A Conceptual Model for Digital Forensic Readiness in Security Operation Centres: A South African Study

A dissertation submitted to the

Department of Information Systems

Faculty of Commerce

University of Cape Town

In partial fulfilment of the requirements for the degree

Master of Commerce in Information Systems

By Boitumelo Nkwe

Supervisor: Professor Michael Kyobe

University of Cape Town

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

University of Cape Town

Plagiarism Declaration

1. This dissertation has been submitted to Turnitin (or equivalent similarity and originality checking software) and I confirm that my supervisor has seen my report, and any concerns revealed by such have been resolved with my supervisor.
2. I certify that I have received Ethics approval (if applicable) from the Commerce Ethics Committee.
3. This work has not been previously submitted in whole, or in part, for the award of any degree in this or any other university. It is my own work. Each significant contribution to, and quotation in, this dissertation from the work, or works of other people has been attributed, and has been cited and referenced.

Student number	NKWBOI002
Student name	Boitumelo Nkwe
Signature of Student	Signed by candidate
Date:	

ABSTRACT

The increase in the adoption of technology has resulted in the number of cyber-attacks and security breaches also rising. These cyber-attacks and breaches have become advanced and can go undetected for months. With the rise in cyber-attacks, the need for organizations to tighten cybersecurity measures and be ready to investigate the breaches speedily has become crucial. These measures include the adoption of Security Operations Centres (SOC) that integrate digital forensic capabilities with various cybersecurity tools.

The reviewed literature shows that having a well-defined digital forensic readiness (DFR) strategy in place is important to ensure quick and efficient investigations that do not have a huge impact on the organization. In addition, conducting internal investigations helps an organization reduce costs. While there are proposed frameworks that aim to help an organization become forensically ready, none have a specific focus on a SOC. SOCs are complex, making conducting a digital forensic investigation challenging.

The objective of this study was to develop a conceptual model for DFR that focused on SOCs in South Africa. To achieve this, the study first analysed existing DFR frameworks and drew key factors that were common in all frameworks. Management support, policies, processes and procedures, forensic technologies, legal frameworks, technical skills, and training were identified as the key factors that have a potential influence on the forensic readiness of a SOC.

The study was conducted using a quantitative research approach and a survey questionnaire. Data were collected from professionals who work in organizations running a SOC in South Africa through a survey. The data were analysed using statistical methods and the results of the study indicate that the digital forensic readiness of a SOC is dependent on management support, organizational policies, processes and procedures, the integration of forensic and cybersecurity technologies, understanding various legal requirements, technical skills, and continuous training. All participants had at least one form of formal qualification and one industry-related certificate.

The proposed DFR conceptual model examined various factors that SOCs can use to assess their forensic readiness. The findings also highlight the importance of having a holistic approach to forensic readiness which also include continuous investment in both technology and technical skills to keep up with evolving technology. Furthermore, the findings can be used by SOCs to identify areas in their DFR plan they need to focus on to enhance their cyber-resilience.

Keywords: *Security operations centre, digital forensic readiness, conceptual models*

ACKNOWLEDGEMENTS

To my supervisor Prof M. Kyobe, no words can ever describe how grateful I am to have had you guiding and supporting me throughout my journey from Honors to Masters. The lessons I learnt from you are invaluable and I hope to one day pay it forward.

To my husband, I would not have made it this far without your love and support. Thank you for holding the fort while I was busy with my studies. My dad, siblings, friends and colleagues, thank you for all your words of encouragement and motivation.

Sindiswa, thank you for making time to listen to all my cries and frustrations throughout this journey. It really meant a lot.

My mentor Dr Nenekazi Mkuzangwe, thank you for all the critical questions you have asked, and making me realise that I must always think of a lay person who might be interested in the subject matter.

Lastly, everyone who took their time to respond to my questionnaire. You are truly appreciated. Le kamoso!

DEDICATION

I dedicate this dissertation to the memory of my late mother, Dikeledi ‘MaFox’ Phokoje. I would also like to dedicate it to my kids and all my nieces and nephews. I hope this serves as a motivation to you.

Table of Contents

Table of Figures

CHAPTER 1:

INTRODUCTION

1.1 Background

The increased reliance on technology and the Internet has led to an unprecedented increase in the number of cybersecurity breaches and incidents experienced by organizations. With technology evolving, more system vulnerabilities are inevitable, which criminals are ready to exploit. In 2022, more than 4,100 breaches were publicly disclosed globally (Powell, 2022). Worth noting are the breaches on social media platforms Twitter and WhatsApp where millions of user data were left exposed (Powell, 2022). During the third quarter of 2024 alone, over 422 million records were reported to have been exposed globally (Petrosyan, 2024).

These breaches do not only bring reputational damage but also financial losses. In 2023, the average cost of a data breach reached $4.45 million US Dollars globally (Morgan, 2024). The total cost of these breaches was estimated to be $8 trillion US Dollars in 2023 (Kerner, 2023). These losses are expected to reach $9.5 trillion US Dollars in 2024 and further increase to $10.5 trillion US Dollars by 2025 (Morgan, 2024).

The African Cyberthreat Assessment Report released by Interpol in 2024 highlighted the ongoing cyber trends and threats that are prevalent in Africa (Puchert, 2024). The report indicates that cyberattacks have become more sophisticated, with ransomware, business email compromise (BEC), and online scams seeing a noticeable increase in the continent (Puchert, 2024). While ransomware attacks have been around for years, the report notes that the attacks have now evolved to target critical infrastructure. The five BEC attacks that have been on the rise include data theft, account compromise or system breach, CEO impersonation, government, law enforcement or attorney impersonation, and the Bogus invoice scheme (Puchert, 2024). Finally, the report highlights an emerging exploitation of Artificial Intelligence (AI) to commit cyber-attacks.

In 2023, it was reported that South Africa ranked 8th in the world with incidents related to ransomware (Mzekandaba, 2023). A survey conducted by the Council for Scientific and Industrial Research (CSIR) in collaboration with the Cybersecurity hub found that almost 90% of the organizations in South Africa admitted having suffered at least one cybersecurity breach. The cost of these breaches is estimated to be R53.10 million per incident, which is an increase from R49.45 million in 2023 (Mzekandaba, 2024).

Some of the notable attacks in South Africa include the Transnet ransomware attack in 2021 that impacted the country's port operations and forced the company to declare a force majeure (Docrat,

2022). In the same year, the South African Department of Justice also experienced a ransomware attack that affected its online payment systems (Richardson, 2021). In 2024, the Department of Justice reported another ransomware attack in which electronic payments for child support were affected (Moyo, 2024). Another noteworthy attack in 2024 was The National Health Laboratory Service (NHLS) ransomware attack that compromised the pathology services of over 265 laboratories nationally (Sunny, 2024)

To respond to the increasing threats posed by cyberattacks, most organizations have increased their investment in cybersecurity technologies and cyber breach reporting mechanisms to support the detection, mitigation, and investigation of attacks (Puchert, 2024). One such investment is through the deployment of a Security Operations Center (SOC). A SOC allows an organization to continuously monitor its information technology (IT) systems and infrastructure to identify vulnerabilities and security breaches and respond to them swiftly (Onwubiko & Ouazzane, 2022). It achieves this through incorporating people, processes, and technologies (Vielberth et al., 2020). For a SOC to be effective in responding to incidents, it needs to have a holistic approach that includes digital forensic capabilities to investigate security breaches. Clancy (2023) argues that a SOC that is not forensically ready will likely miss important evidence when collecting data for analysis. Therefore, a proper digital forensic readiness (DFR) plan for a SOC environment is required to limit the damage caused by disruptions in IT systems in an organization. Rowlingson (2004) defines DFR as the ability of an organization to optimize the use of digital evidence while at the same time reducing the cost of an investigation. The research considers DFR an important element in creating a cyber-resilient SOC.

1.2 Problem Statement

The continuous increase in cyber breaches and incidents in South Africa has put the spotlight on incident responders and SOC analysts to contain the breach promptly with minimal disruptions to business. Although a SOC is equipped to identify and respond to incidents, it sometimes cannot investigate the source of the breach (Onwubiko & Ouazzane, 2022). Once there is a breach, an effective forensic readiness plan should be in place to ensure rapid resolution and resumption of operations.

The focus of studies related to SOC environments has mostly been on proactive measures such as threat hunting and automated mechanisms to detect threats (Schlette, Vielberth, & Pernul, 2021; Mutemwa, Mtsweni, & Zimba, 2018; Maziana & Khairul, 2021). These studies do not prepare for the

eventuality of a cyber breach. As a result, reactive measures, such as forensic investigations, are often neglected. Most organizations do not have documented procedures to which SOC analysts can refer during a forensic investigation. Furthermore, there is a lack of sufficient training and experience among SOC analysts to perform forensic investigations (Janos & Dai, 2018; Chamkar, Maleh, & Gherabi, 2023).

1.3 Significance of the study

This study offers a useful foundation for improving forensic capabilities within SOCs by developing a DFR conceptual model that is targeted at SOCs. The study highlights the importance of having a well-defined DFR plan for a SOC, including investigating incidents and breaches effectively and reducing the costs of the investigation. Furthermore, organizations can use the findings to effectively allocate its resources and prepare a SOC to handle emerging technologies and threats. The study aims to help South African organizations that are running SOCs to address challenges that are related to conducting forensic investigations. The study also contributes to the existing body of knowledge on DFR in South Africa.

1.4 Research Question & Objectives

The current focus of SOC operations is on threat hunting and incident detection, response, and remediation. Despite the various incident monitoring and prevention tools being deployed in SOCs, a security breach can still happen. When a breach occurs, SOC analysts need to be prepared to conduct a forensic investigation. Therefore, a digital forensic readiness approach is required that will allow an investigation to be carried out faster and with minimal disruptions to business. Most studies conducted on SOC operations focus on the proactive part while not addressing the reactive part of SOC operations (Schlette et al., 2021; Mutemwa et al., 2018; Maziana & Khairul, 2021). Therefore, the research seeks to answer the following questions:

- *What are the key factors that influence the DF readiness of Security Operations Centres in South Africa?*

In answering the main research question, the following sub-research question has been formulated:

- To what extent do existing DFR frameworks cover SOC environments?

The primary objective that follows the research questions is to:

- Identify and analyse key factors that influences DF readiness of a SOC.

The secondary research objectives are to:

- Evaluate the extent to which the existing DFR frameworks address the requirements of SOC environments.
- Develop a DFR conceptual model for SOC environments in South Africa.

1.5 Overview of the Dissertation

Below is an outline of how the dissertation is structured.

Chapter 1 – Introduction: This chapter discusses the background of the study. It further presents the problem statement, the research questions, and the objectives of the study.

Chapter 2 - Review of the literature: Chapter 2 introduces and explains the concepts of SOC, DF, and DFR. The chapter then evaluates the existing frameworks before identifying the literature gaps. Finally, the chapter produces a proposed conceptual DFR model for SOC environments.

Chapter 3 - Research Design: This chapter covers the underlying research philosophy used in this study. The chapter also describes the research methodology, research strategy, and the research sample. Finally, this chapter outlines the time frames for the research and the ethical considerations that were made before data collection.

Chapter 4 – Data Analysis: Chapter 4 covers the descriptive analysis and demographics of the data collected. The chapter presents the results of the validity and reliability tests of the research instruments. This chapter also shows the results from the hypotheses testing. Finally, the summary of the findings is discussed.

Chapter 5 - Conclusions: This chapter concludes the dissertation and gives the limitations of the study and recommendations for future studies.

CHAPTER 2:

LITERATURE REVIEW

This chapter presents an overview of SOC and digital forensics (DF). The chapter begins by defining a SOC, as well as the components that make up a SOC. It then proceeds to discuss DF, digital evidence, and DFR. The developments in technology have given birth to other forms of forensics such as cloud forensics, IoT forensics, image forensics, which are also discussed in this chapter. Additionally, the chapter discusses four digital forensic readiness frameworks and concludes with a proposed conceptual model.

2.1 Definition of a SOC

Chamkar et al. (2023) define a SOC as a centralized facility that monitors, detects, and remediates identified cybersecurity threats and incidents within an organization. The primary objective of a SOC is to ensure the confidentiality, integrity, and availability (CIA) of an organization's information technology (IT) systems, while at the same time helping ensure compliance. A SOC plays an important role in any organization as it supports the overall security strategy (Onwubiko & Ouazzane (2019). Further, they help an organization achieve its governance and legal obligations such as compliance with different data privacy regulations and security standards (Onwubiko & Ouazzane, 2019). In addition to governance benefits, a SOC also assists in minimizing the impact of breaches by reducing the time it takes to detect a breach. Finally, a SOC helps an organization to be ahead of attackers by providing proactive threat-hunting mechanisms.

There are various SOC operating models that an organization can choose from, depending on its size, needs, and budget. The first SOC model is an internal or dedicated SOC. This type of SOC is run and operated entirely by the organization. Furthermore, it has a dedicated team, infrastructure, and a set of processes that are designed to meet the security needs of an organization (Salinas, 2023). In contrast, a managed SOC is run entirely by a third-party provider. A managed SOC provides SOC services to organizations that cannot afford the initial infrastructure as well as the skilled personnel to run it (Chamkar et al., 2023). The third SOC model, a hybrid SOC, offers a bridge between an internal and a managed SOC (Anson, 2020). This type of SOC allows an organization to choose which security tasks they host internally, and which can be hosted by an external party.

2.2 Elements of a SOC

Previous studies indicate that an effective SOC consists of three crucial elements: people, processes, and technology (Onwubiko & Ouazzane, 2019; Majid & Ariffi, 2019; Chamkar, Maleh, & Gherabi, 2023). The sub-sections below discuss these three elements in depth.

2.2.1 People

The people aspect of a SOC includes incident responders and SOC managers who are responsible for continuous monitoring of an organization's systems (Onwubiko & Ouazzane, 2019). Mughal (2022) adds that for a SOC to perform optimally, it also needs vulnerability management specialists, penetration testers, and, most importantly, forensic analysts. Each member of a SOC team plays an important role in maintaining the overall security posture of the organization. Mughal (2022) describes some of these roles as follows.

Incident Responders

Incident responders investigate and respond to security incidents within a SOC. They are responsible for ensuring that the incident is contained, gathering evidence, and remediate the damage caused.

SOC Managers

The SOC manager oversees the operations of a SOC. Their responsibilities include managing the staff, developing processes, and setting performance standards.

Threat Intelligence Analysts

These analysts gather and analyze all the threat intelligence data before sharing it with the SOC team. They provide information on emerging security trends which assists the SOC team to stay ahead of evolving threats.

Vulnerability Management Specialists

Vulnerability management specialists are responsible for assessing the organization's systems for all the security gaps and ensuring that patches and updates are applied promptly to address those gaps.

Penetration Testers

The role of penetration testers in a SOC is to identify and exploit security vulnerabilities in the organization's systems. They provide a more in-depth analysis of the organization's security posture and help the SOC team to profile and identify areas for improvement.

Forensic Analysts

Forensic analysts are responsible for analyzing and interpreting data related to security incidents. They gather and preserve evidence that is used in investigating breaches or that might potentially be used during legal proceedings.

2.2.2 Processes

Another aspect of the SOC is processes. Processes in a SOC include all the standard operating procedures (SOPs) and workflows that need to be followed to investigate and classify incidents (Majid & Ariffi, 2019). Processes in a SOC help with consistency in responding to cyber threats. Additionally, having well-defined processes helps improve the efficiency of a SOC and ensures that tasks are not duplicated between different teams. There are key processes in a SOC that include:

Incident Response Plans: This plan outlines all the procedures that must be followed to detect, respond, and recover from any incidents. Additionally, this plan includes the roles and responsibilities of different teams, as well as the escalation procedures (Mughal, 2022).

Containment, eradication, and recovery plan: This plan includes short- and long-term strategies to prevent damages from spreading further within an organization. It also outlines the steps required to identify and eliminate the root cause before systems can be restored (Vielberth et al., 2020).

2.2.3 Technology

Technology includes all the security tools deployed within a SOC (Chamkar, Maleh, & Gherabi, 2021). The advancements in technology have seen an increase in the number of security tools that are now deployed in SOC environments. Below is a discussion of three of the most popular tools deployed in a SOC environment.

Security Incident and Events Management System (SIEM) - At the heart of every SOC is a SIEM, which integrates all the security tools such as firewalls, antivirus, and intrusion detection/prevention systems and generates logs and alerts for SOC analysts (Perera, Rathnayaka, Perera, Madushanka, & Senarathne, 2021). Additionally, a SIEM helps make a SOC more effective by actively performing threat hunting and threat intelligence.

Security Orchestration, Automation, and Response (SOAR) - SOAR solutions are designed to improve the efficiency and effectiveness of security teams by integrating different security tools and processes, automating repetitive tasks, and enabling faster and more informed responses to security incidents. Since processes are automated, a SOAR requires little human interaction (Mughal, 2022). SOAR platforms integrate with various security tools such as SIEM, firewalls, endpoint protection, and threat intelligence platforms. This integration allows for seamless data exchange and coordination among tools.

Endpoint Detection and Response (EDR) - Although SIEM and SOAR technologies offer integration of different security technologies, EDR focuses on identifying and responding to security threats from endpoint devices (Shweta, Adithan, & Hoeper, 2024). An EDR differs from a traditional antivirus in that it provides enhanced capabilities to monitor both known and unknown threats. EDR solutions employ behavioural analytics and machine learning techniques to detect suspicious activities (Shweta et al., 2024).

2.3 Digital Forensics (DF)

No definition of DF is universally accepted. For example, Mrdovic (2021) describes digital forensics as a branch of forensic science that focuses on analysing and investigating evidence contained in digital format. Sule (2014) adds that DF uses a combination of information systems and legal knowledge to analyse and store digital evidence in a legally acceptable manner. With the increase in crimes committed through digital means, the need for organisations to conduct digital forensic investigations has also increased. These investigations can be initiated by organizations to conduct either a criminal investigation or an internal investigation.

The literature has differing views on the number of investigative phases involved in digital forensics. For example, Mckemmish (1999) describes the phases as Evidence Identification, Preservation, Analysis, and Presentation. In 2001, the Digital Forensics Research Workshop (DFRWS) described six phases that define digital forensics as Identification, Preservation, Collection, Examination, Analysis and Presentation. Other authors (Mrdovic, 2021; Yassin, Abdollah, Ahmad, Yunos, & Ariffin, 2020) define the phases as Identification, Collection, Recovery, Analysis, and Preservation. Although there is a difference in the number of phases involved during a digital forensic investigation, the authors agree that the evidence needs to be handled in a forensically sound manner. Therefore, the need to collect evidence legally and preserve the chain of custody plays a critical role in DF.

2.4 Cloud Forensics

Cloud forensics can be defined as a cyber-crime investigation that requires gathering evidence from cloud computing platforms or services (Purnaye & Kulkarni, 2022). The investigation involves the cloud as a subject, an object, or an environment (Purnaye & Kulkarni, 2022). Other researchers describe cloud forensics as a combination of network forensics and digital forensics (Ruan, Carthy, Kechadi, & Crosbie, 2011). While the investigator controls the evidence in traditional forensics, in the cloud, the evidence is dependent on different cloud service providers (Akter, Akther, Uddin, & Islam, 2020).

Ruan et al. (2011) describe cloud forensics as a multi-dimensional issue that consists of technical, organizational, and legal dimensions. The technical dimension looks at the tools and procedures that are required to perform a forensic analysis on the cloud. These include the process of identifying and acquiring forensic data, performing live forensics and segregating the evidence between the client and cloud service provider or virtualized environments (Ruan et al., 2011). The organizational dimension involves collaboration between various cloud actors to facilitate internal and external investigations. These actors include cloud providers, cloud consumers, cloud brokers, and cloud carriers. The final dimension, legal, focuses on developing regulations and agreements to ensure that forensic activities in the cloud adhere to laws and regulations in the jurisdictions where the data resides (Ruan et al., 2011).

2.5 Internet of Things Forensics

The Internet of Things (IoT) forensics is a child domain of digital forensics whose main objective is to uncover digital evidence that can potentially be presented in a court of law or civil proceedings (Karie & Karume, 2017). The difference between the two lies in the evidence collected. DF deals with evidence found in traditional digital mediums such as personal computers, servers, and smart phones (Stoyanova, Nikoloudakis, Panagiotakis, Pallis, & Markakis, 2020). While evidence used in IoT forensic investigations is divided into three levels: *device, network, and cloud* (Stoyanova et al., 2020; Mrdovic, 2021). In device-level forensics, evidence is gathered from the local memory of the device itself (Yaqoob, Hashem, Ahmed, Kazmi, & Hong, 2019). Network-level forensics involves capturing logs from various forms of networks used in IoT, such as Personal Area Network (PAN), Body Area Network (BAN), Local Area Networks (LAN), and Wide Area Networks (WAN) (Alenezi, Atlam, Alsagri, Alassafi, & Wills, 2019; Yaqoob et al., 2019). Lastly, cloud-level forensics

deals with the IoT evidence that is stored in the cloud (Lutta, Sedky, Hassan, Jayawickrama, & Bakhtiari Bastaki, 2021).

The forensic investigation in an IoT context is carried out in a way similar to a traditional digital forensic investigation. However, due to the complex computing architecture of IoT devices, standardizing evidence collection is a challenge (Yaqoob et al., 2019; Mrdovic, 2021). Moreover, IoT devices differ in type, features, and how and where they store data (Caviglione, Wendzel, & Mazurczyk, 2017). Therefore, more contextual evidence is required for the type of IoT application or device being investigated (Zia, Liu, & Han, 2017).

2.6 Image Forensics

The increase in digital image manipulation, which is often referred to as deepfake, has necessitated the need for audio and video forensics. Image forensics investigates digital images to identify any manipulations that have been done on them (Sharma, Jha, & Dr. Bharti, 2016). Image forgery techniques are classified into two: the *active approach*, which requires prior information about the image being examined, and the *passive approach*, which analyzes the binary of the image without having any prior information about the image (Sharma et al., 2016; Kaur and Jindal, 2020). The process of performing image forensics is more cumbersome than traditional digital forensics. The process entails the following steps:

Step 1: Image Acquisition - During the image acquisition stage, the imaging sensor can introduce artifacts in the image due to irregularities in the camera imaging sensors, which are then filtered using the Colour Filter Array (Kaur & Jindal, 2020).

Step 2: Color-to-gray scale conversion - During this step, coloured images may be changed to a grayscale image to reduce computational complexities (Nabi, Kumar, Singh, Aggarwal, & Kumar, 2022).

Step 3: Block division – During this step, the resultant image from step 2 gets divided into blocks to further reduce its complexity and speed up the feature-matching process in the future (Nabi et al., 2022).

Step 4: Feature extraction - Features of the image are extracted for localization and detecting forgery, which helps in the later steps (Nabi et al., 2022).

Step 5: Feature sorting - The features extracted in step 4 are stored in a matrix to group all matching blocks using different sorting algorithms (Nabi et al., 2022).

Step 6: Feature matching - Feature matching is performed to identify similar blocks in an image and bring them closer together. Different methods like Euclidean distance, Clustering, and K-nearest neighbor (KNN) are used for this purpose (Kaur & Jindal, 2020).

Step 7: Forgery detection and localization – During this step, a score of similarities that were found during feature matching is used to locate the forged region. To improve the localization, various mathematical morphological operations are performed. These include the convolutional neural network (CNN) and robust clustering using J-linkage (Kaur & Jindal, 2020).

2.7 Digital Evidence

Traditionally, investigators collected digital evidence from computer systems such as desktops, servers, and laptops. With technology evolving, other sources of evidence such as cloud computing environments, IoT devices, and mobile devices have become more common (Purnaye & Kulkarni, 2022). For digital evidence to be accepted as valid, a chain of custody must be maintained specifying who encountered the evidence in every step of the investigation, needs to be kept (Mrdovic, 2021). Additionally, to maintain the integrity of the chain of custody and digital evidence, proper documentation is required. Yan, Shen, Cao, & Dong (2020) define chain of custody as a process to maintain a chronological history of how digital evidence has been handled. In addition to the chain of custody, digital evidence should be extracted and analysed in a forensically sound manner. The term forensically sound is widely used in the digital forensics community to justify the use of a particular methodology or technology over the other (Sachowski, 2019).

Digital evidence for forensic purposes can either be captured and analysed postmortem or live. Analysing postmortem digital evidence requires turning off the device to inspect its contents (Chan, Venkataraman, David, Chaugule, & Campbell, 2010). The primary focus of this method is to recover and analyse data stored on the hard drive while eliminating the risk of the same data being altered (Chan et al., 2010). The challenge with this method, however, is that volatile data are lost as soon as the device is shut down. Additionally, breaking down network connections to retrieve evidence could lead to possible disruptions of critical systems (Chan et al., 2010).

While postmortem forensics deals with the analysis of evidence from a device that is powered off, live forensics involves capturing and analysing the evidence on a device that has not been shut down before the investigation. While this method ensures that volatile data is not lost during analysis, it runs the risk that an investigator will alter the evidence.

2.7.1 Admissibility of Digital Evidence

Evidence collected from digital devices can end up in a court of law; therefore, investigators need to exercise proper care when collecting such evidence. In 1993, the United States Supreme Court handed down a landmark ruling on the case of *Daubert v. Merrel Dow Pharmaceuticals Incorporation* regarding the admissibility of scientific evidence in a court of law (Cappellino, 2022). In what has now become known as the Daubert standard, judges found that any expert giving scientific evidence in a court of law should be qualified to give such testimony and such testimony must meet the following criteria: *a) whether the theory or technique in question can be tested, b) whether the theory or technique has been subject to peer review, c) the known error rate of the theory or technique, d) the existence and maintenance of standards controlling its operation, e) whether the theory or technique has been widely accepted in the scientific community* (Cappellino, 2022). This standard has also been widely adopted in digital forensics.

2.8 Digital Forensic Readiness (DFR)

DFR offers a proactive approach to digital forensics in anticipation of a breach eventually occurring. According to Daneilsson and Tjostheim (2004), DFR is a discipline within digital forensics that increases the availability and quality of raw data needed to perform an investigation postmortem. The concept of DFR was introduced by John Tan in 2001. Tan (2001) breaks down the DFR into two objectives: a) to maximize the ability of the environment to collect credible digital evidence, and b) to minimize the cost of forensic investigation during incident response. This definition is further echoed in Rowlingson (2004, p5) who defines DFR as 'the ability of an organisation to maximise its potential to use digital evidence while minimizing the costs of an investigation'.

Sachowski (2019) outlines the following five objectives that DFR achieves: a*) gathering evidence in a legal manner without any business disruptions, b) gathering required evidence to show how incidents impact business risks, c) ability to conduct investigation at a cost lower than the cost of the incident, d) minimize business disruptions, and e) ensure evidence produced for legal proceedings results in positive outcomes*.

2.8.1 Cloud Forensics Readiness

Advancements in technology, such as the increased use of the cloud and the Internet of Things (IoT), have created a need for cloud forensics readiness (CFR). The objectives of CFR are similar to those

already discussed for DFR. However, with CFR, the focus is on reducing costs by preparing information that might be required for performing a forensic investigation in a cloud environment (Alenezi, Hussein, Walters, & Wills, 2017).

2.8.2 Cost and benefits of Forensic Readiness

The cost of forensic readiness for an organization should be informed by performing a risk assessment first. Through a risk assessment, an organization can see if it will get a return on investment (ROI) by proactively preparing for incident occurrences. The benefits of a forensic readiness plan should therefore outweigh the cost of implementing it (Sachowski, 2019). Sachowski (2019) also outlines the five factors that have a direct influence on the cost of implementing a forensic readiness program.

(i) *Maintaining governance documents*- includes constantly reviewing the security standards, policies, and procedures.

(ii) *Awareness training* – this involves continuously training non-technical and technical staff on security.

(iii) *Incident management* – involves the ability to identify, analyse and mitigate potential risks.

(iv) *Data security* - includes the ability of an organization to gather information systematically and preserve it securely.

(v) *Legal counsel* - Legal counsel provides assurances that methodologies and tools used during an investigation can stand legal scrutiny.

Rowlingson (2004) provides several benefits associated with having a forensic readiness plan. Among the benefits is the ability of an organization to conduct internal investigations at a reduced cost. Additionally, having a forensic readiness plan in place enables organizations to investigate a major incident efficiently and rapidly with minimal disruptions to business. Karie and Karume (2017) add that being digitally forensic-ready provides a tool for organizations to fight insider threats and may deter employees from not complying with organizational rules.

2.9 DFR Frameworks

Various frameworks have been developed for DFR in various contexts and industries. This section discusses four of these frameworks that formed the basis of the proposed conceptual model. These

are the *a) Homogeneous, Answerable and Unified Strategy (HAUS) Forensic Readiness Model, b) DFR Framework for Nigerian Banks, c) DFR Framework for IoT-enabled Organizations, and d) DFR for Cybersecurity Practitioners.*

2.9.1 Homogeneous, Answerable and Unified Strategy (HAUS) Forensic Readiness Model

Collie (2018) developed a HAUS Forensic Readiness model that is mainly driven by management and implemented by staff. The model emphasizes the need for all staff, both technical and nontechnical, to be involved in the DFR process. Collie (2018) argues that staff must prepare and know what to do in the event of a digital incident. The participation of staff, particularly non-technical staff, is encouraged by giving inputs to the Aware, Alert, and Always-On (AAA) cycle (Collie, 2018). The AAA cycle encourages staff to participate in the following: i) protection of the assets; ii) identifying a problem and knowing the reporting channels; iii) gathering information such as how data can be compromised; and finally, iv) being able to review all the information at hand.

As depicted in Figure 1, the HAUS model proposes a AAA cycle for each department in an organisation. The model further proposes a chain of command, where staff reporting structures are defined (Collie, 2018). The model proposes that information and input should flow both ways, from management to staff and from staff to management.

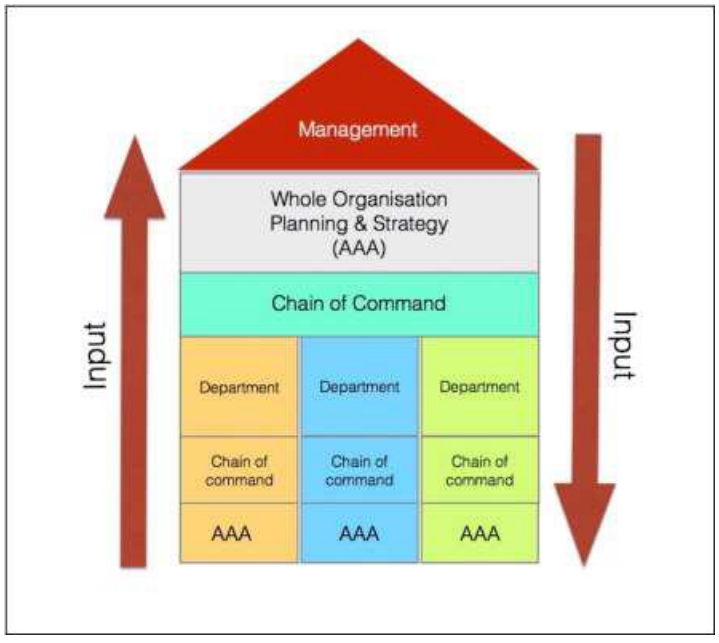

Figure 1: HAUS Forensic Readiness Model

Source: Collie (2018)

Although the HAUS readiness model places emphasis on the people and processes aspects, it is mute on the technology aspect. The model does not address the forensic tools that are necessary for an organization to be forensically ready. Furthermore, the model does not address the legal and regulatory challenges that often accompany forensic investigations.

2.9.2 Digital Forensic Readiness Framework for Nigerian Banks

Garba and Bade (2019) developed a DFR framework for Nigerian Banks that covers seven components, namely: *Strategy, policies and procedures, people, training, system and events, monitoring and reporting, and risk assessment*. The framework is driven by the system and events component, which focuses on all the potential policies and technologies that may be incorporated into the DFR strategy. This component also identifies potential sources of evidence, such as firewalls and network devices.

Although the model highlights the importance of having personnel within the banking sector who perform DF investigations, it does not elaborate on the tools that these personnel will have to use to do so. Integration of forensic tools with existing security tools within banks is also not discussed. Furthermore, given the strict compliance that banks need to follow, the model does not address any specific legal and regulatory requirements for DFR in Nigeria.

2.9.3 DFR Framework for IoT-enabled Organizations

Kebande et al. (2020) developed a holistic DFR framework focused on organizations with IoT. The framework is based on the ISO/IEC 27043 standard, which is and international standard that seeks to provide a formal method of conducting DFR. The standard is defined by four readiness process groups within the ISO/IEC 27043 standard, namely *planning, implementation, assessment, and concurrent processes* (Kebande et al., 2020).

Figure 2 below is a depiction of the four process groups. The planning process group defines how the forensic evidence will be collected, stored, analysed, and presented before the incident occurs. The planning process group also identifies the actions required when an incident is detected. Additionally, this process group ensures that the DFR process identifies and considers all legal requirements and business-specific requirements (Kebande et al., 2020).

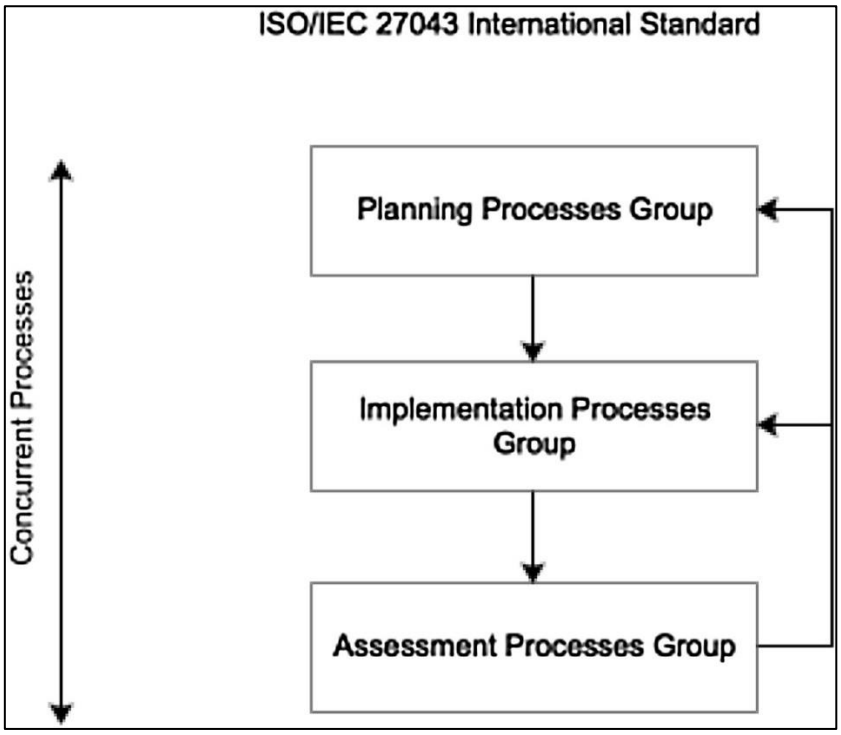

Figure 2: ISO/IEC 27043 standard

Source: Kebande et al. (2020)

During the implementation process, the system architecture process is implemented. Furthermore, all systems and policies that will be used to collect forensic evidence are installed. These systems range from incident logging systems, and systems that track any changes in software and hardware across the organization (Kebande et al., 2020).

In the assessment process group, the results of the implementation process group are compared with the objectives that were set out for achieving DFR. The results of the assessment are used to enhance the overall DFR process. Furthermore, compliance with legal requirements and the DF principles of various jurisdictions to ensure the admissibility of digital evidence in a court of law is also assessed (Kebande et al., 2020).

The final group, concurrent processes do not occur in any order, they happen alongside the digital investigation processes. Although concurrent processes do not occur in any order, they apply to other processes in the digital investigation process (Kebande et al., 2020).

Kebande et al. (2020) focus their framework on the planning and implementation processes of the ISO standard. The framework replaces these processes with organizational, readiness, and IoT security processes. Figure 3 below shows the proposed framework. Organizational processes ensure

that there is consistency in the application of IoT DFR in an organization. The organizational processes further emphasise the need for management participation to ensure compliance with relevant legal and regulatory requirements (Kebande et al., 2020). Kebande et al. (2020) also include the establishment of a DF strategy and DF policy, scenario definitions, definition of roles, responsibilities, and training requirements, as part of the organization processes.

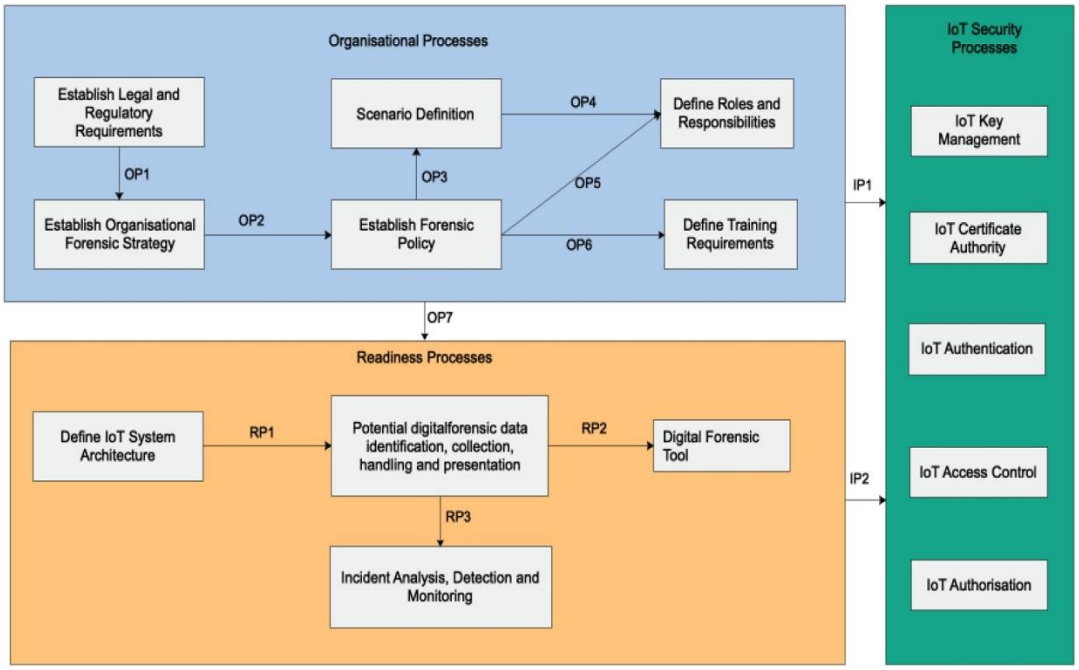

Figure 3: IoT DFR Framework

Source: Kebande et al. (2020)

The readiness processes, which are the second processes added by Kebande et al. (2020), ensure that all potential data that are relevant to DF are identified, collected, and handled accordingly. Kebande et al. (2020) suggest first defining the architecture of an organization's IoT system. The architecture of the IoT system is made up of all endpoint devices, software, the network, and data. It assists in identifying all key data sources across the organization. In addition, Kebande et al. (2020) emphasise the importance of deploying IoT forensic tools that are compatible with the IoT environment.

The third group of processes discussed in the framework focuses on IoT security. These processes ensure that the security of both the IoT and the potential DF data is maintained throughout the data lifecycle. However, the authors concede that traditional security mechanisms are not possible with IoT devices due to their low computational memory (Kebande et al., 2020).

Through the framework, the authors highlight six factors that are required for an organisation to be forensically ready. These factors include *management buy-in, legal and regulatory requirements, digital forensic policy, clearly defined roles for non-technical and technical stakeholders, training requirements, and appropriate forensic tools for evidence gathering* (Kebande et al., 2020). The

framework falls short of what this study aims to achieve as it only focuses on DFR for organizations running IoT environments.

2.9.4 DFR for Cybersecurity Practitioners

Zainudin et al. (2022) developed a DFR framework aimed at assisting cybersecurity specialists to be forensically ready. The framework integrates the psychological factors found in the Technology Readiness Index (TRI) with the DFR factors. The authors argue that having cybersecurity specialists who are mentally ready to adopt new technologies better prepares them for forensic incidents. DFR for cybersecurity practitioners uses TRI to measure cybersecurity personnel's mental preparedness and resilience to challenges they may face during the investigation (Zainudin et al., 2022). Parasuraman (2000) developed the 36-item TRI framework to measure an individual's propensity to embrace and use new technologies. In 2014, TRI 2.0 was introduced, which streamlined the 36 items to 16 (Parasuraman & Colby, 2015).

The framework developed by Zainudin et al. (2022) focused on only four items in TRI 2.0 which are: (i) *Optimism- measures the positive view of cybersecurity specialists in relation to a forensic investigation, (ii)Innovativeness – which measures the specialists' eagerness to learn new DF technologies, (iii) Discomfort – measures the specialists' perception of being overwhelmed or having a lack of control over DF technologies, and (iv) Insecurity – this is a concern about the ability of DF technologies to work properly* (Zainudin et al., 2022).

Although the framework includes other DFR factors, it places more emphasis on people, which in this case refers to cybersecurity specialists, and their propensity to accept new forensic tools. However, the framework does not give a practical demonstration of how the TRI will be integrated with the DF factors. Therefore, this study considered the framework inadequate to address the objectives of this study.

Table 1 below shows the comparison of components in the frameworks discussed. From the reviewed literature, it is evident that researchers use different naming conventions for components of DFR. For example, what Collie (2018) and Kebande et al. (2020) term technical and non-technical stakeholders, Garba & Bade (2019) and Zainudin et al., (2022) refer to as people.

Table 1: Frameworks Comparison

Framework	Digital Forensic Readiness Components						
	Management Support	**Policies and Procedures**	**Legal and Regulatory Requirements**	**Forensic tools**	**Technical Skills**	**Training**	**Non-Technical Factors**
Collie (2018)	X						X
Garba and Bade (2019)		X			X	X	
Kebande et al. (2020)	X	X	X	X	X	X	X
Zainudin et al. (2022)	X		X	X	X	X	

Based on the comparison of the frameworks, the following common constructs were identified: *management support, policies and procedures, legal and regulatory requirements, forensic tools, technical skills, training, and non-technical factors.* Each of these constructs will be discussed and summarized below:

A. Management support

The successful implementation and organizational adoption of a DFR strategy depends on the support received from top management. Top management must understand the importance of being forensically ready and lead the implementation thereof. The top management should make funds available for different activities that are required for DFR to be successfully implemented (Zainudin et al., 2022). Additionally, top management should ensure the recruitment of skilled and capable personnel who can effectively implement the DFR strategy. The critical role that management plays in the successful implementation and integration of digital forensics tactics inside a business is covered by Johansen (2017). It highlights how important senior management support is for allocating resources and gaining organizational buy-in (Johansen, 2017).

B. Training

According to Sachowski (2019) conducting awareness training plays a critical role in educating different stakeholders about their roles during an incident. Kebande et al. (2020) suggest clearly defining roles and responsibilities for different stakeholders and making training proactive. This view is further expanded in Rowlingson (2004) by listing group of employees that should be mostly targeted for awareness training. Rowlingson (2004) further adds that training staff to know their roles during an incident response helps to eliminate confusion and reduce the chances of evidence being tainted. Johansen (2017) also stresses the importance of comprehensive staff training involved in digital forensics and incident response. He highlights how training ensures that personnel are equipped with the skills and knowledge needed to effectively execute a DFR strategy (Johansen, 2017).

C. Technical skills

Technical skills describe all technical aspects that affect the DFR plan of an organization (Zainudin et al., 2022). This includes the technical proficiency of the personnel tasked with performing digital forensics. For a DFR plan to succeed, a team of technical experts in performing digital forensics investigations is important (Johansen, 2017).

D. Forensic tools

Forensic tools that are fit for purpose help organizations perform a full-scale investigation Kebande et al. (2020) state the importance of defining the system architecture of an organisation to identify potential data sources. Evidence collected from these data sources should be time-stamped to allow correlation between different sources. Thus, it is important to use sound forensic tools to ensure the integrity of the evidence collected.

E. Legal and Regulatory Requirements

Legal and regulatory requirements should be established and complied with based on the industry in which an organisation operates (Kebande et al., 2020). Additionally, gathering of evidence should be done in compliance with the jurisdiction of the investigation. For example, the United States of America (USA) and Canada use the Federal Rules of Civil Procedure (FRCP) law for the electronic discovery of evidence (Sachowski, 2019). According to FRCP, digital evidence should be provided quickly and in a forensically sound manner.

F. Policies and Processes

Rowlingson (2004) proposes having a policy in place for securely storing evidence and handling potential evidence. The policy should be developed by the top management and supported by the entire organization (Kebande et al., 2020). Having such a policy in place will ensure the authenticity and integrity of digital evidence as it travels through different custodians. In addition to policies, there must also be clearly defined processes for staff to follow. Kebande et al. (2020) add that having proper processes in place ensures management buy-in and commitment to the implementation of DFR.

2.10 Gaps in Literature

The previous sections show that there is no standardization of DFR frameworks. The frameworks discussed show several different scenarios and environments where DFR can be deployed. For example, Collie (2018) proposed a generic framework that places more emphasis on people in an organization. Garba and Bade (2019) developed a framework for banks in Nigeria. The framework by (Kebande et al., 2020) focuses on implementing DFR in an IoT environment. While a framework by Zainudin et al. (2022) focuses on cybersecurity practitioners. Research conducted on the development of DFR frameworks does not consider the complexity of a SOC environment. Furthermore, the discussed frameworks are silent on how emerging technology trends, and cybersecurity tools, can be incorporated into existing forensic technologies to prepare a SOC to be forensically ready, particularly from a South African context.

2.11 Proposed Conceptual Model

This section highlights the proposed conceptual model based on the reviewed literature. The conceptual model draws from the frameworks analysed in section 2.9. The proposed conceptual model highlights the requirements that a SOC needs to fulfil for it to be forensically ready. SOC operations are technical in nature, which require technical proficiency of the personnel, knowledge of various tools, and continuous training. Although SOC operations are technical, other non-technical factors are required to have a holistic conceptual model. These non-technical factors include management support, policies, processes, and procedure, and the being familiar with legal requirements in different jurisdictions. Therefore, this conceptual model proposes infusing both technical and non-technical aspects of DFR. The proposed conceptual model is represented in Figure 4 below.

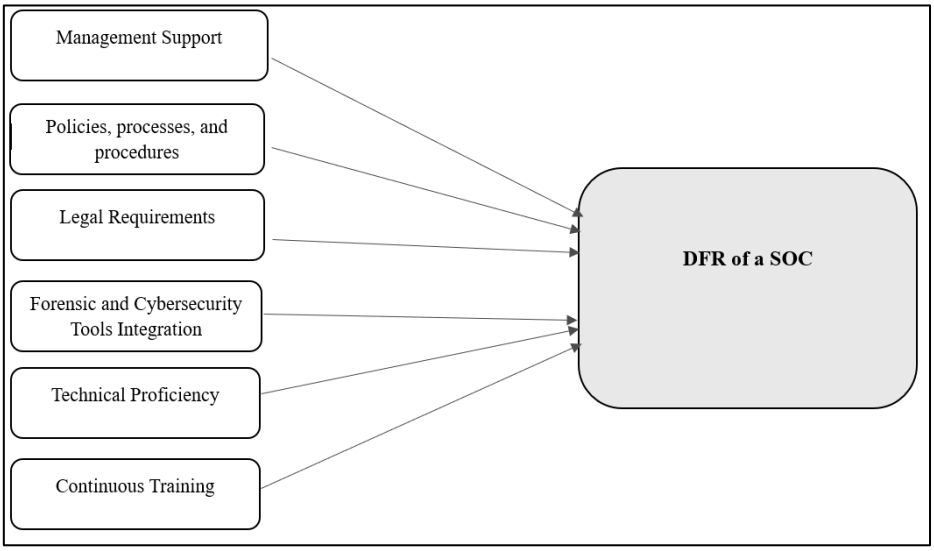

Figure 4: Proposed conceptual model

The conceptual model summarizes the relationships that exist between the constructs and the DFR of a SOC. Good management support leads to the improved DFR of SOC. The conceptual model also shows that having policies, processes and procedures in place also enhances the DFR of a SOC. The provision of appropriate legal requirements also improves the DFR of SOC. According to the model, forensic and cybersecurity tools integration also have a significantly positive impact on the DFR of SOC. The conceptual model also supposes that technical skills and continuous training also have a positive influence on DFR of SOC.

2.11.1 Definition of Constructs and Hypothesis

Table 2 gives a summary of the constructs that make up the conceptual model.

Table 2: Definition of Constructs

Construct	Definition	Reference
Management Support	This defines the level of involvement by top management in supporting DFR initiatives.	Rowlingson (2004) Collie (2018)
Policies, Processes and Procedures	These define all the policies and guidelines that forensic investigators need to follow	Garba and Bade (2019); Kebande et al. (2020)

	to ensure integrity of evidence collected.	
Legal and Regulatory Requirements	These are all the legal and regulatory frameworks that govern how a DF investigation should be conducted within a specified jurisdiction.	Kebande et al. (2020)
Forensic and cybersecurity tools	These refer to all the technologies that are used to extract evidence from all potential sources of evidence.	Kebande et al. (2020)
Technical Skills	These are the skills and expertise required for DF investigators to conduct investigations.	Zainudin et al. (2022)
Training	This refers to awareness training for all staff members, as well as forensic training aimed technical staff.	Kebande et al. (2020) Dilijonaite (2017)

The constructs of the proposed conceptual model are discussed in detail below:

Management support

Top management play a crucial role in the development and implementation of a forensic strategy. Rowlingson (2004) suggests having senior management support when implementing a DFR programme. All activities that need to be funded, such as technologies to be used and training, need to be supported by management. Additionally, all the policies and processes that SOC analysts must implement need to be supported by the top management level.

Policies, Processes, and Procedures

Policies and processes refer to guidelines that must be followed in response to incidents. Clearly defined DFR policies can give an organization the ability to gather and review digital evidence internally (Githinji, 2021). Internationally, policy guidelines have been developed that organisations can use for their DFR plan. For example, the National Institute of Standards and Technology (NIST) developed a four-step guide for integrating digital forensics into incident response (NIST, 2006).

One of the standard recommendations is the development of forensic capability by organizations. The International Organization for Standards (ISO) and the International Electrotechnical Commission (IEC) also developed a standard, ISO 27043: 2015, which provides generic guidelines on how DFR can be implemented in an organisation (ISO, 2015).

At the national level, the United Kingdom (UK) made the DFR policy mandatory in 2008 for all government departments through the Her Majesty's Government (HMG) Security Policy Framework (Park et al., 2018). In Germany, Bundesamt fuer Sicherheit in der Information stechnik (*Federal Agency for Security of Information Technology*) (BSI) developed DFR guidelines, which it divided into strategic and operational readiness. For SOC analysts to follow and implement set policies and processes, they need to be first aware and understand the value of having a forensic readiness policy in place.

Legal and Regulatory Requirements

SOC forensic investigators operating in South Africa need to familiarize themselves with the different legal and regulatory requirements of the country. South Africa has seen a significant improvement in the legislation and regulations that have been introduced to combat cybercrime and protect consumers from data breaches. Some of these regulatory frameworks are discussed below:

Protection of Personal and Information Act (POPIA) – POPIA gives clear directions on how personal data in the hands of organizations should be handled and protected. The act stipulates that any personal information collected by the responsible party should be kept secure through appropriate, reasonable, organisational, and technical measures to protect against security breaches (Adams et al., 2021). In terms of transferring personal data to a different jurisdiction, the act stipulates that measures must be taken to ensure that the foreign country with which personal information is being shared or transferred has as high a level of data protection as offered under POPIA. The act further outlines timelines for an organization to report any breaches and penalties that can be imposed against organizations if personal data is leaked (Adams et al., 2021).

Cybercrime Act (SA, 2021) – The South African Cybercrime Act came into effect in 2021 and defines all activities that relate to the unlawful use of computer systems. The most notable activities that are covered by the act include hacking, extortion, which is commonly referred to as ransomware, and cyber fraud, which includes phishing and spoofing attacks (Snail ka Mtuze & Musoni, 2023). The act is still in its infancy, as a result, some of its provisions, such as dealing with requests from jurisdictions outside of South Africa, are not yet in effect.

In addition to South African legislation, SOC forensic investigators must also consider regulatory requirements in other countries with which their organizations might be doing business. For example, the 2014 African Union Convention on Cybersecurity and Personal Data Privacy (Malabo Convention) sought to establish a continent-wide framework that ensures uniformity in data protection policies across the continent. Furthermore, the convention sought to make cooperation between law enforcement agencies in different member states easier (Snail ka Mtuze & Musoni, 2023). In Europe, the General Data Protection Regulation (GDPR) provides guidelines on how personal data should be handled and protected (Stoyanova et al., 2020). GDPR was designed to harmonize privacy laws across Europe and offer protection and privacy to individual data. According to GDPR, any entity that has data stored within European countries must comply with these prescripts.

Forensic and Cybersecurity Technologies

Research has shown that technology has evolved, and digital evidence no longer resides solely on traditional devices such as personal computers and servers (Purnaye & Kulkarni, 2022). Other potential sources of evidence such as the cloud and mobile devices should also be taken into consideration (Sachowski, 2019). In addition, the cybersecurity technologies used within a SOC have evolved and can retain evidence that can help speed up the investigative process. Forensic analysts in a SOC environment need to have appropriate and up-to-date tools to extract digital evidence from any potential data sources in a forensically sound manner.

Technical Skills

A successful DFR plan depends on the skills and expertise of the personnel tasked with handling investigations. Dilijonaite (2017) suggests that every organization needs to be equipped with the following five roles to prepare for an investigation: a) *first responder* – responsible for securing the evidence and ensuring that forensically sound procedures are followed, *b) forensic specialist* – responsible for the identification and collection of evidence, *c) forensic analyst* – responsible for the analysis of digital evidence from all identified sources, *d) lead investigator* – they are responsible for

coordinating all investigation activities and interpreting the findings from the analysis, and *e) data retention specialist* – ensures safe keeping of evidence. Therefore, SOC personnel need to have the relevant skills and expertise required for forensic investigations.

Training

The literature has shown the importance of awareness training for all stakeholders (Rowlingson, 2004). For the DFR plan to be successful, everyone in an organisation must be aware of its importance and the benefits it brings. Additionally, the SOC personnel responsible for forensic investigations also need to receive proper training to allow them to conduct the investigations successfully.

2.11.2 Hypothesis Development

The following propositions are derived from the literature and based on the developed conceptual model.

The successful implementation and organizational adoption of a DFR strategy depend on the support received from top management. It is critical that top management understands the importance of being forensically ready and leads its execution. Top management should make funds available for different activities that are required for DFR to be successfully implemented (Zainudin et al., 2022). Additionally, top management should ensure the recruitment of skilled and capable personnel. The following hypothesis is thus put forward:

H_1: *Management support in various DFR initiatives has a significantly positive influence on facilitating the forensic readiness of a SOC.*

Rowlingson (2004) proposes having a policy in place for securely storing evidence and handling potential evidence. The policy should be developed by the top management and supported by the entire organization (Kebande et al., 2020). Having such a policy in place within a SOC will ensure the authenticity and integrity of digital evidence as it traverses different custodians. In addition to policies, there must also be clearly defined processes for staff to follow. Kebande et al. (2020) adds that having proper processes in place ensures management buy-in and commitment to the implementation of DFR. Therefore, the following hypothesis is put forward:

H_2: *The availability of well-defined* p*olicies, processes, and procedures has a significantly positive influence on the ability of a SOC to be forensically ready.*

Forensic investigators within a SOC environment in South Africa need to familiarize themselves with the different legal and regulatory requirements of the country. For example, the Protection of Personal and Information Act (POPIA) gives clear directions on how personal data in the hands of organizations should be handled and protected. The act also specifies penalties that can be meted against organizations in the event of personal data being leaked (Adams et al., 2021). Thus, the following hypothesis is proposed:

H_3: *Knowledge of various legislative frameworks has a significantly positive influence on facilitating the data forensic readiness of a SOC.*

Research has shown that technology has evolved, and that digital evidence no longer solely resides on traditional devices such as personal computers and servers (Purnaye & Kulkarni, 2022). Other potential sources of evidence such as the cloud and mobile devices should also be taken into consideration (Sachowski, 2019). Moreover, security technologies within a SOC environment can collect logs that can be used during an investigation. Forensic analysts in a SOC environment need to have appropriate and up-to-date tools to extract digital evidence from any potential data sources in a forensically sound manner. Therefore, the following hypothesis is proposed:

H_4: *Integration of forensic and cybersecurity technologies has a significantly positive influence on the digital forensic readiness of a SOC.*

A successful DFR plan depends on the skills and expertise of the personnel tasked with handling investigations. SOC analysts therefore need to have the relevant skills and expertise required for forensic investigations. Therefore, the following hypothesis is proposed:

H_5: *The availability of technically proficient personnel has a significantly positive influence on enhancing the forensic readiness of a SOC.*

Literature has shown the importance of awareness training for all stakeholders. For the DFR plan to be successful, everyone in an organisation must be aware of its importance and the benefits it brings. Additionally, forensic analysts in SOC environments need to constantly upskill themselves to stay abreast of developments in the field. Thus, the following hypothesis is proposed:

H_6*: Continuous training on the importance of being forensically ready has a significantly positive influence on enhancing the forensic readiness of a SOC.*

Table 3 below summarizes the discussed hypotheses.

Table 3: Research Hypotheses

Hypotheses	***Description***
H_1	*Management support in various DFR initiatives has a significantly positive influence on facilitating the forensic readiness of a SOC.*
H_2	*The availability of well-defined* p*olicies, processes, and procedures has a significantly positive influence on the ability of a SOC to be forensically ready.*
H_3	*Knowledge of various legislative frameworks has a significantly positive influence on facilitating the* data *forensic readiness of a SOC.*
H_4	*Integration of forensic and security technologies has a significantly positive influence on the d*ata *forensic readiness of a SOC.*
H_5	*The availability of technically proficient personnel has a significantly positive influence on enhancing the data forensic readiness of a SOC.*
H_6	*Continuous training on the importance of being forensically ready has a significantly positive influence on enhancing the forensic readiness of a SOC.*

2.12 Chapter Summary

The literature review chapter highlighted the importance of a SOC as one of the defence mechanisms for fighting cybercrime. The chapter highlighted the three elements that are important for the success of a SOC. These are people, processes, and technology. The literature review also explored how digital forensics has evolved to embrace new technological developments such as cloud computing, IoT, and the manipulation of images. It should be noted that although both a SOC and a DFR include people, processes, and technology, their application is different.

This chapter further outlined the research hypotheses. First, the chapter evaluated and critiqued four existing DFR frameworks which then led to the foundation for the development of the proposed conceptual model. In this chapter, a summary of the proposed conceptual model that incorporates the

hypotheses was also presented. The next chapter will discuss the methodology of the research followed by an analysis of data.

CHAPTER 3:

RESEARCH METHODOLOGY

This section discusses the research methodology that was used for the study. Research methodology described the methods of investigation used by the researcher to conduct the study.

3.1 Research Philosophy

Research philosophy is defined as 'a system of beliefs and assumptions about the development of knowledge' (Saunders, Lewis, & Thornhill, 2019, p.130). The way social science researchers view, and study social phenomena is shaped by two fundamental sets of philosophical assumptions: ontological assumptions and epistemological assumptions (Burrell & Morgan, 2017). The following subsections define the ontological and epistemological assumptions.

3.1.1 Ontology

Ontological assumptions define how one views the world or reality and what makes something real (Bhattacherjee, 2012). These assumptions shape how one studies research objects and can be objective or subjective (Saunders et al., 2019) . The objective ontological stance suggests that reality exists independent of social actors and that their interpretations and experiences do not influence the existence of the social world (Saunders et al., 2019). On the contrary, the subjective ontological position holds that reality is relative according to an individual who experiences it and that no one true reality exists (Moon & Blackman, 2014).

The study seeks to determine the factors that influence digital forensic readiness in a SOC context by examining existing DFR frameworks. This information exists independent of social actors within organizations that SOCs. Thus, an objective ontological position was taken to conduct this study, since the knowledge already exists and can be used to draw generalizations (Saunders et al., 2019).

3.1.2 Epistemology

Epistemological assumptions deal with the best way to investigate the world and its reality. It is how we differentiate between justified beliefs and opinions (Bhattacherjee, 2012). There are two main epistemological positions, positivism and constructivism. Positivists believe that the world can be best studied through objective observations and that reality is consistent and independent of

perception (Muijis, 2011). Constructivists contrast this with the belief that reality does not exist by itself, it is created by people. This study adopted the positivist approach. This approach was chosen since the researcher intends to conduct this study objectively and minimize their participation in the research process (Muijis, 2011).

3.2 Research Approach

There are two main research approaches to developing theory: inductive and deductive reasoning. Inductive reasoning builds theoretical concepts from observed data (Bhattacherjee, 2012). On the contrary, deductive reasoning tests concepts and patterns that are known from theory using new empirical data (Bhattacherjee, 2012).

This study followed a deductive approach since it used existing theories to develop a conceptual model. Furthermore, the study tests the hypotheses derived from the conceptual model to draw valid conclusions.

3.3 Research Strategy

Saunders et al. (2019) list the following as the most common research strategies used: *Experiments, Surveys, Archival and documentary research, Case studies, Ethnography, Action Research, Grounded Theory, and Narrative Inquiry*. The choice of which research strategy to use is guided by, among others, the research approach, the amount of time available to conduct the research, and access to participants (Saunders et al., 2019). Therefore, the research strategy selected for this study was a survey as it relates to the deductive approach and allows standardized data to be collected from participants (Saunders et al., 2019). The data collection technique used for the survey was a questionnaire. Survey questionnaires ensure that data is collected without engaging directly with participants, which is in line with the ontological and epistemological assumptions of this study.

3.4 Time Frame

Research time frames can be either cross-sectional or longitudinal. A cross-sectional study allows a phenomenon to be studied at a particular time, while longitudinal studies study a phenomenon over time (Saunders et al., 2019). This study used a cross-sectional time frame. This is informed by the duration of the master's program, which is two years.

3.5 Instrument Design

The research instrument used for this study was an online survey questionnaire distributed to all participants. The questionnaire was structured, which allowed respondents to select responses from a set of given choices (Bhattacharjee, 2012). Section A of the questionnaire focused on the demographics of the respondents. Section B focused on the management support for DFR initiatives. Section C looked at the policies, processes, and procedures. Section D measured the legal requirements in different jurisdictions. Section E measured the DF technologies. Section F focused on the technical skills related to DF. Finally, Section G measured the DF training of SOC analysts.

For Section A, the study measured the responses of participants using a categorical scale. A categorical scale has two or more categories with no intrinsic ordering. For example, answers that require yes or no responses. Section B measured the responses using a Likert scale. Developed in the 1930s by Rensis Likert, this scale measures the responses based on the extent the respondents agree or disagree with a statement (Chyung, Swanson, Roberts, & Hankinson, 2018). Sections B, C, D, E, F, and G measured the responses using a combination of categorical and Likert scales. The questionnaire measured all the constructs in the conceptual model proposed. The tool that was used to develop the questionnaire is Google Forms.

Table **4** below summarises the research design instrument.

Table 4: Research instrument design summary

Construct	**Data Type**
Section A: Demographics	Categorical scale
Section B: Management Support	Some questions were measured on a categorical scale, while others on a Likert scale
Section C: Policies, processes, and procedures	Some questions were measured on a categorical scale, while others on a Likert scale
Section D: Legal requirements	Some questions were measured on a categorical scale, while others on a Likert scale
Section E: Forensic and cybersecurity Technologies	Some questions were measured on a categorical scale, while others on a Likert scale
Section F: Technical Skills	Some questions were measured on a categorical scale, while others on a Likert scale
Section G: Training	Some questions were measured on a categorical scale, while others on a Likert scale

3.6 Population and Sample Size

This section discusses the target population and the sample size that was used to conduct the study. A population in research refers to an entire group from which information is required (Banerjee & Chaudhury, 2010).

3.6.1 Target Population

A target population in research refers to the population from which the sample of the study has been selected (Banerjee & Chaudhury, 2010). The targeted population for this study was SOC analysts, cybersecurity managers, Information Technology (IT) security managers, Chief Information Officers (CIO) and Chief Information Security Officers (CISOs) within organizations that run SOCs in South Africa. The Council for Scientific and Industrial Research (CSIR) estimates that the cost of cybercrime in South Africa is estimated to reach 2.2 billion rands per annum (Moyo, 2024). Furthermore, it is reported that on average, 150 data breaches are recorded monthly by the South African Information Regulator (Moyo, 2024). For this reason, South African professionals within a SOC environment were chosen as they are responsible for securing an organization's IT infrastructure. Additionally, these professionals are the first point of contact for any forensic investigation that needs to be conducted.

3.6.2 Sampling

Saunders et al. (2019) refer to sampling as a technique that allows the collection of data from a subgroup instead of the entire population. There are two types of sampling: probability and nonprobability sampling. With probability sampling, the chances of each case being selected from a target population are known, while with nonprobability sampling the chance of each case being selected from a target population is not known.

Probability sampling has four main techniques: *simple random, systematic random, stratified random, and cluster sampling.* This study was conducted using stratified random sampling. The technique allows the population to be divided into a series of relevant strata, making the population more likely to be representative (Saunders et al., 2019). The selected population for this study comprises professionals who have different decision-making powers. As a result, the target population was divided into top/middle-level managers and SOC analysts. Selecting a random sample from each stratum ensures that the study is free of bias and that each group is fairly represented.

Although a sample size of thirty is recommended, this study aimed for a minimum sample size of seventy (Saunders et al., 2019). The number of organizations that are running SOC environments in South Africa is not known to the researcher, which affected the sample frame. As a result, the minimum sample size of seventy was deemed sufficient for the study.

3.7 Data Collection

Data for this study were collected using a survey questionnaire. Although there are other data collection methods, such as interviews and observation, a questionnaire was considered more appropriate, as it is normally used in studies employing a survey strategy. Furthermore, questionnaires allow data to be collected from respondents in a standardized manner (Saunders et al., 2019). The questions were closed-ended to allow uniformity in responses, which are easier to compare. The study participants were identified through social media platforms such as LinkedIn, where professionals in the field can be accessed. Other social media platforms, such as Facebook and Twitter, were also used to identify participants. Additionally, referrals from other professionals in the field were also used to identify participants.

3.8 Data Analysis

Data collected from respondents were analysed using quantitative methods. The study used Statistical Package for the Social Sciences (SPSS), which is a quantitative data analysis tool, to interpret and analyse the collected data. The data was first cleaned using Microsoft Excel before being analysed using SPSS. The data was analysed using descriptive and inferential statistics.

The descriptive statistics summarizes data in an organized manner by describing the relationship between variables in a sample or population. Descriptive statistics uses measures of tendency (such as mean, median, mode) and measures of variability (such as range and standard deviation) to present data in a meaningful manner (Fisher & Marshall, 2009). The use of descriptive statistics enabled the computation of the average perception of DF analysts on factors affecting forensic readiness in a SOC.

Inferential statistics compare two or more samples and infer conclusions about a larger population based on the sample (Marshall & Jonker, 2011). These statistics typically include correlations, regression analysis, confidence levels, analysis of variance (ANOVA), and hypotheses testing (Marshall & Jonker, 2011). Using inferential statistics, the researcher was able to answer the study research questions.

The normality test was performed to determine how the data is distributed between constructs. While there are several methods that can be used to assess whether the data follows a normal distribution, the Kolmogorov-Smirnov (K-S) and Shapiro-Wilk (S-W) statistics are commonly used (Razali & Wah, 2011). The K-S statistic and S-W statistic are measures of the deviation of the sample distribution from a normal distribution. This study adopted both the K-S and S-W statistics to test the normality of the constructs.

3.9 Validity and Reliability Tests

Validity and reliability tests were used in this study to measure how thorough the research process was and the extent to which the research findings were trustworthy (Roberts & Priest, 2006). Saunders et al. (2019) list three measurements of validity in a quantitative study: *content validity, criterion-related validity, and construct validity.*

Content validity refers to the extent to which the questions in the questionnaire adequately address the investigative questions. Criterion-related validity is concerned with the ability of the questions to make predictions accurately. Lastly, construct validity refers to the extent to which a set of questions measures the presence of the construct you intended them to measure (Saunders et al., 2019). This study used construct validity.

Reliability tests are used to determine the degree to which the results of the study are consistent and whether they can be reproduced using a similar methodology (Golafshani, 2003).To prove the reliability of the constructs, the study used the Cronbach's alpha test. Cronbach's Alpha ranges from 0 to 1, where values closer to 0 indicate lower consistency while values closer to 1 indicate greater consistency. While a Cronbach's Alpha reliability score of 0.7 or is generally acceptable, Hinton, McMurray, and Brownlow (2004) argue that a reliability score of > 0.5 can be used.

3.10 Ethics

Research ethics relates to gaining access to appropriate participants, collecting, storing and analysing data, and interpreting results for the formulation of research findings in an ethical manner (Saunders et al., 2019). Ethical clearance was obtained from the Ethics Committee of the University of Cape Town before any data could be collected. During data collection, participants were informed of the confidentiality and anonymity of the survey. To ensure their confidentiality, no participant was required to provide identifiable information. Each participant was required to give their consent before taking the survey. All data collected was stored on a password-protected computer.

Additionally, a backup of all the data was stored in a secured cloud. Lastly, participants were informed that the information collected will be published. The ethical clearance form is attached.

3.11 Summary

This chapter presented the research methodology used for this study. A quantitative approach was deemed appropriate to achieve the objectives of the study. The chapter provided the philosophical stance, research strategy, and research approach that were used for the study.

CHAPTER 4:

RESULTS AND DISCUSSION

4.1 Introduction

This chapter provides a discussion of the findings of the study based on the results of the data analysis. The data collected from the survey were analysed per question and sub-questions.

4.2 Data Cleaning and Sample Size

The online survey recorded 58 responses out of the 70 that were initially targeted. This indicates a response rate of 81.43%. This study used Microsoft Excel for data cleaning. Data cleaning is a process that involves the detection, diagnosis, and editing of faulty data (Van den Broeck, Argeseanu Cunningham, Eeckels, & Herbst, 2005). The data collected did not have any outliers. Of the 58 responses, one participant declined to participate, thus taking the number of participants to 57.

4.3 Pilot Study

A pilot test was conducted to ensure that the questionnaire would be clearly understood by the participants. Two industry experts participated in the pilot tests and gave recommendations on how to better structure the questionnaire. Some of the questions were then edited based on the recommendations of the experts. The edited questionnaire was sent back to the two experts, who then advised that the questions were clear, and no further edits were required.

4.4 Reliability and Validity Statistics

Reliability measures how stable and consistent the measuring instrument is, while validity refers to the extent to which the chosen instrument measures what is purported to be measured (Saunders et al., 2016). Cronbach's Alpha test was used to measure the reliability of the constructs, *Management Support, Policies, processes and procedures, Legal requirements, Forensic and cybersecurity technologies, technical skills, and Training.*

Four of the constructs had a Cronbach's Alpha score of > 0.7, while two constructs, management support and training had a Cronbach's Alpha score of < 0.7. Hinton et al. (2004) argue that while the Cronbach's Alpha score of 0.7 or above is generally acceptable, scores > 0.5 can also be reliable. Based on this, the two construct with a score < 0.7 were not discarded as they were deemed a

significant part of the study. The following subsections discuss the results of the reliability and validity tests.

4.4.1 Reliability Statistics

The results of the reliability test for each construct produced values greater than 0.7, except for the construct management support, and training which had scores of 0.517 and 0.674 respectively. The following sub-sections discuss in detail the results of the reliability statistics for each construct.

4.4.1.1 Reliability statistics for the Management Support construct

Table 5 shows the results of Cronbach's Alpha test for the management support construct. The construct has three variables with a score of 0.517. This indicates that the management support construct is moderately reliable.

Table 5: Reliability Statistics: Management Support

Cronbach's Alpha	N of Items
.517	3

4.4.1.2 Reliability statistics for the Policies, Processes, and Procedures construct.

The results of the Cronbach's Alpha test for the policies, processes, and procedures construct are shown in Table 6. The Cronbach's Alpha score of 0.828 indicates that the policies, processes, and procedures construct is highly reliable.

Table 6: Reliability Statistics: Processes, Policies and Procedures

Cronbach's Alpha	N of Items
.828	3

4.4.1.3 Reliability statistics for the Legal requirements construct.

The legal consideration construct had 3 variables as shown in Table 7 below. Table 7 also shows the Cronbach's Alpha results for this construct, which is 0.816. This shows that the legal requirements construct is highly reliable.

Table 7: Reliability Statistics: Legal requirements

Cronbach's Alpha	N of Items
.816	3

4.4.1.4 Reliability statistics for Forensic and cybersecurity technologies construct

The forensic and cybersecurity technologies construct had 3 items. Table 8 shows the result of Cronbach's Alpha for this construct, which is 0.899. This illustrates that the forensic and cybersecurity technologies construct is highly reliable.

Table 8: Reliability Statistics: Forensic and cybersecurity technologies

Cronbach's Alpha	N of Items
.899	3

4.4.1.5 Reliability statistics for the technical skills construct

The technical skills construct had four variables as shown in Table 9 below. Table 9 also shows the Cronbach's Alpha results for this construct, which is 0.916. This shows that the technical skills construct is highly reliable.

Table 9: Reliability Statistics: Technical skills

Cronbach's Alpha	N of Items
.916	4

4.4.1.6 Reliability statistics for the Training construct

Table 10 shows the results of Cronbach's Alpha test for the training construct. The construct has four variables with a score of 0.674. This indicates that the training construct is moderately reliable.

Table 10: Reliability Statistics: Training

Cronbach's Alpha	N of Items
.674	4

A summary of the reliability statistics for all the constructs is shown in Table 11.

Table 11: Summary of reliability statistics for all the constructs

Construct	No. of items	Cronbach's Alpha
Management support	3	0.517
Processes, policies, and procedures	3	0.828
Legal requirements	3	0.816
Forensic and cybersecurity technologies	3	0.899
Technical skills	4	0.916
Training	4	0.674

4.5 Demographics and Background Information of Participants

This section summarizes the categorical data for age, job title, qualifications, certifications, and experience. The variables discussed here correspond to the data presented in the pie charts below.

4.5.1 Age

Figure 5 below shows the age composition of the participants. The results show that most of the participants were in the 31-40 age bracket with 22 responses. This constituted 38.6% of the total number of respondents. The age group between 21-30 followed with 19 participants. That translated to 33.3% of the total number of respondents. The age group 41-50 constituted 22.8% of the total number of respondents with 13 responses. The over-50 age group was the least represented, with only two respondents, which made up 3.5% of the total number of respondents.

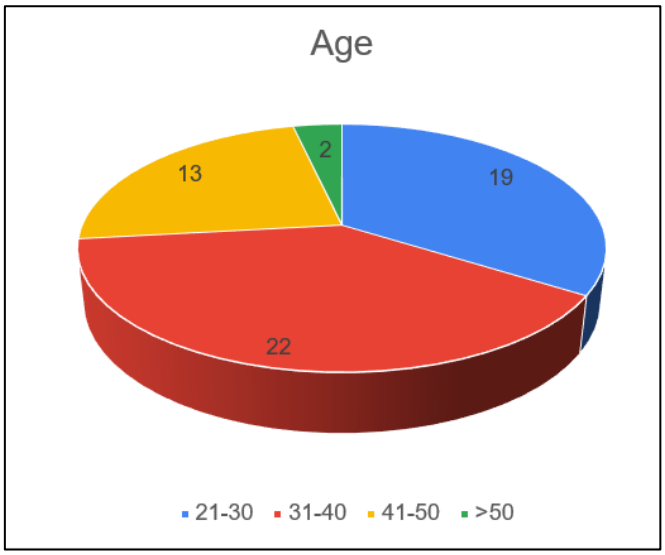

Figure 5: Age of the participants

4.5.2 Job Title

Figure 6 shows the representation of different occupations and the number of professionals who were surveyed. The results show that most of the participants were SOC analysts with 24 responses. This translated to 42.1% of the total number of respondents. IT security managers made up 14% of the respondents with 8 responses. The participants who held a CIO position were 4, which constituted 7% of the total responses. This was followed by CISOs with three responses that made up 5.3% of the total responses. There were 18 participants with 'other' job titles. This was the second largest response, which translates to 31.6% of the total number of respondents.

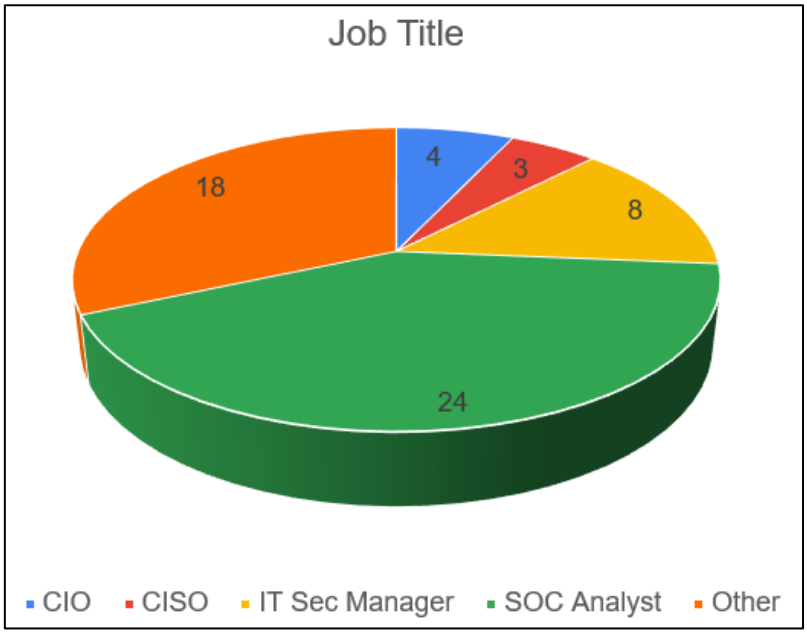

Figure 6: Job titles of participants

4.5.3 Qualifications

Figure **7** shows the number of people with different qualifications interviewed in this study. The results show that 21 respondents have a degree. This translated to 36.8 % of the total number of respondents. Participants with a national diploma made up 17.5% of the study with 10 responses. Participants with an Honors qualification were also 10, making up 17.5% of the total responses. This was followed by participants with an Advanced Diploma with two responses that made up 3.5% of the total responses. There were 14 participants with 'other' qualifications. This was the second largest response, which was equivalent to 24.6% of the total number of respondents. Based on this analysis, it was deduced that the large pool of people who were interviewed are at degree level.

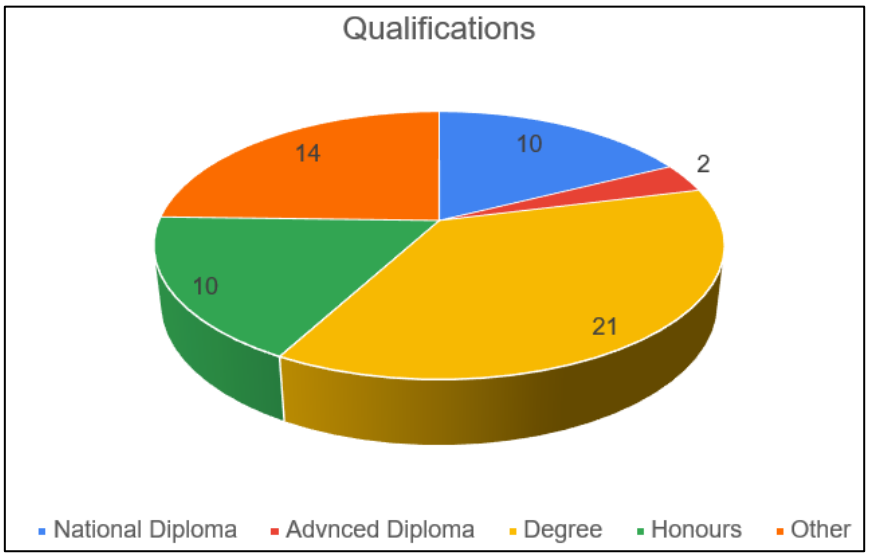

Figure 7: Qualifications of participants

4.5.4 Certifications

Participants were required to indicate their industry-specific certifications. It is important to note that some participants indicated holding more than one of the certifications listed. Figure 8 shows the industry-specific certifications held by the participants. From the responses, 39 participants indicated that they do not hold any industry-specific certifications. This represented 68.4% of the overall respondents. The number of participants with a Certified Ethical Hacker (CEH) certification was 18, which made up 31.6% of the total number of participants. This was followed by 8 participants with Certified Information Security Manager (CISM) certification, which constitutes 14% of the total number of respondents. There were 2 participants with a Certified Information Systems Security Professional (CISSP) certificate, which translated to 3.5% of the total number of respondents. Only

one participant had a Computer Hacking Forensic Investigator (CHFI) certificate. The number of participants with other certifications was 18, making up 31.6% of the respondents.

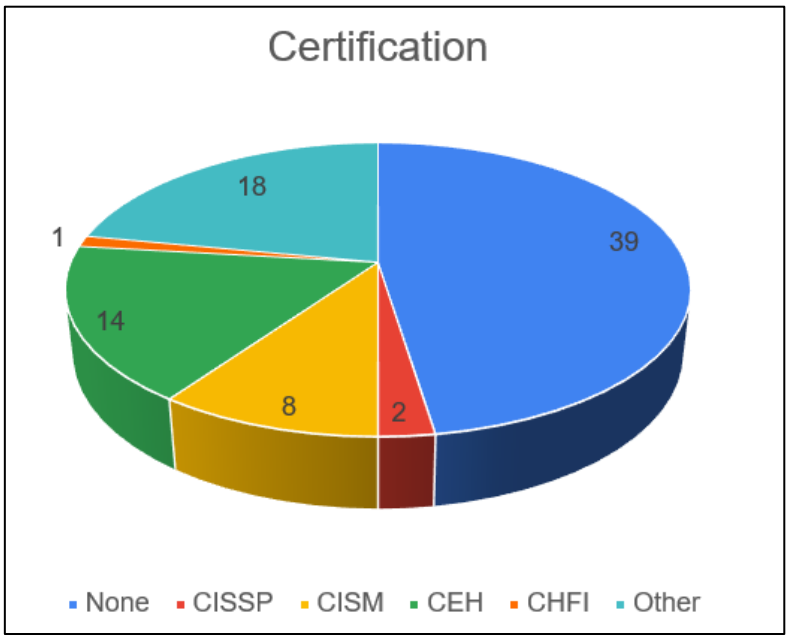

Figure 8: Industry certification

4.5.5 Experience

The survey conducted also categorizes the work experience of the participants. Figure 9 shows the number of years each participant has been in the industry. From the responses, the number of participants with 4-10 years of experience was 21, which is 36.8% of the total number of respondents. This was followed by 16 participants with 0-3 years of experience, who made up 21.8% of the total number of respondents. There were 10 participants with experience between 11-15 years, which constituted 17.5% of the total number of respondents. Participants with 16-20 years of experience were 5, which made up 8.8% of the total number of respondents. Lastly, participants with over 21 years of industry experience were 5, which made up 8.8% of the total number of respondents.

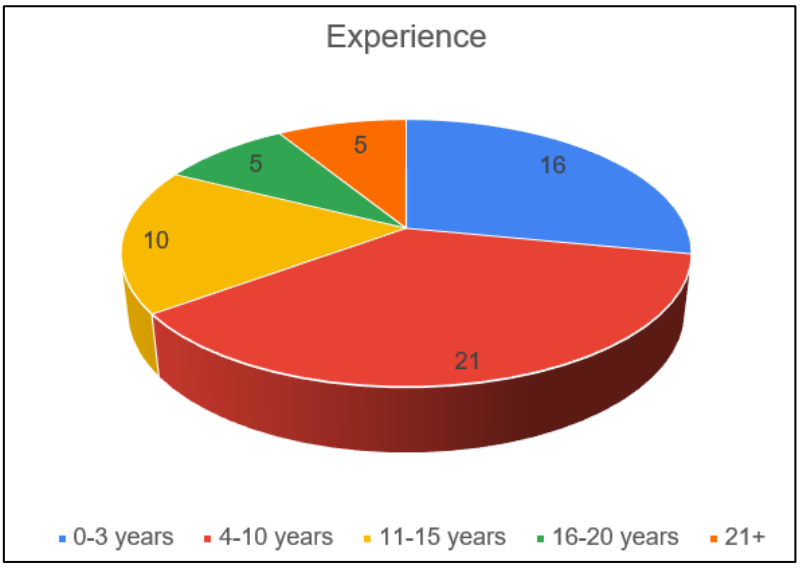

Figure 9: Job experience of participants

4.6 Descriptive Statistics

This section presents the results of the descriptive statistics for the study variables. The study used the following Likert scale measures: 1 = Totally Disagree; 2 = Disagree; 3= Somewhat Disagree, 4 = Agree; 5 = Totally Agree.

The number of responses for all variables is represented by N (N = 57). The Mean represents the average response, which gives insight into the central tendency for each variable. Standard Deviation (Std. Deviation) show how spread out the responses are from the mean. Means above 3 indicate that respondents generally perceive the factors as positive, while Standard deviations greater than 1 suggest a wide range of opinions on certain aspects. Table 12 shows summary of the results of the descriptive statistics of the study variables, followed by an analysis of each construct.

Table 12: Descriptive Statistics

Variable	**Descriptive Statistics**				
Management Support					
	N	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
SnrMan_PolicyFormulation	57	1	5	3.44	1.000
SnrMan_IRPParticipation	57	1	5	3.61	1.065
SnrMan-DFToolsFunding	57	1	5	3.72	1.013
Policies, processes, and procedures					
DFRPolicy-AnnualReview	**57**	**1**	**5**	**3.35**	**1.110**
IRPAddressed_DFPolicy	**57**	**1**	**5**	**3.54**	**1.036**

SOPs_For_EvidenceAcquiAndPreservation	**57**	**2**	**5**	**3.75**	**.950**
Legal Requirements					
Legal_Req_DuringInvestigation	**57**	**1**	**5**	**3.81**	**1.093**
SecBreach_ReportingProcedure	**57**	**1**	**5**	**3.91**	**1.090**
DataBreach_Penalties	**57**	**1**	**5**	**4.02**	**1.061**
Forensic and cybersecurity technologies					
FTools_SecTools_IRTReduction	**57**	**1**	**5**	**3.16**	**1.031**
FTools_SecToolsI_SecPosture	**57**	**1**	**5**	**3.37**	**1.080**
FTools_SecTools_ImprovedAnalysis	**57**	**1**	**5**	**3.28**	**.978**
Technical skills					
SOC_DFAnalysts	**57**	**1**	**5**	**3.67**	**1.123**
SOC_Analysts_EvidenceExtraction	**57**	**1**	**5**	**3.86**	**.990**
SOC_Analysts_DFRUnderstanding	**57**	**1**	**5**	**3.60**	**1.015**
SOC_Analysts_CommSkills	**57**	**1**	**5**	**3.81**	**.895**
Training					
SOC_Analysts_Training	**57**	**2**	**5**	**3.68**	**1.020**
Budget_DFSkillsDev	**57**	**1**	**5**	**3.51**	**1.120**
Certifications_DFStaff	**57**	**1**	**5**	**4.02**	**1.044**
IncidentReporting_Awareness	**57**	**1**	**5**	**3.96**	**1.034**

4.6.1 Management support

SnrMan_PolicyFormulation

The results indicate that on average, the respondents perceive management's involvement in policy formulation as slightly positive (mean = 3.44). However, with a standard deviation of 1, responses are somewhat spread out, suggesting differing views.

SnrMan_IRPParticipation

The results show that senior management's participation in incident response plans (IRP) is seen as moderately positive (Mean = 3.61). The responses are again varied, as the standard deviation is above 1 (Std.Deviation = 1.065).

SnrMan_DFToolsFunding

Funding for digital forensic tools is perceived as positive, but not overwhelming (Mean = 3.72), with a standard deviation suggesting a moderate spread in responses (Std. Deviation = 1.013).

4.6.2 Policies, Processes, and Procedures

DFRPolicy-AnnualReview

Results show that annual reviews of forensic policies are viewed slightly positively (Mean – 3.35), but with some variance in perceptions (Deviation = 1.110).

IRPAddressed_DFPolicy

The results show that on average, respondents perceive having an incident response plan in the DF policy as positive (Mean = 3.54), with a moderate spread in responses (Std. Deviation = 1.036.)

SOPs_For_EvidenceAcquiAndPreservation

Based on the results**,** Standard operating procedures (SOPs) for evidence acquisition and preservation are positively viewed (Mean = 3.75). The deviation shows moderate consistency in responses (Std. Deviation = 0.950).

4.6.3 Legal requirements

Legal_Req_DuringInvestigation

The results from the analysis show that respondents generally perceive that legal requirements during investigations are well addressed (Mean = 3.81), with some deviation (Std. Deviation = 1.093).

SecBreach_ReportingProcedure

Results show that participants are aware of Security breach reporting procedures (Mean = 3.91). However, the standard deviation indicates some variance in views (Std. Deviation = 1.090).

DataBreach_Penalties

The results indicate a strong agreement of awareness of the penalties associated with data breaches (Mean = 4.02). The deviation shows a moderate spread in opinion (Std. Deviation = 1.061).

4.6.4 Forensic and cybersecurity technologies

FTools_SecTools_IRTReduction

The results indicate that integrating forensic and security tools to reduce incident response time is perceived as only slightly effective (Mean = 3.16), with a standard deviation indicating moderate disagreement (Std. Deviation = 1.031).

FTools_SecToolsI_SecPosture

The results show that the integration of forensic and security tools is seen as moderately positive in improving the security posture (Mean = 3.37), though the variance suggests a range of opinions (Std. Deviation = 1.080).

FTools_SecTools_ImprovedAnalysis

The results show that integrating forensic and security tools to improve incident analysis is perceived positively, though not strongly (Mean = 3.28). Additionally, there is less variation compared to other questions related to integration of forensic and security tools (Std. Deviation = 0.978).

4.6.5 Technical skills

SOC_DFAnalysts

The results indicate that having competent DF analysts in a SOC is viewed positively (Mean = 3.67), though the variation suggests differing views on their effectiveness (Std. Deviation = 1.123).

SOC_Analysts_EvidenceExtraction

The results show that the ability of SOC analysts to extract evidence is perceived positively (Mean = 3.86). However, there is less variation in opinion (Std. Deviation = 0.990).

SOC_Analysts_DFRUnderstanding

The results indicate that understanding of DFR requirements by SOC analysts is positively viewed (Mean = 3.60), though there is some disagreement among respondents (Std. Deviation = 1.015).

SOC_Analysts_CommSkills

The results show that the ability of SOC analysts to effectively communicate technical outcomes with non-technical personnel is perceived positively (Mean = 3.81), with a standard deviation below 1 (Std. Deviation = 0.895), indicating more consistent agreement.

4.6.6 Training

SOC_Analysts_Training

The results of the analysis show that training for SOC analysts is generally seen as effective (Mean = 3.68), though responses vary moderately (Std. Deviation = 1.020).

Budget_DFSkillsDev

The results show that the budget for DF skills development is viewed as adequate (Mean = 3.51), though the higher standard deviation suggests some significant disagreement among respondents (Std. Deviation = 1.120).

Certifications_DFStaff

The results of the analysis indicate that certifications for digital forensics staff are strongly viewed as important and effective (Mean > 4), with disagreements in responses (Std. Deviation = 1.044).

IncidentReporting_Awareness

The results indicate that awareness training for incident reporting perceived positively (Mean = 3.96), with disagreements in responses (Std. Deviation = 1.034).

4.6.7 Summary of Descriptive statistics

The results of the descriptive statistics show that Certifications and legal requirements are perceived most positively, with means closer to 4. Forensic and cybersecurity technologies variables are perceived less positively, with means closer to 3.

4.7 Normality Tests and Correlation Analysis

This section discusses the normality tests that were performed to determine how the data are distributed. Based on the results of the normality test, a correlation test was performed to determine the strength of relationships between the constructs.

4.7.1 Normality Tests

The normality test was performed to determine how the data is distributed between constructs. The K-S and S-W statistics were used to perform this test. A higher K-S statistic value indicates greater deviation from normality, while a lower K-S statistic value suggests the data is closer to being normally distributed (Razali & Wah, 2011). For S-W statistic, a higher value indicates that the data is closer to normality, while a lower S-W statistic indicates greater deviation from normality.

Additionally, a significance level (p-value < 0.05) indicates that the distribution is non-normal. Table 13 illustrates the results of the normality test performed for all variables.

Table 13: Normality Test Results

	Kolmogorov-Smirnov[a]			**Shapiro-Wilk**		
	Statistic	**Df**	**Sig.**	**Statistic**	**Df**	**Sig.**
MANAGEMENT_SUPPORT	.138	57	.009	.963	57	.077
POLICIES_PROCESSES	.132	57	.015	.949	57	.019
LEGAL_REQUIREMENTS	.144	57	.005	.912	57	<.001
FORENSIC_CYBERSECURITY_ TECHNOLOGIES	.139	57	.008	.961	57	.062
TECHNICAL_SKILLS	.108	57	.097	.946	57	.012
TRAINING	.120	57	.041	.959	57	.051

4.7.1.1 Interpretation of values for each variable

Management Support

The K-S statistic (0.138) shows moderate deviation from normality, and the S-W statistic (0.963) indicates that the data is somewhat closer to a normal distribution, but still far from perfect normality. The significance value of .009 for K-S indicates non-normality, while S-W shows normality with significance value of .077. Both tests show conflicting results with K-S suggesting non-normality and S-W suggesting normality.

Policies, Processes, and Procedures

The K-S statistic (0.132) is lower than for Management Support, indicating less deviation from normality. The S-W statistic of 0.949 suggests that the data is getting somewhat closer to normality but is still significantly non-normal. Both tests indicate non-normality with significance value of .015 for K-S and .019 for S-W respectively.

Legal Requirements

The K-S statistic (0.144) is quite low, showing a small deviation from normality. The S-W statistic **(**0.912**)** is high, indicating that the Legal Requirements data is closer to being normally distributed. Legal Requirements also shows significant deviation from normality with p-values of .005 and <.001 respectively, indicating the data is not normally distributed.

Forensic and Cybersecurity Technologies

The K-S statistic (0.139) is lower than Legal Requirements, also suggesting a small deviation from normality, and the S-W statistic (0.961) is quite high, indicating that this data is closer to normality. The data for Forensic and cybersecurity technologies also shows conflicting results with K-S indicating non-normality (Sig.008), and S-W indicating normality (Sig.062).

Technical Skills

The K-S statistic (0.108) shows small deviation from normality, while the S-W statistic (0.946) suggests the data is somewhat closer to normality, but it is still non-normal based on the significance test. Technical skills data shows conflicting results with p-value >0.05 (Sig.097) for K-S indicating normality, and p-value <0.05 (Sig.012) for S-W indicating non-normality.

Training

The K-S statistic (0.120) indicates a smaller deviation from normality compared to some other variables. The S-W statistic of 0.959 still shows that the data is not normally distributed but is closer to normality. The Training data also shows conflicting results with p-value <0.05 (Sig.041) for K-S showing non-normality, and p-value >0.05 (Sig.051) for S-W indicating normality.

4.7.1.2 Summary

The results of the normality tests show that Management Support, Forensic and cybersecurity technologies, Technical Skills and Training data show conflicting results. Both the K-S and S-W tests show that Policies, Processes and Legal requirements data are non-normal.

4.7.2 Correlation Analysis

The study performed a correlation and regression analysis to test the relationship between the constructs. The results of the correlation analysis are presented in Table 14. Spearman's correlation coefficient was used to test the relationship between the constructs.

Table 14: Correlation Analysis Results

			SOC_READINESS	MANAGEMENT_SUPPORT	POLICIES_PROCESSES	LEGAL_REQUIREMENTS	FORENSIC_TECHNOLOGIES	TECHNICAL_SKILLS	TRAINING
Spearman's rho	SOC_READINESS	Correlation Coefficient	1,000	,752**	,691**	,696**	,724**	,718**	,685**
		Sig. (2-tailed)	.	<,001	<,001	<,001	<,001	<,001	<,001
		N	57	57	57	57	57	57	57
	MANAGEMENT_SUPPORT	Correlation Coefficient	,752**	1,000	,469**	,482**	,451**	,520**	,477**
		Sig. (2-tailed)	<,001	.	<,001	<,001	<,001	<,001	<,001
		N	57	57	57	57	57	57	57
	POLICIES_PROCESSES	Correlation Coefficient	,691**	,469**	1,000	,361**	,580**	,338*	,318*
		Sig. (2-tailed)	<,001	<,001	.	,006	<,001	,010	,016
		N	57	57	57	57	57	57	57
	LEGAL_REQUIREMENTS	Correlation Coefficient	,696**	,482**	,361**	1,000	,331*	,421**	,351**
		Sig. (2-tailed)	<,001	<,001	,006	.	,012	,001	,007
		N	57	57	57	57	57	57	57
	FORENSIC_TECHNOLOGIES	Correlation Coefficient	,724**	,451**	,580**	,331*	1,000	,419**	,373**
		Sig. (2-tailed)	<,001	<,001	<,001	,012	.	,001	,004
		N	57	57	57	57	57	57	57
	TECHNICAL_SKILLS	Correlation Coefficient	,718**	,520**	,338*	,421**	,419**	1,000	,652**
		Sig. (2-tailed)	<,001	<,001	,010	,001	,001	.	<,001
		N	57	57	57	57	57	57	57
	TRAINING	Correlation Coefficient	,685**	,477**	,318*	,351**	,373**	,652**	1,000
		Sig. (2-tailed)	<,001	<,001	,016	,007	,004	<,001	.
		N	57	57	57	57	57	57	57

Spearman's correlation coefficient (rho) measures the strength and direction of association between two ranked variables. The values of Rho range from -1 to +1, where +1 indicates a perfect positive correlation (as one variable increases, the other increases) and -1 indicates a perfect negative correlation (as one variable increases, the other decreases). Rho value of 0 indicates that there is no correlation between the variables. The next subsections present interpretation of correlation results in Table **14**

4.7.2.1 Digital Forensic Readiness in SOC:

Management support: Spearman's rho = 0.752 ($p < 0.001$), indicating a strong positive correlation between digital forensic readiness and management support. As management support increases, so does digital forensic readiness.

Processes, policies, and procedures: Spearman's rho = 0.691 ($p < 0.001$), indicating a strong positive correlation. Availability of policies and processes is associated with increased forensic readiness.

Legal requirements: Spearman's rho = 0.696 ($p < 0.001$), showing a strong positive correlation. Adherence to legal requirements positively impacts forensic readiness.

Forensic and cybersecurity technologies: Spearman's rho = 0.724 ($p < 0.001$), indicating a strong positive correlation. Availability and use of forensic and cybersecurity technologies are associated with better readiness.

Technical skills: Spearman's rho = 0.718 ($p <0.001$), showing a strong positive correlation that is statistically significant.

Training: Spearman's rho = 0.685 ($p < 0.001$), indicating a strong positive correlation. Better training is associated with improved forensic readiness.

4.8 Hypotheses Testing and Findings

This section presents the results of the regression analysis that was aimed at testing the relationships between the main constructs and hypotheses. In this section, the dependent variable Digital Forensic Readiness in SOC was regressed against each independent variable. The results of the hypotheses test determined which hypothesis was accepted or rejected.

4.8.1 Interpretation of regression analysis: H_1

Hypothesis H_1: The hypothesis suggests that management support has an effect on DFR of a SOC. The following is an interpretation of the regression analysis that was performed to test the relationship between management support and SOC DFR.

4.8.1.1 R^2 Value (0.614):

The R^2 value of 0.614 means that 61.4% of the variation in SOC DFR can be explained by management support. This suggests a relatively strong relationship between the two variables.

4.8.1.2 Beta Coefficient (0.661):

Beta Coefficient represents the strength and direction of the relationship between management support and SOC DFR. The beta coefficient of 0.661 indicates a positive relationship between management support and SOC DFR. As management support increases, SOC DFR is expected to increase as well.

4.8.1.3 F-statistic (87.364):

The F-value is quite high, indicating that the overall regression model is a good fit for the data. A higher F-value suggests that the independent variable (management support) has a strong explanatory power in the model.

4.8.1.4 p-value (<0.001):

The p-value of <0.001 is much smaller than the standard significance level of 0.05. This means that the relationship between management support and SOC DFR is statistically significant.

Since the p-value is below 0.05, we reject the null hypothesis (which typically states that there is no effect) and accept the alternative hypothesis that management support has a significant effect on SOC DFR.

Table **15** presents a summary of the regression analysis.

Table 15: Regression summary: Management Support

Hypothesis	Regression Weights	Beta Coefficient	R^2	F	p-value	Hypothesis Supported
H_1	Management Support ⟹ SOC DFR	.661	.614	87.364	<.001	Yes

4.8.1.5 Findings

The hypothesis is supported based on the following:

- Management support has a significant positive impact on SOC DFR.
- The relationship is statistically significant with a p-value of < 0.001.
- The model explains 61.4% of the variance in SOC DFR, which is relatively strong.

The results show that when management is involved, it leads to the allocation of adequate funding for DFR initiatives in a SOC.

4.8.2 Interpretation of regression analysis: H_2

Hypothesis H_2: This hypothesis suggests that the availability of well-defined policies, processes, and procedures has a positive influence on the ability of a SOC to be forensically ready. The following is an interpretation of the regression analysis that was performed to test the relationship between policies, processes and procedures and SOC DFR.

4.8.2.1 R^2 Value (0.560):

This value of 0.560 means that 56.0% of the variation in SOC DFR is explained by policies, processes, and procedures. While the effect is not as strong as management support in H_1, it is still significant, meaning policies and procedures play an important role in SOC DFR.

4.8.2.2 Beta Coefficient (0.685):

The beta coefficient of **0.685** shows a positive relationship between policies, processes, and procedures and SOC DFR. The availability of well-structured policies and procedures leads to an increase in SOC DFR.

This coefficient is standardized, allowing comparison with other predictors (like management support in H_1). While it is positive, its strength is slightly more than in H_1.

4.8.2.3 F-statistic (70.128):

The F-value of 70.128 indicates that the model is a good fit for the data, meaning that policies, processes, and procedures explain a significant portion of the variation in SOC DFR. A higher F-statistic shows that the model performs well, with policies and procedures being a meaningful predictor.

4.8.2.4 p-value (<0.001):

The p-value of <0.001 indicates that the relationship between policies, processes, and procedures and SOC DFR is statistically significant. Since the p-value is much smaller than 0.05, we reject the null hypothesis (which states there is no effect) and accept the alternative hypothesis that policies, processes, and procedures significantly influence SOC DFR.

Summary of the findings is shown in Table **16**.

Table 16: Regression summary: Policies, processes, and procedures

Hypothesis	Regression Weights	Beta Coefficient	R^2	F	p-value	Hypothesis Supported
H_2	Policies, processes, procedures ➡ SOC DFR	.749	.560	70.128	<.001	Yes

4.8.2.5 Summary

Hypothesis Supported: Yes, the hypothesis is supported based on the following:

- Policies, processes, and procedures have a significant positive effect on SOC DFR.
- The relationship is statistically significant, with a p-value of < 0.001.
- The model explains 56.0% of the variance in SOC DFR, which indicates a moderate impact.

This suggests that having policies, processes, and procedures will positively impact SOC DFR.

4.8.3 Interpretation of regression analysis: H_3

Hypothesis H_3: This hypothesis suggests that being familiar with various legal requirements has a positive influence on the forensic readiness of a SOC. The following is an interpretation of the

regression analysis that was performed to test the relationship between legal requirements and SOC DFR.

4.8.3.1 R^2 Value (0.490):

The R^2 value of 0.490 means that 49.0% of the variation in SOC DFR is explained by legal requirements. This is a relatively strong influence, suggesting that legal requirements play a substantial role in determining the SOC's readiness for digital forensics.

4.8.3.2 Beta Coefficient (0.700):

The beta coefficient of 0.700 indicates a positive relationship between legal requirements and SOC DFR. The relationship is quite strong, meaning that improvements or focus on legal aspects (such as compliance, legal frameworks) will lead to a significant increase in SOC DFR.

4.8.3.3 F-statistic (52.849):

The F-statistic of 52.849 shows that the model fits the data well, and legal requirements are a significant predictor of SOC DFR.

A higher F-statistic suggests a robust relationship between legal requirements and SOC DFR.

4.8.3.4 p-value (<0.001):

The p-value of <0.001 indicates that the relationship between legal requirements and SOC DFR is statistically significant.

Since the p-value is much smaller than 0.05, we reject the null hypothesis (which states there is no effect) and accept the alternative hypothesis that legal requirements significantly affect SOC DFR.

Summary of the findings is shown in Table 17

Table 17: Regression summary: Legal requirements

Hypothesis	Regression Weights	Beta Coefficient	R^2	F	p-value	Hypothesis Supported
H_3	Legal requirements ⟶ SOC DFR	.468	.468	48.352	.001	Yes

4.8.3.5 Conclusion

Hypothesis Supported: Yes, the hypothesis is supported.

- Legal requirements have a significant positive impact on SOC DFR.
- The model explains 46.8% of the variance in SOC DFR, indicating a strong effect.
- The relationship is statistically significant, with a p-value of 0.001.

This shows that understanding the various legal frameworks in SOC operations can significantly enhance the SOC's readiness for digital forensics.

4.8.4 Interpretation of regression analysis: H_4

Hypothesis H_4: The hypothesis suggests that forensic and cybersecurity technologies have an effect on DFR of a SOC. The following is an interpretation of the regression analysis that was performed to test the relationship between forensic and cybersecurity technologies and SOC DFR.

4.8.4.1 R^2 Value (0.506):

The R^2 value of 0.506 means that 50.6% of the variation in SOC DFR is explained by forensic and cybersecurity technologies. The higher percentage indicates that forensic and cybersecurity technologies play a significant role in shaping SOC DFR but are not the most dominant factor.

4.8.4.2 Beta Coefficient (0.712):

The beta coefficient of 0.712 indicates a positive relationship between forensic and cybersecurity technologies and SOC DFR. A high beta suggests that an improvement in forensic and cybersecurity technologies contribute to SOC DFR.

4.8.4.3 F-statistic (56.428):

The F-statistic of 56.428 indicates a reasonable fit for the model. It shows that forensic and cybersecurity technologies are a significant predictor of SOC DFR but with a smaller overall effect compared to other factors.

4.8.4.4 p-value (<0.001):

The p-value of <0.001 signifies that the relationship between forensic and cybersecurity technologies and SOC DFR is statistically significant.

Since the p-value is well below 0.05, we can confidently reject the null hypothesis and accept that forensic and cybersecurity technologies have a significant positive impact on SOC DFR.

Table **18** shows the summary of the findings.

Table 18: Regression summary: Forensic and cybersecurity technologies

Hypothesis	Regression Weights	Beta Coefficient	R^2	F	p-value	Hypothesis Supported
H_4	Forensic and cybersecurity technologies ⟶ SOC DFR	.712	.506	56.428	<.001	Yes

4.8.4.5 Conclusion

Hypothesis Supported: Yes, the hypothesis is supported.

- Forensic and cybersecurity technologies have a significant, positive, but moderate impact on SOC DFR.
- The model explains 50.6% of the variance in SOC DFR, meaning that forensic and cybersecurity technologies are a contributing factor.
- The relationship is statistically significant, with a p-value of <0.001.

This suggests that while forensic and cybersecurity technologies are important for SOC DFR, they are part of a larger set of factors that influence overall readiness.

4.8.5 Interpretation of regression analysis: H_5

Hypothesis H_5: The hypothesis suggests that the availability of technically proficient personnel has a positive influence on the forensic readiness of a SOC. The following is an interpretation of the regression analysis that was performed to test the relationship between technical skills and SOC DFR.

4.8.5.1 R^2 Value (0.526):

The R^2 value of 0.526 means that 52.6% of the variation in SOC DFR is explained by technical skills. This is a very low percentage, indicating that technical skills have a minor impact on SOC DFR compared to other factors like forensic and cybersecurity technologies or management support.

4.8.5.2 Beta Coefficient (0.731):

The beta coefficient of 0.731 suggests a strong positive relationship between technical skills and SOC DFR. A high beta indicates that technical skills contribute significantly to SOC DFR in this model.

4.8.5.3 F-statistic (63.089):

The F-statistic of 63.089 is high, indicating that technical skills are significant when predicting SOC DFR.

4.8.5.4 p-value (<0.001):

The p-value of <0.001 signifies that the relationship between technical skills and SOC DFR is statistically significant.

Since the p-value is well below 0.05, we can confidently reject the null hypothesis and accept that technical skills have a significant positive impact on SOC DFR.

Table 19 shows the summary of the findings.

Table 19: Regression summary: Technical Skills

Hypothesis	Regression Weights	Beta Coefficient	R^2	F	p-value	Hypothesis Supported
H_5	Technical Skills ⟹ SOC DFR	.0731	.526	.63.089	<.001	Yes

4.8.5.5 Summary

Hypothesis Supported: Yes, the hypothesis is supported due to the following:

- Technical skills have a significant impact on SOC DFR based on the current model.
- The model explains 52.6% of the variance in SOC DFR, meaning that technical skills have a significant contribution.

The relationship is statistically significant, with a p-value of < .001. This implies that the effect of technical skills on SOC DFR is strong.

4.8.6 Interpretation of regression analysis: H_6

Hypothesis H_6: The hypothesis suggests that continuous training in relation to being forensically ready has a positive influence on the forensic readiness of a SOC. The following is an interpretation of the regression analysis that was performed to test the relationship between training and SOC DFR.

4.8.6.1 R^2 Value (0.401):

The R^2 value of 0.401 indicates that 40.1% of the variation in SOC DFR is explained by the training variable. This is a relatively high value, meaning training has a substantial influence on SOC DFR.

4.8.6.2 Beta Coefficient (0.642):

The beta coefficient of 0.642 shows a moderate positive relationship between training and SOC DFR. The higher the training, the better the SOC's forensic readiness is likely to be, according to this model.

4.8.6.3 F-statistic (38.499):

A high F-statistic of 38.499 suggests that the model fits the data well and the independent variable (training) significantly contributes to explaining the variability in SOC DFR.

4.8.6.4 p-value (< .001):

The p-value of < .001 is much lower than 0.05, indicating that the relationship between training and SOC DFR is statistically significant**.** Therefore, we can reject the null hypothesis and conclude that training has a significant positive effect on SOC DFR.

Table 20 shows the summary of the findings.

Table 20: Regression summary: Training

Hypothesis	Regression Weights	Beta Coefficient	R^2	F	p-value	Hypothesis Supported
H_6	Training ⟹ SOC DFR	.642	.401	38.499	<.001	Yes

4.8.6.5 Findings

Hypothesis Supported: Yes, the hypothesis is supported.

- Training has a statistically significant and positive impact on SOC DFR.
- The R^2 value (0.401**)** and the p-value (< .001) support the conclusion that training is an important factor in improving SOC digital forensic readiness.

This suggests that investing in training within a SOC can greatly enhance their readiness for digital forensic investigations.

Table 21gives a summary of the hypotheses testing.

Table 21: Summary of the hypotheses testing

Hypothesis	**R^2**	**P-value**	**Hypothesis Supported**
H_1: *Management support in various DFR initiatives has a significantly positive influence on facilitating the forensic readiness of a SOC.*	0.614	< .001	Yes
H_2: *The availability of well-defined* p*olicies, processes, and procedures has a significantly positive influence on the ability of a SOC to be forensically ready.*	0.560	< .001	Yes
H_3: *Knowledge of various legislative frameworks has a significantly positive influence on facilitating the data forensic readiness of a SOC.*	0.490	< .001	Yes
H_4: *Integration of forensic and security technologies has a significantly positive influence on the data forensic readiness of a SOC.*	0.506	< .001	Yes
H_5: *The availability of technically proficient personnel has a significantly positive influence on enhancing the forensic readiness of a SOC.*	.526	< .001	Yes
H_6*: Continuous training on the importance of being forensically ready has a significantly positive influence on enhancing the forensic readiness of a SOC.*	.401	< .001	Yes

4.9 Chapter Summary

This chapter covered the analysis and interpretation of results. The survey attracted a response rate of 81%. The statistical software SPSS was used for the analysis of the results. Most of the respondents

from the survey were between the ages of 31-40, closely followed by respondents between the ages of 21-30. SOC analysts made up 41% of the respondents, followed by IT managers, who made up 14% of the total number of respondents. Most respondents indicated not holding any industry-related certifications.

The Cronbach Alpha test conducted showed that two constructs, management support and training, had an alpha value below 0.7. However, based on prior studies which found an alpha value above 0.5 reliable, the constructs were deemed reliable, and their responses used for the study.

The results of the descriptive statistics indicated that respondents perceived training and legal requirements most positively, with means closer to 4. Forensic and cybersecurity technologies and management support variables are perceived less positively, with means closer to 3.

Normality tests conducted showed that the data were not all normally distributed, which led to the use of Spearman's correlation to test the relationship between the study constructs. The results of the Spearman's correlation test indicated that management support had the greatest effect on the forensic readiness of a SOC, followed closely by forensic and cybersecurity technologies. The construct with the least effect was found to be training.

After conducting extensive statistical analysis, the findings of the study show that the SOC forensic readiness in South Africa is influenced by *a) management support, b) the availability of policies, processes and procedures, c) familiarity with various legal requirements, d) the integration of digital forensic and cybersecurity technologies with security technologies, e) the technical skills of SOC analysts and f) the level of employee training and awareness in digital forensic practices.*

CHAPTER 5:

CONCLUSION AND RECOMMENDATIONS

The previous chapter focused on the data analysis and summary of the findings. This chapter presents the conclusion of the dissertation. This chapter covers the key findings of the and study. Further discussed in this chapter are the limitations and recommendations for future studies.

5.1 Background

The spike in the number of data breaches experienced by South African organizations has prompted some organizations to deploy proactive measures to reduce the impact of the breaches. One such measure is the deployment of a SOC, which provides a multilayered approach to secure the IT infrastructure of an organization. Although SOCs have evolved over time in threat hunting, there is still a challenge in how quickly they perform forensic investigations following a breach.

The study adopted quantitative research methods to answer the research questions and achieve its objectives. The data from the respondents were collected using an online survey questionnaire. The objectives of the study were as follows:

- To determine the extent to which the available DFR frameworks address challenges in SOC environments.
- To identify the key factors that affect the forensic readiness of a SOC.
- To develop a DFR conceptual model for SOC environments in South Africa.

Objective 1: To determine the extent to which the available DFR frameworks address SOC environments. The study examined four DFR frameworks which applied to various sectors. These included the banking sector in Nigeria, sectors with IoT devices, a framework addressing cybersecurity practitioners, and finally a framework addressing management in organizations challenges. The results of the literature showed that these frameworks were not adequate to address the DFR needs of a SOC. However, there were components of the frameworks that deemed important to contribute to this study.

Objective 2: To identify the key factors that affect the forensic readiness of a SOC. This objective was achieved, and six factors were identified. These factors included *management support, policies*

and processes, legal requirements, forensic and cybersecurity technologies, technical skills, and training. These factors were used to form the basis of the conceptual model.

Objective 3: To develop a DFR conceptual model for SOC environments in South Africa. This objective was achieved by examining the relationship between forensic readiness of a SOC and all the six factors identified using regression analysis. Results of the regression analysis showed that all six factors have a statistically significant influence on the readiness of a SOC. The results of the regression analysis supported the hypotheses as follows:

Management Support: The results of the analysis support the previous literature that determined that for an organization to achieve its DFR goals, it needs top management support (Kebande et al., 2020).Therefore, SOC environments that need to implement a successful DFR plan need to ensure that they get management buy-in and alignment with the overall strategy of the organization.

Policies, processes and procedures: The finding that well-defined policies, processes, and procedures have a positive effect on the forensic readiness of a SOC is supported by previous studies by (Rowlingson, 2004; Kebande et al., 2020). A SOC that aims to resolve incidents seamlessly and in a timely manner needs to develop policies, processes, and procedures that will help to understand the separate roles and responsibilities when performing a forensic analysis. Furthermore, when policies, processes, and procedures are well defined and implemented, the proper handling of digital evidence and the chain of custody will be achieved. Finally, all documentation can serve as guides for new SOC forensic analysts so that they can quickly adapt to their roles.

Legal requirements: This finding is in line with previous literature that found that organizations need to be familiar with legal and regulatory requirements for data handling in the country they are operating (Kebande et al., 2020). Depending on the type of SOC that an organization is running, data might be stored in a cloud outside of South Africa. Thus, legal requirements for extracting evidence in jurisdictions outside of South Africa should also be considered when preparing a DFR plan for a SOC.

Evidence collected during a forensic investigation in a SOC has the potential to be presented in a court of law or during an internal disciplinary process. As a result, collaboration with an organization's legal team could help ensure that all compliance with various legal requirements is achieved.

Forensic and cybersecurity tools: Although there is no prior literature on how the integration of forensics and cybersecurity tools can help an organization to be forensically ready, this finding is in

line with prior research that using the right forensic technologies can help an organization become forensically ready (Kebande et al., 2020). The increased sophistication in cyber incidents necessitates a collaborative effort to ensure that forensic investigations within a SOC are resolved timeously.

A SOC deploys a diverse number of cybersecurity technologies such as SIEM and EDR that can actively collect data and logs that can be used during a forensic investigation. Integrating these technologies with forensic technologies ensures that there is little human interaction during evidence collection, which has the potential to compromise the integrity of the evidence. Furthermore, an integration of these technologies allows a SOC to be more proactive in collecting evidence for forensics purposes.

Technical skills: The result of the analysis affirms prior studies that found that technical skills play a significant role in an organization being forensically ready (Rowlingson, 2004; Kebande et al., 2020). This finding implies that it is important to have personnel within a SOC who understand the importance of their organization being forensically ready. Furthermore, technically proficient people should be able to follow the incident response plan and effectively communicate the findings across the organization.

Training: Previous studies in forensic readiness support the finding that training, particularly awareness, has a positive influence on forensic readiness of an organization (Rowlingson, 2004; Sachowski, 2019; Kebande et al., 2020).

Although awareness training is beneficial for the entire organization, training specifically for those employed in a SOC to perform forensic investigations is also necessary. This ensures that SOC forensic analysts are up to date with the latest technologies and forensic techniques. Therefore, it is important that organizations in South Africa make funding available for training specifically focused on improving the technical skills of SOC forensic investigators.

5.2 Limitations and future studies

One of the limitations of this study is that its focus was only limited to organizations that already run a SOC. This had an impact on the sample size as not many participants were reached. Future studies might expand on this and include other organizations that may not necessarily be running a SOC but have a cybersecurity team.

The other limitation of this study is that it focused only on the perspective of technical staff within a SOC. However, an incident can occur from anywhere within an organization. As a result, nontechnical staff also need to be considered when formulating a forensic readiness plan.

The final limitation of the study relates to the ability to perform a case study of the conceptual model in a live SOC environment. Future studies can thus test the conceptual model in a live SOC environment to verify its applicability.

Most SOCs run in South Africa are outsourced and rely on third parties. Future studies should also look at how outsourcing SOC services could impact the readiness plans. Also, the impact that new technologies such as AI and machine learning, which are being integrated into SOC environments, have on the forensic readiness of a SOC.

References

Adams, R., Adeleke, F., Anderson, D., Bawa, A., Branson, N., Christoffels, A., … Ramsay, M. (2021). POPIA Code of Conduct for Research. *South African Journal of Science*, *117*(5–6), 1–12. https://doi.org/10.17159/SAJS.2021/10933

Akter, O., Akther, A., Uddin, A., & Islam, M. (2020). Wireless and Microwave Technologies. *OIC-CERT*, *5*, 1–12. https://doi.org/10.5815/ijwmt.2020.05.01

Alenezi, A., Atlam, H. F., Alsagri, R., Alassafi, M. O., & Wills, G. B. (2019). IoT forensics: A state-of-the-art review, challenges and future directions. *COMPLEXIS 2019 - Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk*, 106–115. https://doi.org/10.5220/0007905401060115

Alenezi, A., Hussein, R. K., Walters, R. J., & Wills, G. B. (2017). A Framework for Cloud Forensic Readiness in Organizations. *2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 199–204. IEEE. https://doi.org/10.1109/MobileCloud.2017.12

Banerjee, A., & Chaudhury, S. (2010). Statistics without tears: Populations and samples. *Industrial Psychiatry Journal*, *19*(1), 60. https://doi.org/10.4103/0972-6748.77642

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices* (2nd ed.). Tampa, Florida. Retrieved from https://digitalcommons.usf.edu/oa_textbooks/3

Burrell, G., & Morgan, G. (2017). Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life. In *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life* (1st Edition). London: Taylor and Francis. https://doi.org/10.4324/9781315242804/SOCIOLOGICAL-PARADIGMS-ORGANISATIONAL-ANALYSIS-GIBSON-BURRELL-GARETH-MORGAN

Cappellino, A. (2022, April 11). Daubert vs. Frye: Standards of Admissibility for Expert Testimony. Retrieved April 3, 2023, from https://www.expertinstitute.com/resources/insights/daubert-vs-frye-navigating-the-standards-of-admissibility-for-expert-testimony/

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Security and Privacy*, *15*(6), 12–17. https://doi.org/10.1109/MSP.2017.4251117

Chamkar, S. A., Maleh, Y., & Gherabi, N. (2021). THE HUMAN FACTOR CAPABILITIES IN SECURITY OPERATION CENTER (SOC). *Https://Doi.Org/10.1080/07366981.2021.1977026*, *66*(1), 1–14. https://doi.org/10.1080/07366981.2021.1977026

Chamkar, S. A., Maleh, Y., & Gherabi, N. (2023). SOC Analyst Performance Metrics: Towards an optimal performance model. *EDPACS*, *68*(3), 16–29. https://doi.org/10.1080/07366981.2023.2259046

Chan, E., Venkataraman, S., David, F., Chaugule, A., & Campbell, R. (2010). Forenscope: A framework for live forensics. *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 307–316. https://doi.org/10.1145/1920261.1920307

Chyung, S. Y. Y., Swanson, I., Roberts, K., & Hankinson, A. (2018). Evidence-Based Survey Design: The Use of Continuous Rating Scales in Surveys. *Performance Improvement*, *57*(5), 38–48. https://doi.org/10.1002/pfi.21763

Collie, J. (2018). A Strategic Model for Forensic Readiness. *Athens Journal of Sciences*, *5*(2), 167–182. https://doi.org/10.30958/ajs.5-2-4

Daneilsson, J., & Tjostheim, I. (2004). (PDF) THE NEED FOR A STRUCTURED APPROACH TO DIGITAL FORENSIC READINESS DIGITAL FORENSIC READINESS AND E-COMMERCE. *IADIS International Conference E-Commerce*, 417–421. Retrieved from

https://www.researchgate.net/publication/268301581_THE_NEED_FOR_A_STRUCTURED_APPROACH_TO_DIGITAL_FORENSIC_READINESS_DIGITAL_FORENSIC_READINESS_AND_E-COMMERCE

Dilijonaite, A. (2017). Digital Forensic Readiness. In *Digital Forensics* (pp. 117–145). Wiley. https://doi.org/10.1002/9781119262442.ch4

Docrat, R. (2022). Ransomware Attacks in South Africa: What You Need to Know - iSite Computers. *Https://Isite.Co.Za/*. Retrieved from https://isite.co.za/ransomware-attacks-south-africa/

Fisher, M. J., & Marshall, A. P. (2009). Understanding descriptive statistics. *Australian Critical Care*, *22*(2), 93–97. https://doi.org/10.1016/j.aucc.2008.11.003

Garba, A. A., & Bade, A. M. (2019). A RECOMMENDED DIGITAL FORENSIC READINESS FRAMEWORK FOR NIGERIAN BANKS. *International Journal of Development Research*, *09*(08), 28920–28928.

Golafshani, N. (2003). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*, *8*(4), 597–607.

Hinton, P., McMurray, I., & Brownlow, C. (2004). *SPSS Explained*. Routledge. https://doi.org/10.4324/9780203642597

Janos, F. D., & Dai, N. H. P. (2018). Security concerns towards security operations centers. *SACI 2018 - IEEE 12th International Symposium on Applied Computational Intelligence and Informatics, Proceedings*, 273–278. https://doi.org/10.1109/SACI.2018.8440963

Karie, N., & Karume, S. (2017). Digital Forensic Readiness in Organizations: Issues and Challenges. *The Journal of Digital Forensics, Security and Law*, *12*(5). https://doi.org/10.15394/jdfsl.2017.1436

Kaur, H., & Jindal, N. (2020). Image and Video Forensics: A Critical Survey. *Wireless Personal Communications*, *112*(2), 1281–1302. https://doi.org/10.1007/s11277-020-07102-x

Kebande, V. R., Mudau, P. P., Ikuesan, R. A., Venter, H. S., & Choo, K.-K. R. (2020). Holistic digital forensic readiness framework for IoT-enabled organizations. *Forensic Science International: Reports*, *2*, 100117. https://doi.org/10.1016/J.FSIR.2020.100117

Kerner, S. M. (2023, January 26). 34 cybersecurity statistics to lose sleep over in 2023. Retrieved February 21, 2023, from Techtarget.com website: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., & Bakhtiari Bastaki, B. (2021). The complexity of internet of things forensics: A state-of-the-art review. *Forensic Science International: Digital Investigation*, *38*, 301210. https://doi.org/10.1016/J.FSIDI.2021.301210

Majid, M. A., & Ariffi, K. A. Z. (2019). Success Factors for Cyber Security Operation Center (SOC) Establishment. *Proceedings of the 1st International Conference on Informatics, Engineering, Science and Technology*. Bandung, Indonesia: European Alliance for Innovation n.o. https://doi.org/10.4108/EAI.18-7-2019.2287841

Marshall, G., & Jonker, L. (2011). An introduction to inferential statistics: A review and practical guide. *Radiography*, *17*(1), e1–e6. https://doi.org/10.1016/j.radi.2009.12.006

Maziana, A. M., & Khairul, A. Z. A. (2021). Model for successful development and implementation of Cyber Security Operations Centre (SOC). *PLOS ONE*, *16*(11), e0260157. https://doi.org/10.1371/journal.pone.0260157

Mckemmish, R. (1999). *What is Forensic Computing? 118*. Retrieved from http://www.aic.gov.au

Moon, K., & Blackman, D. (2014). A Guide to Understanding Social Science Research for Natural Scientists. *Conservation Biology*, *28*(5), 1167–1177. https://doi.org/10.1111/COBI.12326/FULL

Morgan, S. (2024, June 24). 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. Retrieved October 13, 2024, from Cybercrime Magazine website: https://cybersecurityventures.com/cybersecurity-almanac-2024/

Moyo, A. (2024, May 24). Justice department suffers another cyber attack. Retrieved August 3, 2024, from https://www.itweb.co.za/article/justice-department-suffers-another-cyber-attack/rW1xLv5nJkx7Rk6m website: https://www.itweb.co.za/article/justice-department-suffers-another-cyber-attack/rW1xLv5nJkx7Rk6m

Mrdovic, S. (2021). IoT Forensics. *Security of Ubiquitous Computing Systems*, 215–229. https://doi.org/10.1007/978-3-030-10591-4_13

Mughal, A. A. (2022). Building and Securing the Modern Security Operations Center (SOC). *International Journal of Business Intelligence and Big Data Analytics*, *5*(1), 1–15. Retrieved from https://research.tensorgate.org/index.php/IJBIBDA/article/view/21

Mutemwa, M., Mtsweni, J., & Zimba, L. (2018). Integrating a Security Operations Centre with an Organization's Existing Procedures, Policies and Information Technology Systems. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, 1–6. IEEE. https://doi.org/10.1109/ICONIC.2018.8601251

Nabi, S. T., Kumar, M., Singh, P., Aggarwal, N., & Kumar, K. (2022). A comprehensive survey of image and video forgery techniques: variants, challenges, and future directions. *Multimedia Systems*, *28*(3), 939–992. https://doi.org/10.1007/s00530-021-00873-8

Onwubiko, C., & Ouazzane, K. (2019). Challenges towards Building an effective Cyber Security Operations Centre. *International Journal on Cyber Situational Awareness*, *4*(1), 11–39. https://doi.org/10.22619/IJCSA.2019.100124

Onwubiko, C., & Ouazzane, K. (2022). Challenges towards Building an effective Cyber Security Operations Centre. *International Journal on Cyber Situational Awareness*, *4*(1), 11–39. https://doi.org/10.22619/IJCSA.2019.100124

Parasuraman, A. (2000). Technology Readiness Index (Tri). *Journal of Service Research*, *2*(4), 307–320. https://doi.org/10.1177/109467050024001

Parasuraman, A., & Colby, C. L. (2015). An Updated and Streamlined Technology Readiness Index. *Journal of Service Research*, *18*(1), 59–74. https://doi.org/10.1177/1094670514539730

Perera, A., Rathnayaka, S., Perera, N. D., Madushanka, W. W., & Senarathne, A. N. (2021). The Next Gen Security Operation Center. *2021 6th International Conference for Convergence in Technology, I2CT 2021*, 1–9. Maharashtra, India: Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/I2CT51068.2021.9418136

Petrosyan, A. (2024, November 8). Data records breached worldwide Q3 2024| Statista. Retrieved April 29, 2025, from https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/ website: https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/

Powell, O. (2022, December 9). The biggest data breaches and leaks of 2022. Retrieved February 12, 2023, from Cyber Security Hub website: https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022

Puchert, D. (2024, May 7). Interpol cyberthreat assessment for South Africa. Retrieved August 5, 2024, from Mybroadband website: https://mybroadband.co.za/news/security/535235-interpol-cyberthreat-assessment-for-south-africa.html

Purnaye, P., & Kulkarni, V. (2022). A Comprehensive Study of Cloud Forensics. *Archives of Computational Methods in Engineering*, *29*(1), 33–46. https://doi.org/10.1007/S11831-021-09575-W/FIGURES/6

Richardson, P. (2021, September 21). South African Justice Department Is Hit by Ransomware Attack - Bloomberg. Retrieved April 27, 2023, from Bloomberg website: https://www.bloomberg.com/news/articles/2021-09-09/south-african-justice-department-is-hit-by-ransomware-attack?leadSource=uverify%20wall

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence Winter*, *2*(3). Retrieved from www.ijde.org

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). *Cloud Forensics*. https://doi.org/10.1007/978-3-642-24212-0_3

Sachowski, J. (2019). *Implementing Digital Forensic Readiness: From Reactive to Proactive Process* (2nd ed.). CRC Press.

Salinas, S. (2023, January 24). What Is a Security Operations Center? Complete Guide. Retrieved October 13, 2024, from Exabeam website: https://www.exabeam.com/blog/security-operations-center/security-operations-center-ultimate-soc-quick-start-guide/

Saunders, N. K. M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students* (8th ed.). Harlow: Pearson.

Schlette, D., Vielberth, M., & Pernul, G. (2021). CTI-SOC2M2 – The quest for mature, intelligence-driven security operations and incident response capabilities. *Computers & Security*, *111*, 102482. https://doi.org/10.1016/J.COSE.2021.102482

Sharma, V., Jha, S., & Dr. Bharti, R. K. (2016). Image Forgery and it's Detection Technique: A Review. *IRJET*, *3*(3), 756–762.

Shweta, Adithan, K., & Hoeper, M. (2024, May 31). What Is EDR? Endpoint Detection & Response. Retrieved August 5, 2024, from Forbes website: https://www.forbes.com/advisor/business/what-is-edr/

Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, *4*(3), 299–323. https://doi.org/10.1365/s43439-023-00089-8

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Communications Surveys and Tutorials*, *22*(2), 1191–1221. https://doi.org/10.1109/COMST.2019.2962586

Sule, D. (2014, January 1). Importance of Forensic Readiness. Retrieved February 20, 2023, from ISACA website: https://www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness

Sunny, D. (2024, July 3). Cyber attack on South Africa's laboratory service puts healthcare at risk. Retrieved October 13, 2024, from Techpoint.Africa website: https://techpoint.africa/2024/07/03/cyber-security-attack-south-africas-healthcare/

Tan, J. (2001). *Forensic Readiness*. Retrieved from http://project.honeynet.org

Van den Broeck, J., Argeseanu Cunningham, S., Eeckels, R., & Herbst, K. (2005). Data Cleaning: Detecting, Diagnosing, and Editing Data Abnormalities. *PLoS Medicine*, *2*(10), e267. https://doi.org/10.1371/journal.pmed.0020267

Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, *8*, 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514

Yan, W., Shen, J., Cao, Z., & Dong, X. (2020). Blockchain Based Digital Evidence Chain of Custody. *ACM International Conference Proceeding Series*, 19–23. https://doi.org/10.1145/3390566.3391690

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. M. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, *92*, 265–275. https://doi.org/10.1016/J.FUTURE.2018.09.058

Yassin, W., Abdollah, M. F., Ahmad, R., Yunos, Z., & Ariffin, A. (2020). Cloud Forensic Challenges and Recommendations: A Review. *OIC-CERT Journal of Cyber Security*, *2*(1), 19–29. Retrieved from https://www.oic-cert.org/en/journal/vol-2-issue-1/cloud-forensic-challenges-and-recommenda.html

Zainudin, N. M., Hasbullah, N. A., Wook, M., Ramli, S., Afiza, N., & Razali, M. (2022). Digital Forensic Readiness for Cyber Security Practitioners: An Integrated Model. *Journal of Positive School Psychology* , *6*(3), 8423–8433–8423–8433. Retrieved from https://www.journalppw.com/index.php/jpsp/article/view/5108

Zia, T., Liu, P., & Han, W. (2017). Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT). *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 1–7. https://doi.org/10.1145/3098954

Appendix

Appendix 1: Research Instrument: Questionnaire

University of Cape Town
Department of Information Systems
Leslie Commerce Building
Upper Campus
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280

Security Operations Centre Forensic Readiness Survey

Digital Forensic Readiness is defined as a discipline within digital forensics that increases the availability and quality of raw data needed to perform an investigation post-mortem (Daneilsson & Tjostheim, 2004).

Thank you for participating in this survey. The purpose of the study is to investigate factors affecting digital forensic readiness (DFR) in organizations that are running Security Operations Centers (SOC). The survey will take approximately 20 minutes. Participation in the survey is voluntary and you can choose to exit at any time.

A. General Information - Demographics						
1.	Job Title	CIO	CISO	IT Security Manager	SOC Analyst	Other
2.	Age	<21	21-30	31-40	41-50	51 +
3.	Formal Qualifications	National Diploma	Degree	Honors	Masters	Other
4.	Industry Related Certifications	None	CISSP	CISM	CEH	Other
CISSP-Certified Information Systems Security Professional; CISM - Certified Information Security Manager; CEH – Certified Ethical Hacker						
5.	Years of Experience in the field	0-3	4-10	11 - 15	16 - 20	21 +

B. Management Support					
Please indicate your agreement/disagreement with the statement below (1=Strongly Disagree; 2=Disagree; 3=Somewhat Agree; 4=Agree; 5=Strongly Agree)					
6. Senior management in my organization play a leading role in the formulation and implementation of digital forensic readiness policies	1	2	3	4	5
7. Senior management actively participate in incident response planning	1	2	3	4	5
8. Senior management allocates the required funding for digital forensic tools	1	2	3	4	5

C. Policies, Processes, and Procedures					
Which of the following Digital Forensic Policy guidelines do you use in your organization. Please indicate your selection with an X					
National Institute of Standards and Technology (NIST)		ISO\IEC 27037/2012		ISO\IEC 27043:2015	
Other (Please specify)					
Please indicate your agreement/disagreement with the statement below (1=Strongly Disagree; 2 = Disagree; 3= Somewhat Agree; 4= Agree; 5=Strongly Agree)					
9. The digital forensic readiness policy is reviewed and updated annually	1	2	3	4	5
10. Digital forensics is explicitly addressed in our incident response plan	1	2	3	4	5
11. There are documented standard operating procedures for acquiring and preserving digital evidence	1	2	3	4	5

D. Legal Requirements					
Which of the following legal **and regulatory requirements for evidence or data handling, both local and international, are you familiar with. Please indicate your selection with an X**					
Protection of Personal Information Act (POPIA)		Cybercrime Act		Health Insurance Portability and Accountability Act (HIPAA)	
General Data Protection Regulation (GDPR)		Electronic Communication and Transaction Act		**Other (Please Specify)**	
Please indicate your agreement/disagreement with the statement below (1=Strongly Disagree; 2 = Disagree; 3= Somewhat Agree; 4= Agree; 5=Strongly Agree)					
12. I am aware of the legal requirements for evidence handling during an investigation.	1	2	3	4	5
13. I am aware of procedures in my organization for reporting security breaches to law enforcement or regulatory bodies.	1	2	3	4	5
14. I am aware of penalties that my organization can incur in the event of a data breach.	1	2	3	4	5

E. Forensic and Cybersecurity Technologies					
Which of the following Digital Forensic technologies are you familiar with. Please indicate your selection with an X					
Detego		Encase		Autopsy	
Volatility		FTK Forensic Toolkit		**Other (Please specify)**	
Which of the following Security tools do you use in your organization:					
Security Incident and Event Monitoring (SIEM)		Security Orchestration, Automation and Response (SOAR)		**Other (Please specify)**	
Endpoint Detection and Response (EDR)		Xtended Detection and Response (XDR)			
Please indicate your agreement/disagreement with the statement below (1=Strongly Disagree; 2 = Disagree; 3= Somewhat Agree; 4= Agree; 5=Strongly Agree)					
15. The integration of forensic tools with security tools has reduced incident response time	1	2	3	4	5
16. The integration of forensic tools with security tools has improved my organization's overall security posture	1	2	3	4	5
17. The integration of forensic tools with security tools has led to improved accuracy of forensic analysis	1	2	3	4	5

F. Technical Skills					
Please indicate your agreement/disagreement with the statement below (1=Strongly Disagree; 2 = Disagree; 3= Somewhat Agree; 4= Agree; 5=Strongly Agree)					
18. My organization has skilled digital forensics analysts within a SOC	1	2	3	4	5
19. Analysts can extract and analyze digital evidence contained in different devices	1	2	3	4	5
20. There is a high level of understanding of digital forensic readiness amongst SOC analysts	1	2	3	4	5
21. Analysts can effectively communicate findings and technical details to non-technical stakeholders	1	2	3	4	5

G. Training					
Please indicate your agreement/disagreement with the statement below (1=Strongly Disagree; 2 = Disagree; 3= Somewhat Agree; 4= Agree; 5=Strongly Agree)					
22. SOC analysts receive training in digital forensics and evidence handling	1	2	3	4	5
23. There is budget allocated for continuous skills development in digital forensics	1	2	3	4	5
24. Certifications are encouraged or required for digital forensics staff	1	2	3	4	5
25. There are awareness programs held to ensure all staff members understand what to do in case of a cyber incident.	1	2	3	4	5

Other Comments
If there are any comments, please provide them in this section.

Comment:

_____
_____
_____
_____

COMPLETE

Thank you for completing the questionnaire. If you have any queries please contact Boitumelo Nkwe on Tel: 0731635612 or by email: nkwboi002@myuct.ac.za

Appendix 2: Consent Form

University of Cape Town
Department of Information Systems
Leslie Commerce Building
Upper Campus
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280

Request to conduct research: Participation form

Dear prospective participant

I am currently working towards a master's degree in information systems at University of Cape Town. As part of the fulfilment of my studies, I have chosen to conduct a study titled: A Conceptual Framework for Digital Forensic Readiness in Security Operation Centres: A South African Study. The objective of this study is to improve the digital forensic readiness of security operations centres across South Africa. This research has been approved by the Ethics in Research Committee of the faculty of Commerce.

The online questionnaire is designed to ensure the anonymity of your response. You will not be requested to supply any personal identifiable information. Your participation in this research is voluntary. The questionnaire will take approximately 10 minutes to complete. You can choose to withdraw your participation at any stage. If you have any queries, please feel free to contact the researcher on Tel: 0731635612 or by email: nkwboi002@myuct.ac.za

Your participation in this study will be greatly appreciated.

Sincerely

Boitumelo Nkwe
Researcher
Department of Information Systems
University of Cape Town
Contact: nkwboi002@myuct.ac.za

Prof. Michael Kyobe
Research Supervisor
Department of Information Systems
University of Cape Town
Contact: Michael.Kyobe@uct.ac.za

Appendix 3: Ethics Clearance Form

UNIVERSITY OF CAPE TOWN
IYUNIVESITHI YASEKAPA • UNIVERSITEIT VAN KAAPSTAD

2024/01/30

COM/00580/2024

RE: Research Ethics Committee Project Approval Letter

Dear Boitumelo Nkwe,

Your application for ethics review of your project titled

Factors Influencing Digital Forensic Readiness in Security Operations Centers: The Case of South Africa

has been reviewed and evaluated by the

Commerce Research Ethics Committee.

You may proceed with your research project titled:

Factors Influencing Digital Forensic Readiness in Security Operations Centers: The Case of South Africa

Please note that should:

(i) any serious or adverse effects to participants occur and/or,

(ii) aspect(s) of your current project change and/or

(iii) any unforeseen events that might affect continued ethical acceptability of the project occur then you should immediately report this to the approving REC. You may be required to submit an amendment to this application, in order to determine whether the changed aspects increase the ethical risks of your project.

Based on the information supplied your application has been successful and is approved.

Please note the following additional conditions associated with this approval:

(i) Approval conditional on space being provided under the consent declaration for the respondent to e-sign/type name and date their consent to participate

Regards,

Commerce Research Ethics Committee.