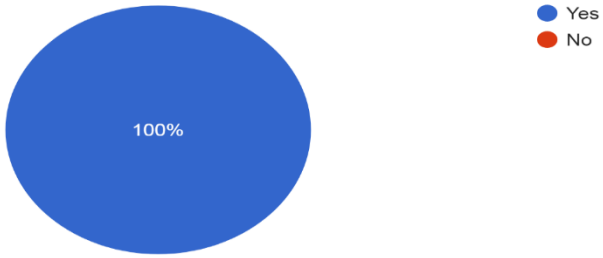
21 responses



Q22.

Does Your Organization Have an Information Security Steering Committee to carry out Information Security program Issues?

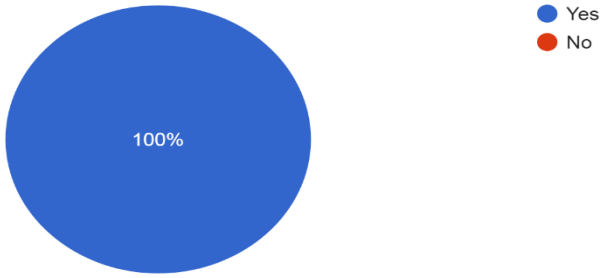
21 responses



Q23.

Does Your Organization Have in Place Process for Conducting Comprehensive Information Security Risk Assessment by Independent Risk Management Function or any other Independent party?

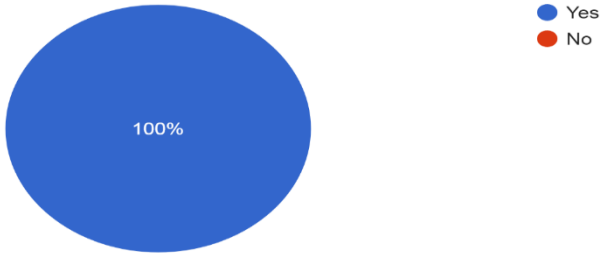
21 responses



Q24.

Does Your Organization Have in Place Process for Information Security Planning? Does it Have an Update Annual Security Plan?

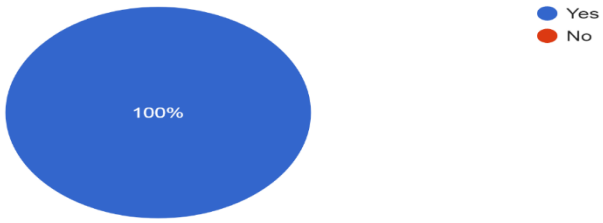
21 responses



Q25.

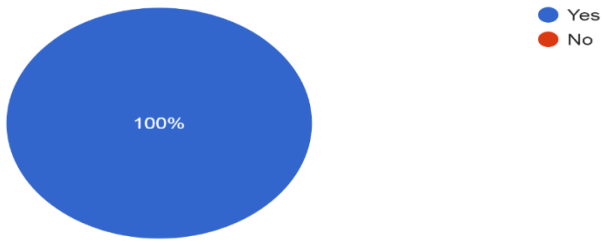
Does Your Organization Have in Place the Information security roles and responsibilities Charter? So that each related party knows about their Security Roles and Responsibilities?

21 responses



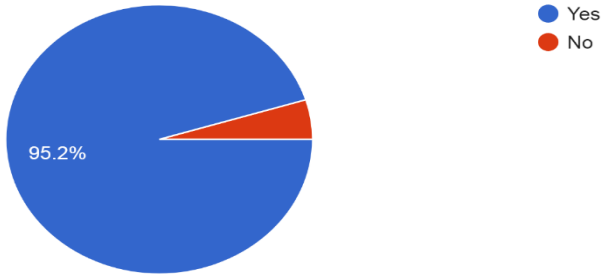
Q26.

Does Your Organization Have in Place Process conducted by security staff for Monitoring System changes? Changes include internal and third-party changes To Information Systems.
21 responses



Q27.

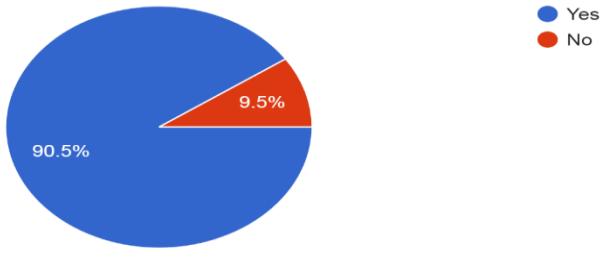
Does Your Organization Have in Place Process for the Enterprise level Security Awareness program?
21 responses



Cyber Security Incidents Response and Handling Capabilities

Q28.

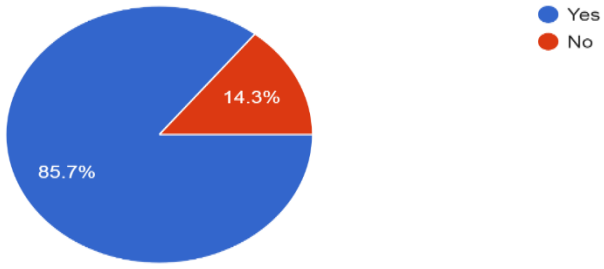
Does Your Organization develop Cyber Incident Response Plan that contains and defines step-by-step guidance for response actions to comm... as well as responses roles and responsibilities.
21 responses



Q29.

Does Your Organization Have trained Staff involved in managing an incident i.e (Cyber Incidents Response Team)

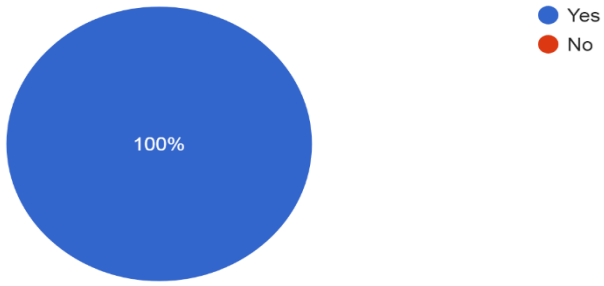
21 responses



Q30.

Does Your Organization have internal or third-party arrangements and capabilities to detect and analyze Cyber Security incidents?

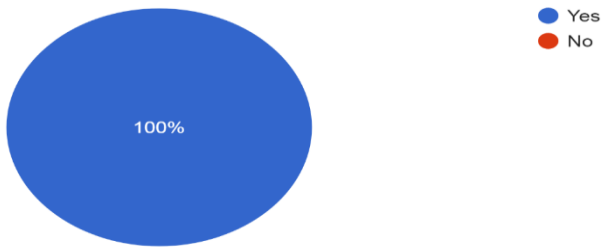
21 responses



Q31.

Does Your Organization has Documented Critical assets inventory (data, applications, and systems)

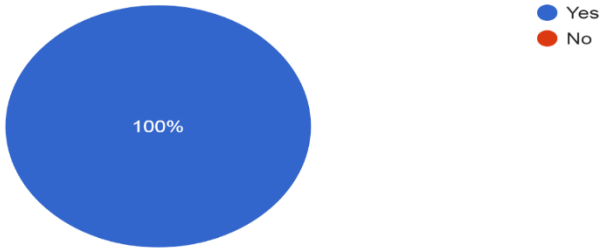
21 responses



Q32.

Does Your Organization have internal or third-party arrangements and capabilities to monitor Internal threats?

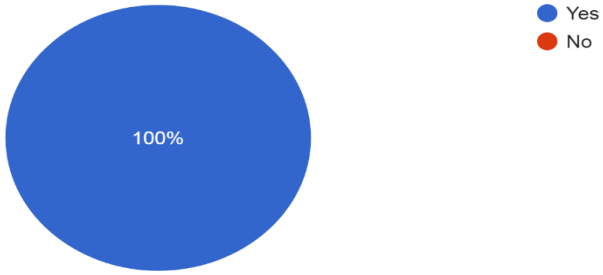
21 responses



Q33.

Does Your Organization have Detection mechanisms that can be used to identify potential information security incidents?

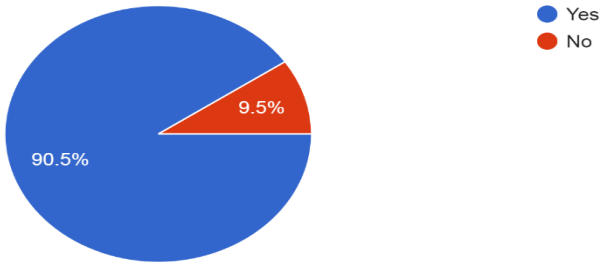
21 responses



Q34.

Does Your Organization establishes a baseline of anomalous activity (IOC, IOA, KRI); which, when combined with logging and alerting mechanisms, can enable the detection of such activity;

21 responses



Q35.

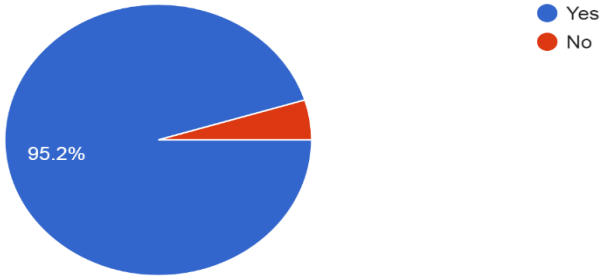
Please list the top 10 (IOC IOA, KRI) that form your organization's baseline regarding pre-defined anomalous activity and insider threat indicators.

- Threats
- Confidential
- Usage patterns and access to sensitive information and functions for users and privileged users
- Na
- Not within my jurisdiction
- Confidential
- The use of highly privileged systems accounts. Database changes to access secretive data copying of data into external storage. Sending email to personal or web-based email. Use of USB storage devices installation of unauthorized software download of software failed login user management activities
- Using privileged accounts in daily operations, abnormal processes or activities detection by EDR, large amounts of files transfer outside the bank, failed access attempts systems or DB's
- Cannot disclose
- The use of high privilege accounts copying large volumes of data add, delete and user changes configuration change. Security changes network access outside working hours any other indicators based on risk assessment results
- Superuser activity data copying user provisioning
- Cannot share
- Baseline
- Excessive firewall denial, scanning, price escalation, multiple logins followed by success, huge outbound traffic, shared accounts, unusual patching, unusual high privilege access, unauthorized access
- Access to sensitive data super user actions use of storage devices copy huge amount of data add user delete user modify user configuration changes un usual logins websites
- IOC, SHA, hash, IPS
- Insider threats indicators like access to systems using privileged accounts, user profile changes, user management, access and transfer of sensitive data
- Use of admin accounts. Copy classified data new user change user delete user's user profile change configuration changes data base changes failed login user behavior
- Admin accounts activities data transfer configuration changes security changes failed login remote access use of mobile codes use of non-original software use of data storage units and sites user provisioning activities
- Priv. Account monitoring, admin access to critical systems, software changes, failed login, account management activities, configuration changes, tele access to systems, new software installation, authorization process, and use of data storage.
- IOC.

Q36.

Does Your Organization have Detection mechanisms for scanning for unauthorized hardware, software, and changes to configurations?

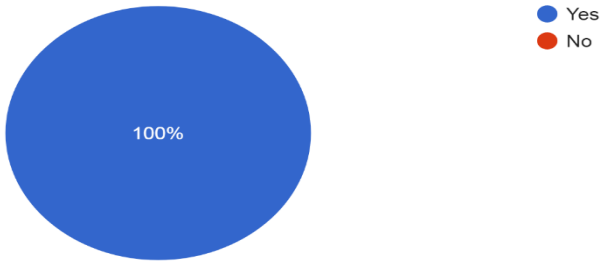
21 responses



Q37.

Does Your Organization have Detection mechanisms for logging and alerting of access to sensitive data or unsuccessful login attempts to identify potential unauthorized access?

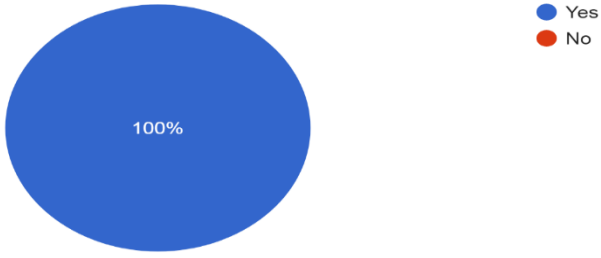
21 responses



Q38.

Does Your Organization have Detection mechanisms that focus on users with highly privileged access accounts and provide a focused level of monitoring in light of the heightened risks involved?

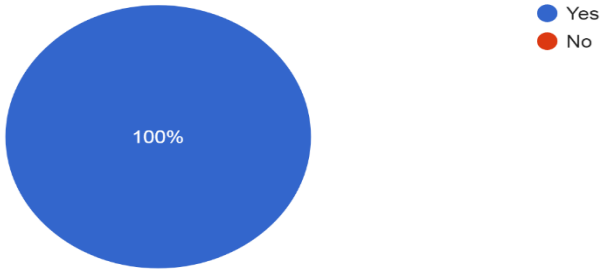
21 responses



Q39.

Does Your Organization have mechanisms for Incident analysis, including how incidents are to be categorized, classified, and prioritized?

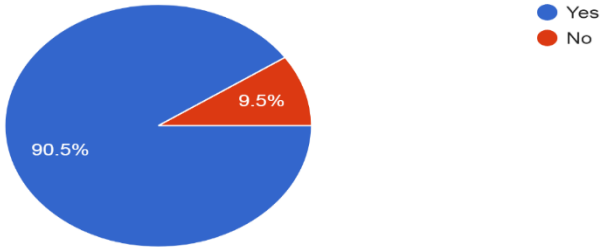
21 responses



Q40.

Does Your Organization have mechanisms for Activating a Cyber Incident Response Team (CIRT) to manage critical incidents?

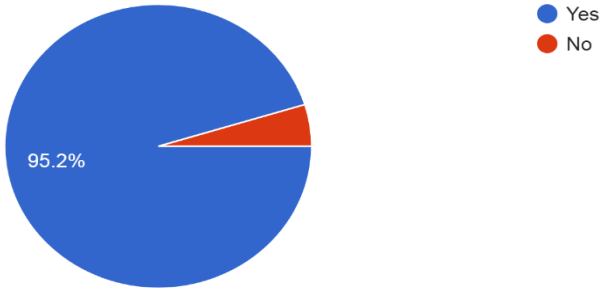
21 responses



Q41.

Does Your Organization have a secure location for storing data captured during an incident, which could be used as evidence of the incident and the a...o be provided to third-party stakeholders if needed

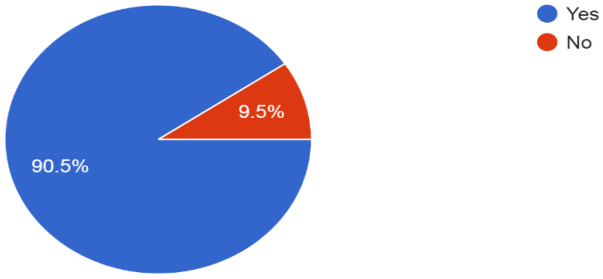
21 responses



Q42.

Does Your Organization have a communication plan during and after Security incidents?

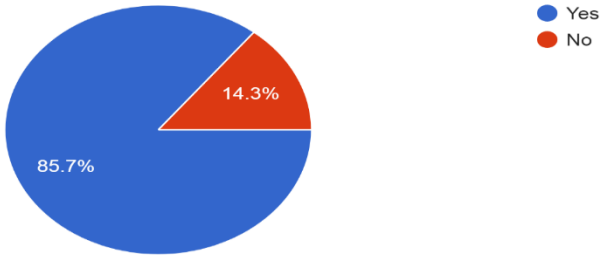
21 responses



Q43.

Does Your Organization have documented process to conduct Post Incident Reviews (PIR) following the conclusion of an incident PIR reports with re...s are submitted to management for an endorsement?

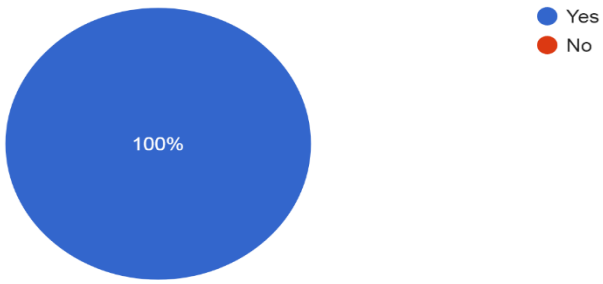
21 responses



Q44.

Does Your Organization have the ability to, and maintain logs for all network, IDS, IPS, and endpoint devices?

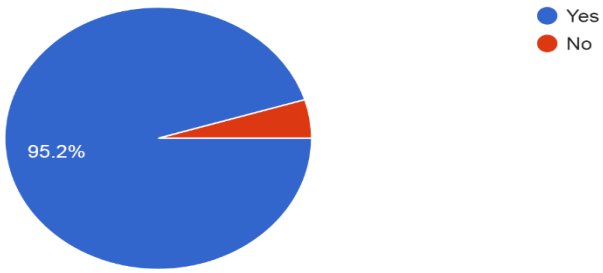
21 responses



Q45.

Does Your Organization have Incident Reporting capability for end users? (dedicated Incident Reporting Hotline, Incident Ticket system, manual forms)?

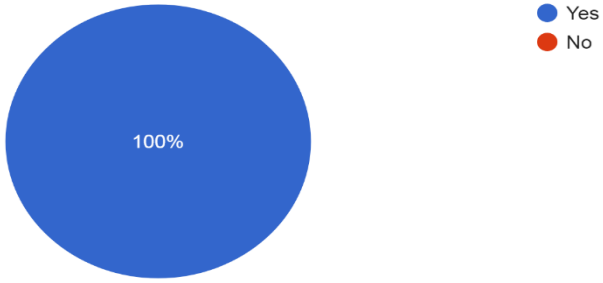
21 responses



Q46.

Does Your Organization conduct regular vulnerability scanning and penetration testing?

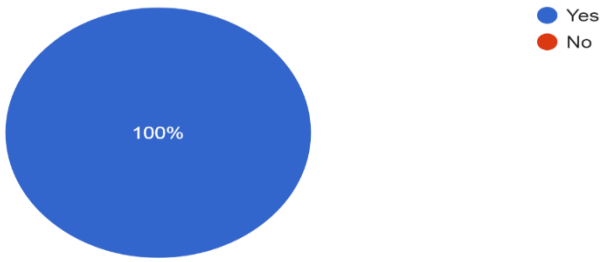
21 responses



Q47.

Does Your Organization monitor insider threats, such as analyzing user activity to spot any anomalous behavior (e.g. logging in from an unusual location, accessing unauthorized files, etc.)?

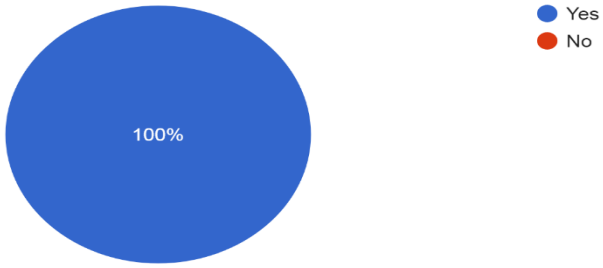
21 responses



Q48.

Does Your Organization have an automated alert system to inform key IT personnel of unwanted behavior or activity on the network?

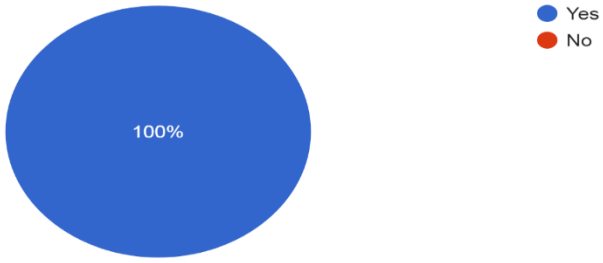
21 responses



Q50.

Does Your Organization have a process in place to regularly review the output from your security systems — anti—malware, firewall, IDS, traffic filte...spot unwanted behaviors or activity on the network?

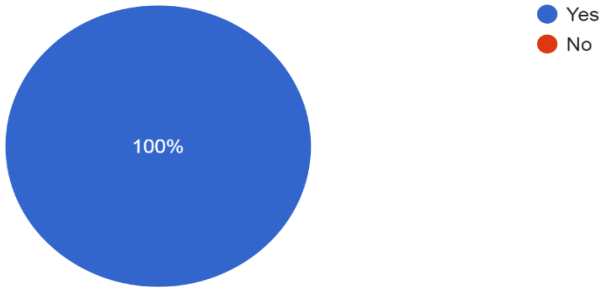
21 responses



Q51.

Does Your Organization have a well-equipped Security Operation Center (SOC)?

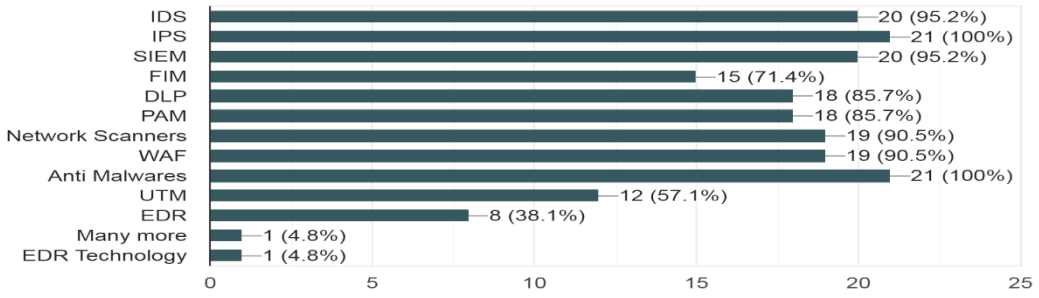
21 responses



Q52.

Does Your Organization have one of the following incidents Prevention, aggregation, Detection, handling, and response Tools? Select more than 1 if applicable.

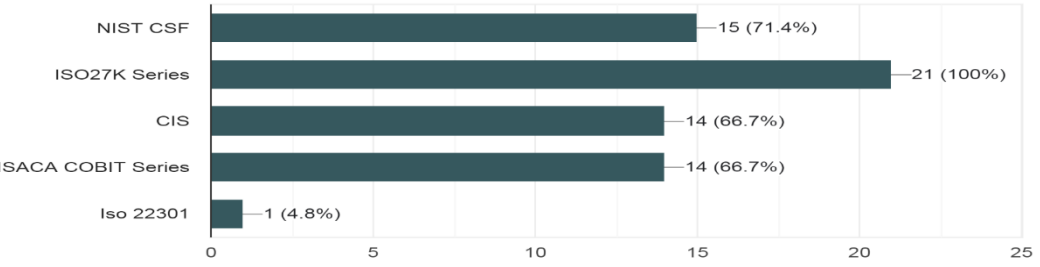
21 responses



Q53.

Does Your Organization follow one of bellow good practice frameworks for Establishing incident handling and response process?

21 responses

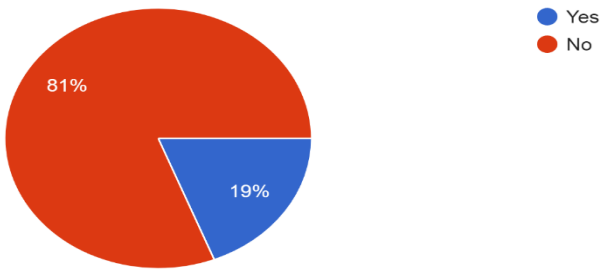


Cybersecurity Forensics Capabilities

Q54.

Does Your Organization Have an Internal Digital Forensics Department, unit, Personal, or Team? who is qualified and trained to investigate incidents within a digital environment?

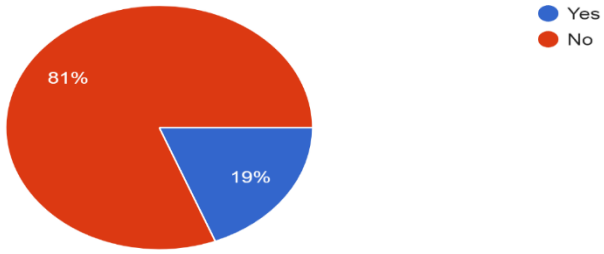
21 responses



Q55.

Does your organization develop or support any professional training courses in Digital Forensics for the Forensics or information security team?

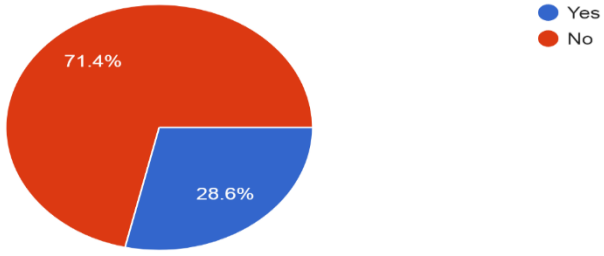
21 responses



Q56.

Does your organization have in Place Process for Cyber Forensics and digital investigation? Does it Have Updated cyber Forensics policies, procedures, or standards?

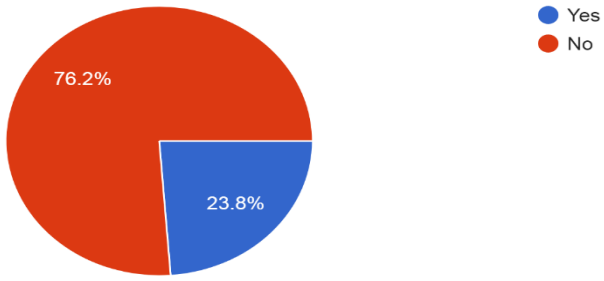
21 responses



Q57.

Does Your Organization Have in Place Cyber Forensics roles and responsibilities Charter? So that each related party knows about their Forensics Roles and Responsibilities?

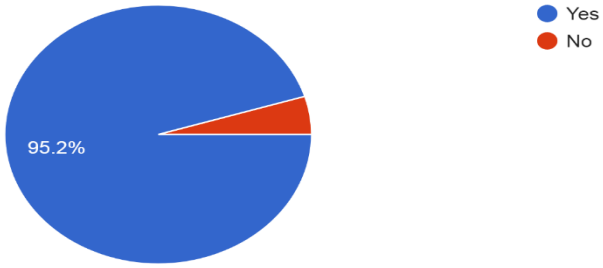
21 responses



Q58.

Does Your Organization have internal or third-party arrangements and capabilities for Investigating Insider Incidents?

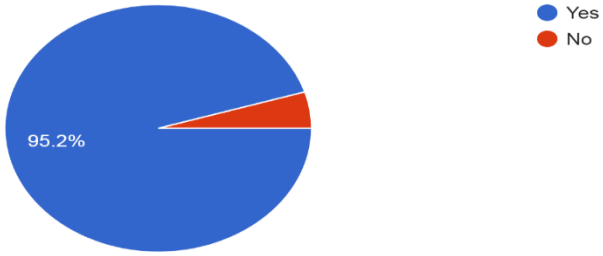
21 responses



Q59.

Does Your Organization have the ability to investigate logs for all network, IDS, IPS, and endpoint devices?

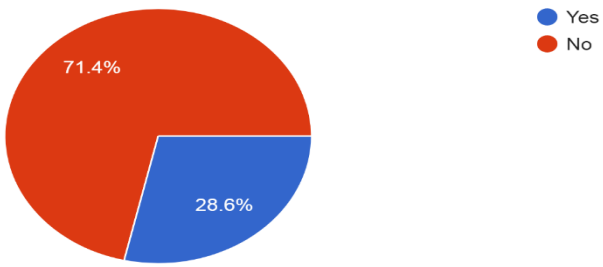
21 responses



Q60.

Does Your Organization follow a good practice framework for Establishing Digital Forensics and Investigation process?

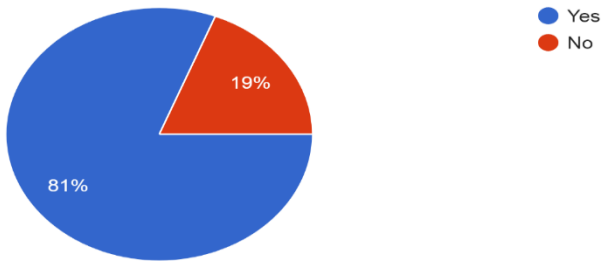
21 responses



Q61.

Does Your Organization have to follow regulatory requirements in regard to Digital Forensics and Investigation process?

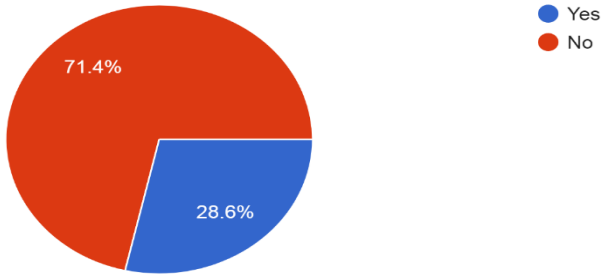
21 responses



Q62.

Does Your Organization use specific tools during the Digital forensics Investigation process?

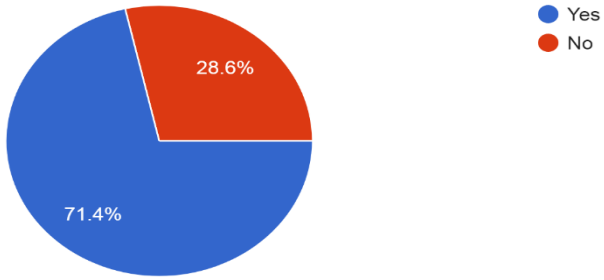
21 responses



Q63.

Does Your Organization Have an integrated forensics process during the cyber security incidents response process?

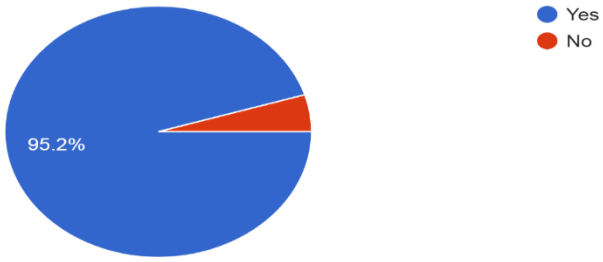
21 responses



Q64.

Does Your Organization have the ability to preserve collected logs and digital evidence for all network, IDS, IPS, and endpoint devices? within safe location

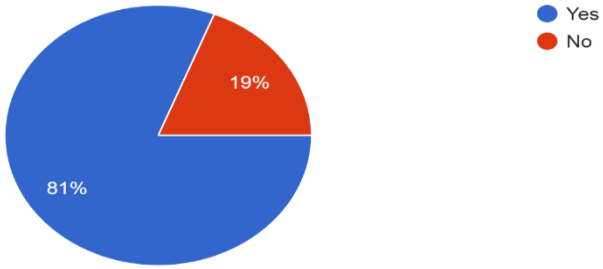
21 responses



Q65.

Does Your Organization Have pre-approved scenarios for all cases and sources of evidence that need digital forensics actions?

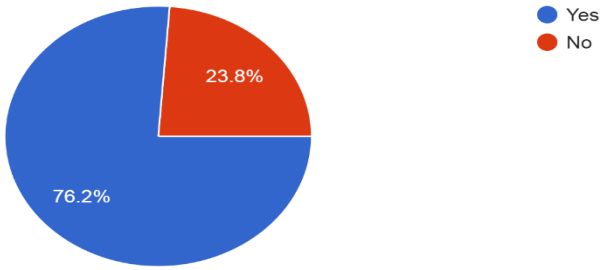
21 responses



Q66.

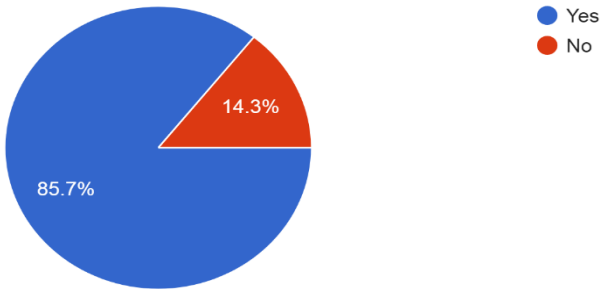
Does Your Organization develop a chain of custody practices and policy in order to ensure the integrity of collected evidence and logs?

21 responses



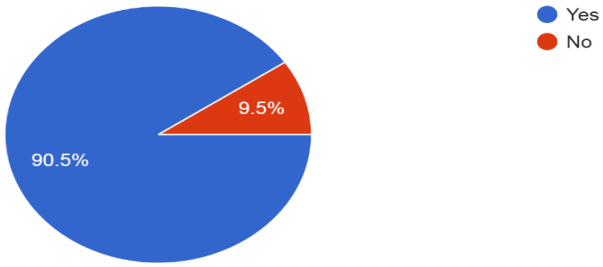
Q67.

Does Your Organization Have an approved practice to Determine evidence-collection requirements?
21 responses



Q68.

Does Your Organization Have an approved practice to Ensure legal review to facilitate appropriate action in response to an incident?
21 responses



Q69.

Please give a brief step-by-step description of the followed process and procedures during cyber incident handling (from the incidents detection phase through the forensics phase, ending with the reporting and documentation phase). 15 responses

- Confidential
- Switzerland has a formalized regulatory framework for banks to handle cyber security incidents, client data disclosure, and thresholds with associated practices for cyber frauds including disclosure to regulators.
- Na
- Not within my jurisdiction
- Incidents identification, detection, analysis, investigation, forensics, containment, reporting

- NIST typical process: preparation, detection and analysis, containment, eradication, and recovery, post-incident activities, and reporting
- Detection, collection, analysis, preserving, presenting
- N
- There are no clear procedures or process
- Detection, analysis, investigations, mitigation, response, recovery, and report
- Prepare; identify; contain; eradicate; restore; lessons learned
- Incidents indicators identification, activity detection, incident analysis, investigation and forensics, treatment and responses, recovery and reporting
- We follow the NIST process model
- Detection then analysis then escalation then forensics then treatment then mitigation then reporting
- Identify the list of internal threats, threat events, detect events, analyze events, investigate and forensics, examine, mitigate or authorize, reporting

Q70.

What process do you believe, should be embedded within your organization's current practices to develop and enhance cyber incident, forensics, and response capabilities? 15 responses

- Nothing
- None in particular
- Na
- A dedicated and trained forensics team
- Enhance forensics capabilities to ensure proper investigation of all incidents by establishing forensics formal and documented forensics process
- Incident response and handling simulation
- Forensics process (following detection & analysis phase)
- The forensics process should be included in the incident response process
- N
- Incident management procedure built on best practice
- Soar automation
- Standard and solid forensics process
- Building integrated incident response and forensics process as an early warning system
- Establish solid forensics processes that ensure proper training and preparation for all stakeholders
- Establish a well-defined process model during incidents response activities

End of Survey

Appendix 4: Framework's Theoretical Validation Attestation Form*

1. Assessor's General Information and Overall Opinion:

- Name: ……
- Job Title:……..
- Information, Cybersecurity, or IS Audit Experience (Year):……
- Financial Related Services Experience (Y, N):……
- Overall Expert Opinion (Relevance &Valid, Relevance & Not Valid, Not Relevance &Valid, Not Relevance & Not Valid) …….
- Comments & Recommendations: (If Any)…..……

2. The Proposed Framework Model – Summary View

The Proposed Framework Summary

Proposed Framework (Pillars)	Proposed Framework (Pillars Enablers)	Processes (To-Do List)	Elements Overall Assessment (Y, N)
Governance	G1. Strategy	(GS1 – GS6): 6	
	G2. Policy and Procedure	(GP1 – GP5): 5	
	G3. Culture	(GC1 – GC4): 4	
	G4. Top Management Support	(GT1 – GT4): 4	
	G.5 Risk Assessment	(GR1 – GR5): 5	
	G.6 Legal Requirement	(GL1 – GL3): 3	
People	P1. Non-Technical Stakeholders	(PN1 – PN5): 5	
	P2. Technical Stakeholders	(PT1 – PT5): 5	
	P3. Training	(PTr1 – PTr5): 5	
Infrastructure	I1. Technology	(IT1 – IT10): 10	
	I2. System Architecture	(IS1 – IS5): 5	
Monitoring	M1. System Monitoring - Preparation	(MSP1 – MSP8): 8	
	M2. System Monitoring - Detection	(MSI1 – MSI51): 51	
	M3. System Monitoring - Analysis	(MSA1 – MSA4): 4	
	M4. System Monitoring - Forensics	(MSF1 – MSF5): 5	
	M5. System Monitoring - Contained	(MSC1 – MSC4): 4	
	M6. Forensic Preparation	(MF1 – MF2): 2	
Reporting	R1. Reporting	(RR1 – RR3): 3	

***Important Note: "This Form is Designed for Scientific Research Purposes Only, and Shall not be Used for Any Other Purposes, Neither by Researcher nor by Assessors."**

Appendix 5: Focus Group Distribution List & Meeting Invitation – Email Messages

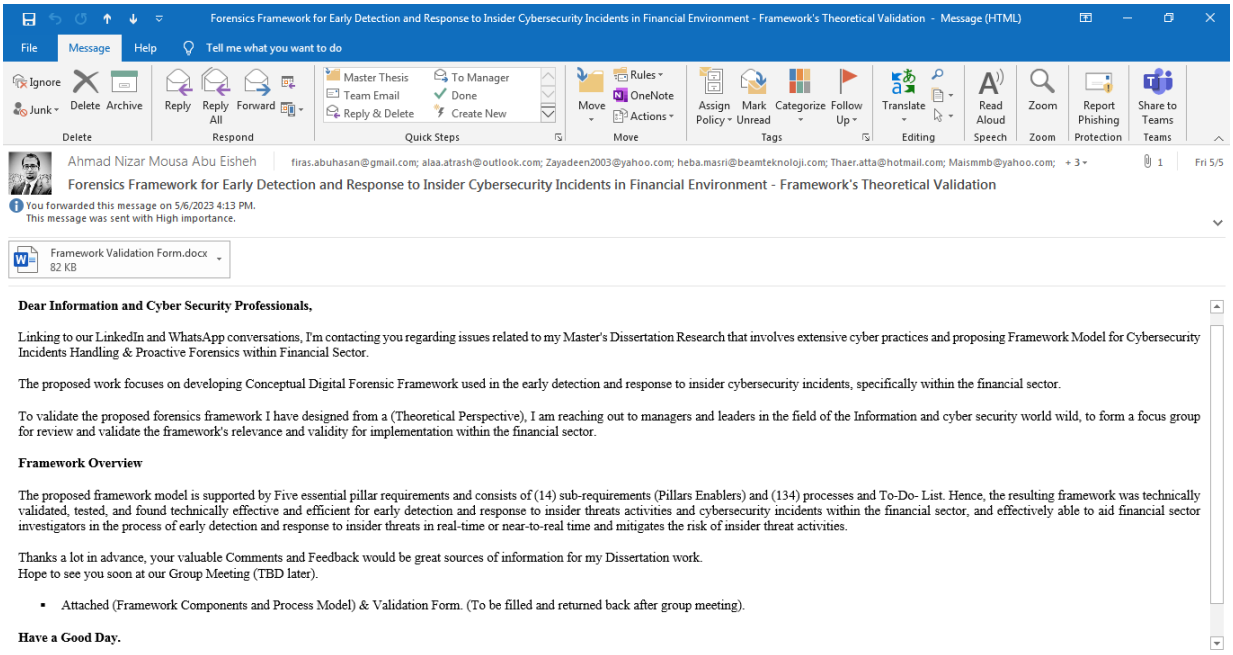


Figure A5.1: Focus Group Distribution List – Email Messages.

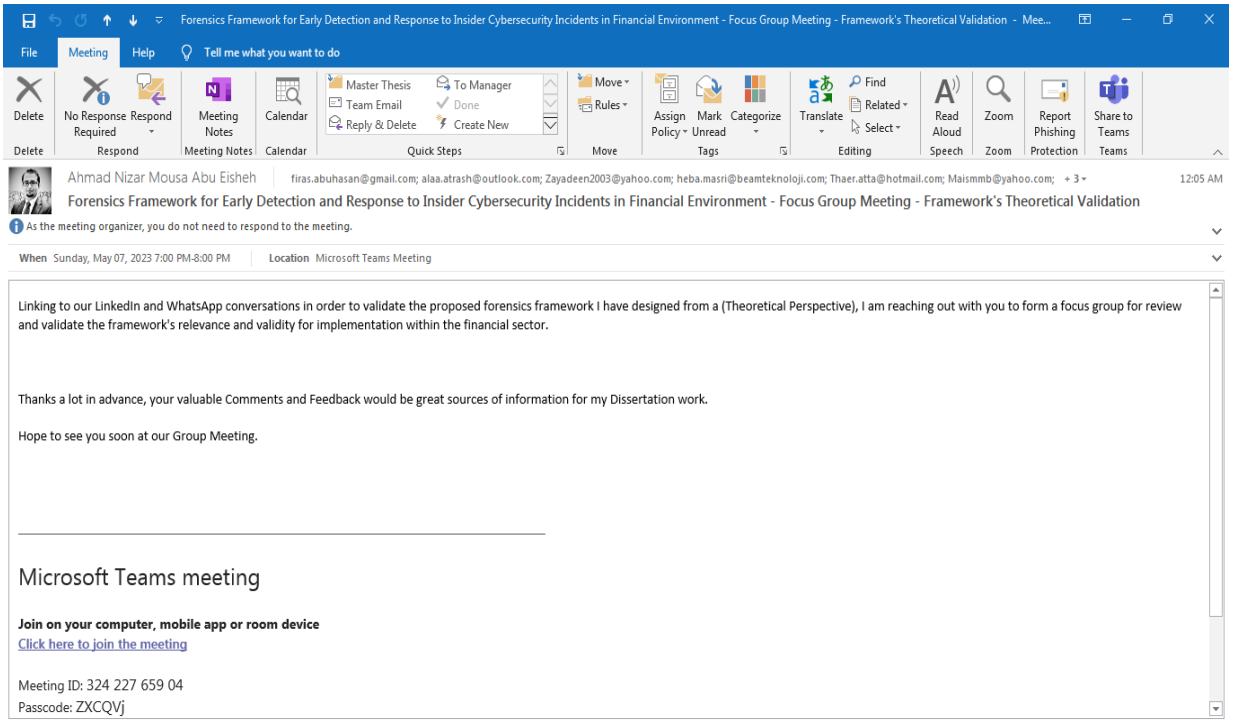


Figure A5.2: Focus Group Meeting Invitation – Email Messages.

Appendix 6: Focus Group Meeting (Start & End) – Microsoft Teams

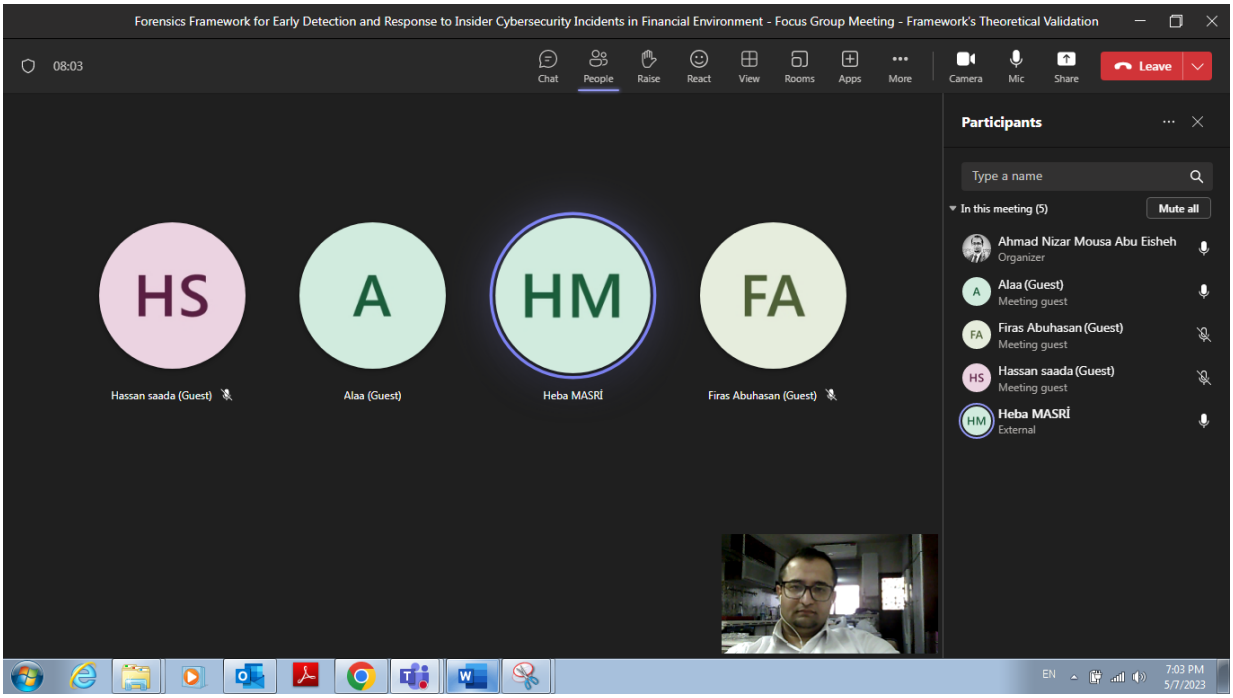


Figure A6.1: Focus Group Meeting (Start) – Microsoft Teams.

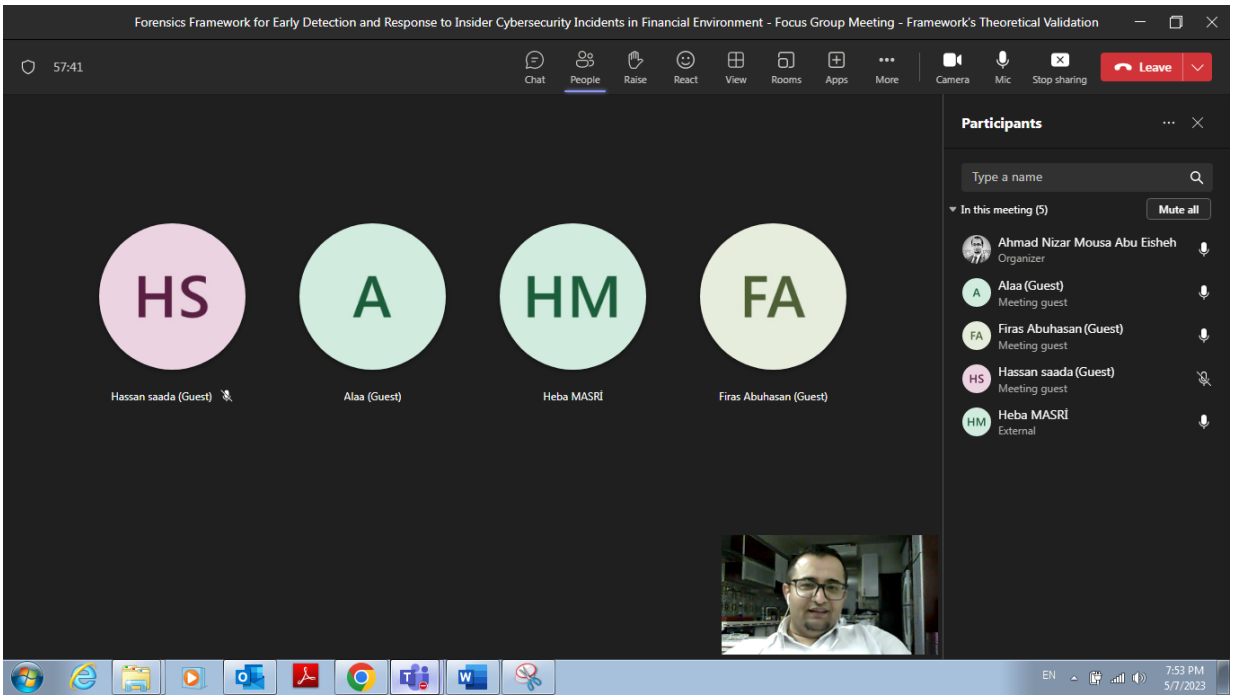


Figure A6.2: Focus Group Meeting (End) – Microsoft Teams.

Appendix 7: Focus Group Meeting – Microsoft Teams Invitation & Attendees List

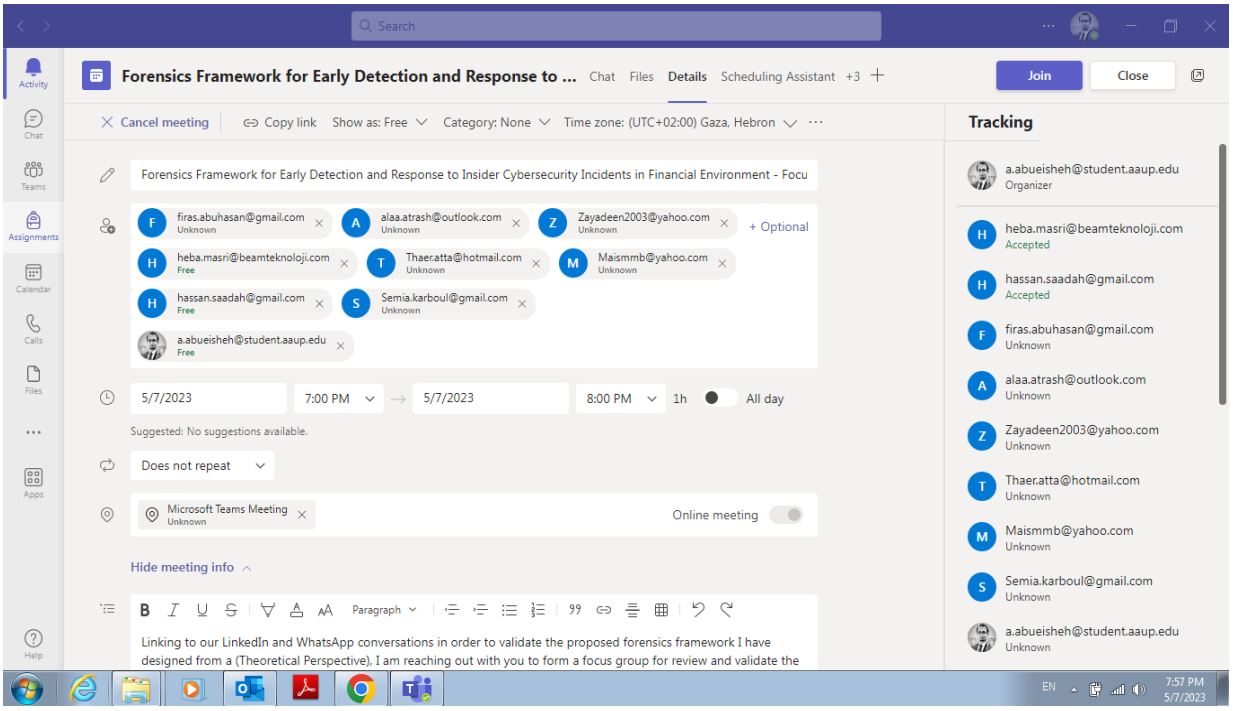


Figure A7.1: Focus Group Meeting – Microsoft Teams Invitation.

Appendix 8: Focus Group Meeting – Microsoft Teams Attendees List and Overall Opinion

Table A8.1: Focus Group Meeting – Microsoft Teams Attendees List Information.

The Invited Person	Job Title	Linkedin Profile	Attendance Status	Overall Opinion
Ahmad N. Abu Eisheh	Head of Information Security and Business Continuity Unit At Quds Bank	**https://www.linkedin.com/in/%D9%90ahmad-n-abu-eisheh-cisa%C2%AE-726831176/**	**Attended**	**Relevant and valid**
Ala' Zayadeen	Head of Information Security and Data Privacy at BinDawood holding	**https://www.linkedin.com/in/alazayadeen/**	**Absence (Response by Mail)**	**Relevant and valid**
Firas AbuHasan	Head Information Security Management at Central Bank of Palestine (PMA)	**https://www.linkedin.com/in/firas-abuhasan-profile/**	**Attended**	**Relevant and valid**
Alaa Alatrash	Information Security Consultant (Financial Sector)	**https://www.linkedin.com/in/alaa-alatrash/**	**Attended**	**Relevant and valid**
Heba Masri	Security Solutions Sales Business Development at BEAM Teknoloji A.Ş.	**https://www.linkedin.com/in/heba-masri/**	**Attended**	**Relevant and valid**
Thaer Atta	Manager | Advisory Services - Technology Risk at EY	**https://www.linkedin.com/in/thaer-atta-cisa-cobit-ceh-7450821b/**	**Absence**	**No Response**
Mais Badarneh	Information & Cyber Security Manager at Housing Bank for Trade and Finance	**https://www.linkedin.com/in/maisbadarneh/**	**Absence**	**No Response**
Hassan Saada	Risk Management & Information Security Manager at Jerusalem District Electricity Co.	**https://www.linkedin.com/in/hassansaada/**	**Attended**	**Relevant and valid**
Samia Karboul	Financial Audit Management Specialist at The World Bank	**https://www.linkedin.com/in/samia-karboul-cpa-cisa-13ab19a5/**	**Absence**	**No Response**

Appendix 9: Framework's Theoretical Validation Attestation Form – Sample of Responses

Framework's Theoretical Validation Attestation Form*

1. **Assessor's General Information and Overall Opinion:**

- Name: Firas Abuhasan.....
- Job Title: Information Security Division Chief.....
- Information, Cybersecurity, or IS Audit Experience (Year):10 years .....
- Financial Related Services Experience (Y, N):Y (11 Years).....
- Overall Expert Opinion (Relevance &Valid, Relevance & Not Valid, Not Relevance &Valid, Not Relevance & Not Valid) ..... Relevant &Valid .....
- Comments & Recommendations: (If Any).....

2. **The Proposed Framework Model – Summary View**

The Proposed Framework Summary

Proposed Framework (Pillars)	Proposed Framework (Pillars Enablers)	Processes (To Do List)	Elements Overall Assessment (Y, N)
Governance	G1. Strategy	(GS1 – GS6): 6	Y
	G2. Policy and Procedure	(GP1 – GP5): 5	Y
	G3. Culture	(GC1 – GC4): 4	Y
	G4. Top Management Support	(GT1 – GT4): 4	Y
	G.5 Risk Assessment	(GR1 – GR5): 5	Y
	G.6 Legal Requirement	(GL1 – GL3): 3	Y
People	P1. Non-Technical Stakeholders	(PN1 – PN5): 5	Y
	P2. Technical Stakeholders	(PT1 – PT5): 5	Y
	P3. Training	(PTr1 – PTr5): 5	Y
Infrastructure	I1. Technology	(IT1 – IT10): 10	Y
	I2. System Architecture	(IS1 – IS5): 5	Y
Monitoring	M1. System Monitoring - Preparation	(MSP1 – MSP8): 8	Y
	M2. System Monitoring - Detection	(MSI1 – MSI51): 51	Y
	M3. System Monitoring - Analysis	(MSA1 – MSA4): 4	Y
	M4. System Monitoring - Forensics	(MSF1 – MSF5): 5	Y
	M5. System Monitoring - Contained	(MSC1 – MSC4): 4	Y
	M6. Forensic Preparation	(MF1 – MF2): 2	Y
Reporting	R1. Reporting	(RR1 – RR3): 3	Y

***Important Note: " This Form is Designed For Scientific Research Purposes Only, and Shall not be Used for Any Other Purposes, Neither by Researcher nor by Assessors."**

Firas Abu Hasan

Figure A9.1: Signed Framework's Theoretical Validation Attestation Form – Firas Abu Hasan.

Framework's Theoretical Validation Attestation Form*

1. **Assessor's General Information and Overall Opinion:**

- Name: Hasan Saada
- Job Title: Information Security and Risk Management Manager
- Information, Cybersecurity, or IS Audit Experience (Yeare): 14 years
- Financial Related Services Experience (Y, N):Y
- Overall Expert Opinion (Relevance &Valid, Relevance & Not Valid, Not Relevance &Valid, Not Relevance & Not Valid) : Relevance &Valid
- Comments & Recommendations: (If Any).....

2. **The Proposed Framework Model – Summary View**

The Proposed Framework Summary

Proposed Framework (Pillars)	Proposed Framework (Pillars Enablers)	Processes (To Do List)	Elements Overall Assessment (Y, N)
Governance	G1. Strategy	(GS1 – GS6): 6	Y
	G2. Policy and Procedure	(GP1 – GP5): 5	Y
	G3. Culture	(GC1 – GC4): 4	Y
	G4. Top Management Support	(GT1 – GT4): 4	Y
	G.5 Risk Assessment	(GR1 – GR5): 5	Y
	G.6 Legal Requirement	(GL1 – GL3): 3	Y
People	P1. Non-Technical Stakeholders	(PN1 – PN5): 5	Y
	P2. Technical Stakeholders	(PT1 – PT5): 5	Y
	P3. Training	(PTr1 – PTr5): 5	Y
Infrastructure	I1. Technology	(IT1 – IT10): 10	Y
	I2. System Architecture	(IS1 – IS5): 5	Y
Monitoring	M1. System Monitoring - Preparation	(MSP1 – MSP8): 8	Y
	M2. System Monitoring - Detection	(MSI1 – MSI51): 51	Y
	M3. System Monitoring - Analysis	(MSA1 – MSA4): 4	Y
	M4. System Monitoring - Forensics	(MSF1 – MSF5): 5	Y
	M5. System Monitoring - Contained	(MSC1 – MSC4): 4	Y
	M6. Forensic Preparation	(MF1 – MF2): 2	Y
Reporting	R1. Reporting	(RR1 – RR3): 3	Y

***Important Note: " This Form is Designed For Scientific Research Purposes Only, and Shall not be Used for Any Other Purposes, Neither by Researcher nor by Assessors."**

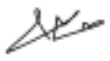


Figure A9.2: Signed Framework's Theoretical Validation Attestation Form – Hasan Saada.

Framework's Theoretical Validation Attestation Form*

1. **Assessor's General Information and Overall Opinion:**

- Name: *Alaa Azmi Alatrash*
- Job Title: *Information Security Consultant*
- Information, Cybersecurity, or IS Audit Experience (Yeare):*13*
- Financial Related Services Experience (Y, N):*Yes*
- Overall Expert Opinion (Relevance &Valid, Relevance & Not Valid, Not Relevance &Valid, Not Relevance & Not Valid) *Relevant and Valid.*
- Comments & Recommendations: (If Any) *A modular framework that includes various components to ensure the readiness of organizations to detect cybercrimes. By implementing such a framework and continuously monitoring and idjusting. organizations can enhance their ability to detect cyber crimes.*

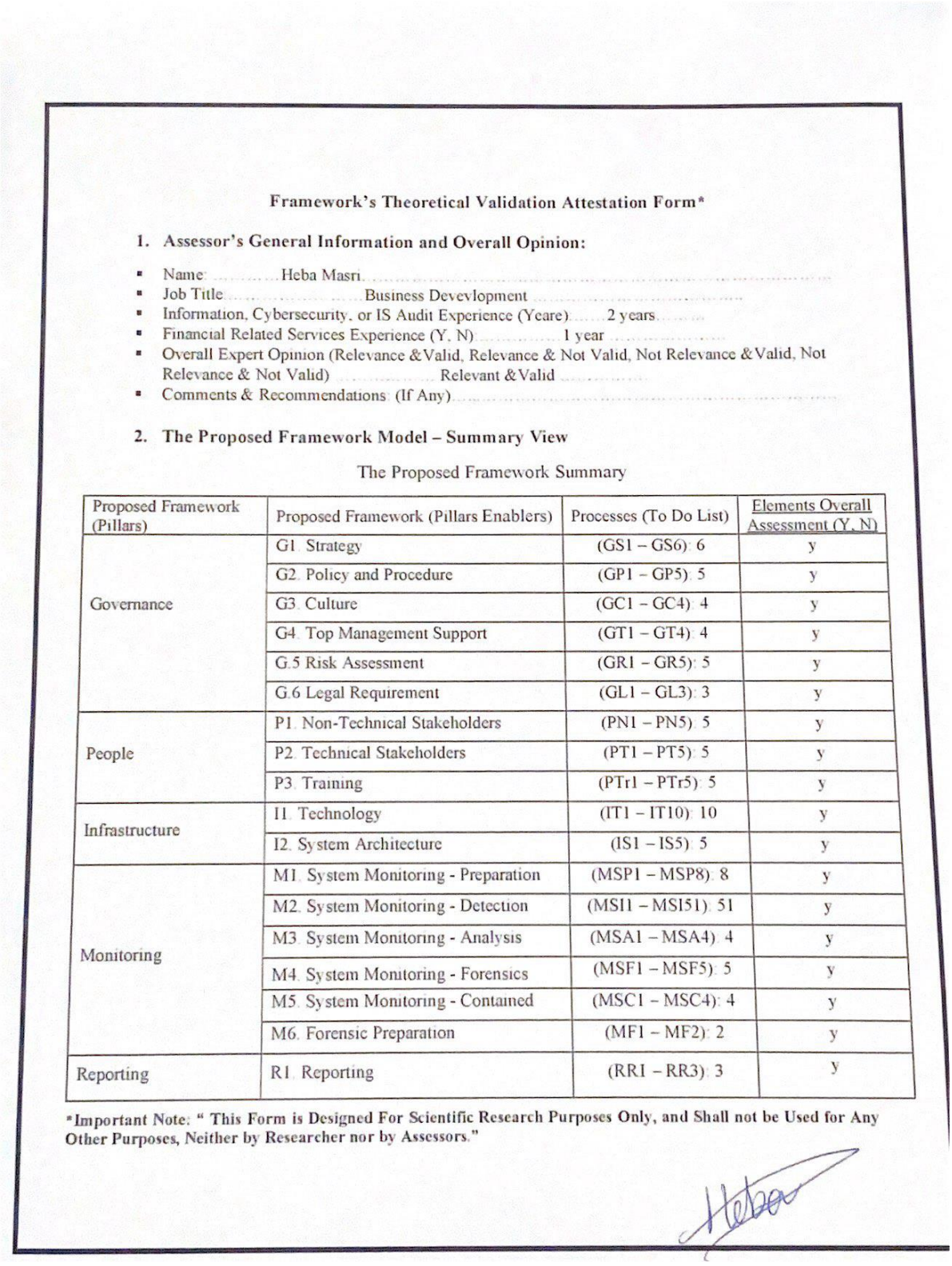
Alaa Alatrash 11/5/2023

2. **The Proposed Framework Model – Summary View**

The Proposed Framework Summary

Proposed Framework (Pillars)	Proposed Framework (Pillars Enablers)	Processes (To Do List)	Elements Overall Assessment (Y, N)
Governance	G1. Strategy	(GS1 – GS6): 6	
	G2. Policy and Procedure	(GP1 – GP5): 5	
	G3. Culture	(GC1 – GC4): 4	
	G4. Top Management Support	(GT1 – GT4): 4	
	G.5 Risk Assessment	(GR1 – GR5): 5	
	G.6 Legal Requirement	(GL1 – GL3): 3	
People	P1. Non-Technical Stakeholders	(PN1 – PN5): 5	
	P2. Technical Stakeholders	(PT1 – PT5): 5	
	P3. Training	(PTr1 – PTr5): 5	
Infrastructure	I1. Technology	(IT1 – IT10): 10	
	I2. System Architecture	(IS1 – IS5): 5	
Monitoring	M1. System Monitoring - Preparation	(MSP1 – MSP8): 8	
	M2. System Monitoring - Detection	(MSI1 – MSI51): 51	
	M3. System Monitoring - Analysis	(MSA1 – MSA4): 4	
	M4. System Monitoring - Forensics	(MSF1 – MSF5): 5	
	M5. System Monitoring - Contained	(MSC1 – MSC4): 4	
	M6. Forensic Preparation	(MF1 – MF2): 2	

Figure A9.3: Signed Framework's Theoretical Validation Attestation Form – Alaa Atrash.



Framework's Theoretical Validation Attestation Form*

1. **Assessor's General Information and Overall Opinion:**

- Name: Heba Masri
- Job Title: Business Devevlopment
- Information, Cybersecurity, or IS Audit Experience (Yeare): 2 years
- Financial Related Services Experience (Y, N): 1 year
- Overall Expert Opinion (Relevance &Valid, Relevance & Not Valid, Not Relevance &Valid, Not Relevance & Not Valid): Relevant &Valid
- Comments & Recommendations (If Any):

2. **The Proposed Framework Model – Summary View**

The Proposed Framework Summary

Proposed Framework (Pillars)	Proposed Framework (Pillars Enablers)	Processes (To Do List)	Elements Overall Assessment (Y, N)
Governance	G1. Strategy	(GS1 – GS6): 6	y
	G2. Policy and Procedure	(GP1 – GP5): 5	y
	G3. Culture	(GC1 – GC4): 4	y
	G4. Top Management Support	(GT1 – GT4): 4	y
	G.5 Risk Assessment	(GR1 – GR5): 5	y
	G.6 Legal Requirement	(GL1 – GL3): 3	y
People	P1. Non-Technical Stakeholders	(PN1 – PN5): 5	y
	P2. Technical Stakeholders	(PT1 – PT5): 5	y
	P3. Training	(PTr1 – PTr5): 5	y
Infrastructure	I1. Technology	(IT1 – IT10): 10	y
	I2. System Architecture	(IS1 – IS5): 5	y
Monitoring	M1. System Monitoring - Preparation	(MSP1 – MSP8): 8	y
	M2. System Monitoring - Detection	(MSI1 – MSI51): 51	y
	M3. System Monitoring - Analysis	(MSA1 – MSA4): 4	y
	M4. System Monitoring - Forensics	(MSF1 – MSF5): 5	y
	M5. System Monitoring - Contained	(MSC1 – MSC4): 4	y
	M6. Forensic Preparation	(MF1 – MF2): 2	y
Reporting	R1. Reporting	(RR1 – RR3): 3	y

*Important Note: " This Form is Designed For Scientific Research Purposes Only, and Shall not be Used for Any Other Purposes, Neither by Researcher nor by Assessors."

Figure A9.4: Signed Framework's Theoretical Validation Attestation Form – Heba Masri.

الملخص

تتعرض أنظمة تكنولوجيا المعلومات والفضاء الإلكتروني وخاصة في مؤسسات القطاع المالي، إلى شريحة واسعه جدا من الهجمات الإلكترونية والمخاطر الأمنية التي قد تنتج بشكل رئيسي من الأنشطة الخبيثة التي قد تتعرض لها تلك المؤسسات، سواء كانت تلك الأنشطة مصدرها من الداخل أو من خارج المؤسسة، والتي تكون في معظمها مدفوعة بمبررات ودوافع خبيثة مختلفة لدى المهاجمين (التخريب والتدمير المتعمد للأصول والبيانات، الاحتيال المالي، سرقة البيانات والوصول غير المصرح به لها... إلخ).

وفي الوقت الذي تشكل فيه التهديدات الداخلية وأنشطتها الخبيثة الخطر الأكبر على المؤسسات المالية وفقا للأبحاث والدراسات الأمنية العالمية، تعتبر ممارسات الكشف المبكر، التحقيق، والاستجابة الفاعلة في تلك الأنشطة ومسبباتها، ومعالجتها في الوقت المناسب، عملية حيوية ومهمة جدًا للكشف عن معلومات تلك الأنشطة وتتبعها داخل البيئة الرقمية لضمان امن وحماية الأصول الرقمية للمؤسسة المالية من تلك التهديدات، من خلال تحديد وتطوير وتنظيم وإنفاذ ممارسات التحقيق الرقمي الفاعل للأنشطة الداخلية الخبيثة وبناء اطار عمل ومنظومة نظرية متكاملة لإدارة عمليات التحقيقات الرقمية في بيئة تكنولوجيا المعلومات للمؤسسات المالية العالمية.

تقدم هذه الأطروحة إطار عمل التحقيقات الرقمية المستخدمة في الكشف والاستجابة المبكرين للتهديدات الأمنية الداخلية وحوادث الأمن السيبراني التي قد تنشا من داخل مؤسسات القطاع المالي العالمي. حيث تم وبالاستناد إلى منهجية النظرية المتجذرة (Grounded Theory) كإحدى اهم أدوات البحث العملي النوعي وجمع البيانات النوعية، تطوير نموذج الإطار المقترح من خلال مراجعة الأدبيات الحالية وعمليات البحث الشامل لمجموعة من نماذج اطر عمل التحقيقات الرقمية والاستجابة للحوادث الأمنية وتحسينها. بالإضافة إلى التعرف على الممارسات الفعلية والحقيقية للتحقيقات الرقمية والاستجابة للحوادث الأمنية داخل القطاع المالي المنتشرة عالميا من خلال استخدام استبيانات تقييمية لجمع المعلومات وضمان إدخال التحسينات المناسبة للإطار قيد التطوير.

يرتكز نموذج الإطار المقترح على خمسة متطلبات أساسية (دعامات)، ينبثق عنها (14) من المتطلبات الفرعية (عوامل التمكين للدعامات) و (134) عملية ونشاط فرعي (قوائم المهام). تم التحقق من صحة الإطار من قبل مجموعة من الخبراء، كما تم اختباره ووجد أنه فعال في الكشف المبكر والاستجابة لأنشطة التهديدات الداخلية وحوادث الأمن السيبراني داخل القطاع المالي. تم تحقيق الغاية والإسهام العلمي في

الإطار المقترح من خلال تزويد مختصيي الأمن السيبراني في المؤسسات المالية، بإطار عمل جديد لمساعدتهم خلال عمليات التحقيق في الحوادث السيبرانية الداخلية في مؤسساتهم. بالإضافة إلى إغلاق الفجوة القائمة في اطر التحقيقات الرقمية الحالية- العامة وتصميم إطار عمل جديد صمم خصيصا للقطاع المصرفي.