A Coordinated Communication and Awareness Approach towards the enhancement of Information Security Incident Management:

An Empirical Study of Ethiopian Organisations

By

ELIAS WORKU WORDOFA

(50839489)

Submitted in accordance with the requirements for

The degree of

DOCTOR OF PHILOSOPHY

In the subject

INFORMATION SYSTEMS

At the

University of South Africa

Supervisor: **PROFESSOR KESHNEE PADAYACHEE**

04 August 2023

Submitted

DECLARATION

Name: **Elias Worku Wordofa**

Student number: **50839489**

Degree: **PhD in Information Systems**

Supervisor: **Professor Keshnee Padayachee**

Title of the Research: **A Coordinated Communication and Awareness Approach towards the enhancement of Information Security Incident Management: An Empirical Study of Ethiopian Organisations**

I hereby declare that:

- The above thesis is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

- I submitted the thesis to originality checking software and that it falls within the accepted requirements for originality.

- I have not previously submitted this work, or part of it, for examination at UNISA for another qualification or at any other higher education institution.

- All data presented in this work is neither fabricated nor falsified.

_______________________________ August 04, 2023

SIGNATURE DATE

ACKNOWLEDGEMENTS

First, thanks to the almighty God for providing me with the endurance to enable me to pass through a series of vicissitudes and challenging circumstances. I would sincerely and respectfully like to thank Professor K Padayachee (my supervisor) from the University of South Africa (UNISA) for her constructive leadership, enthusiasm, immense knowledge, and supervision from the commencement of the research, during the whole process up to the end of the research endeavours. She was extremely supportive in providing critical academic feedback, identifying suitable methodology and advising the utilisation of appropriate technical aspects. Moreover, I appreciate her encouragement to publish articles in peer-reviewed journals which served as a lesson and an honour in my career. My thanks also go to Professor Isabella M. Venter from the University of Western Cape for reading, reviewing and providing comments on the draft thesis that ultimately has improved the quality of the thesis.

My thanks go to the UNISA for the academic study opportunity and bursary funding support that allowed me to undertake the research activities. I would like to thank Dr Solomon Mekonnen for his inspiration, sharing his preceding experiences and lessons at various phases of the journey of the study. In addition, I would gratefully like to thank Mr Fasika Tesfaye for his support and kind cooperation in the process of the implementation of the model and the interface prototype. My special thanks also go to my colleague, Dr Yohannes Shiferaw, for his guidance and advice on some of the quantitative, statistical, and technical aspects of the study. Also, my study would not have been complete without the strong encouragement of family, friends, and colleagues.

Finally, I am grateful to my employer, Addis Ababa University (AAU) and the Ministry of Education (MOE) of Ethiopia for providing me with the opportunity to study and the sponsorship offer.

A Coordinated Communication and Awareness Approach towards the enhancement of Information Security Incident Management: An Empirical Study of Ethiopian Organisations

by

Elias Worku Wordofa

Abstract

Information Security Incident Management is an essential process within an organisational context, as it provides a strategic approach towards monitoring and containing incidents and vulnerabilities. The coordination of communication and awareness efforts in the process of Information Security Incident Management has been identified as a critical means of enhancing information security protection in organisations. However, the arbitrary process involved in creating a shared understanding within the context of Information Security Incident Management often negates the effective containment of incidents. This study aims to explore the nuances of organisational information security concerning the coordination of communication and awareness efforts among organisational stakeholders towards achieving a shared, interactive, and participatory management of information security incidents in organisations.

The Design Science Research methodology was applied to conceptualise and design an appropriate artefact to respond to the core research questions. The major research question considered was: *How can the coordination of awareness and communication efforts be enhanced to support the processes of ISIM?* The study involved two distinct phases – the first phase (Phase I) involved conducting an exploratory study to assess the extent of the application of communication and awareness efforts within purposively selected organisations in Ethiopia, while Phase II involved the design and development of an artefact to address the problem domain identified in Phase I. Ethiopia was selected for this study as it typifies regions where the level of cyber security advancement is limited and because a study in this context would be more relevant in providing applicable empirical data to the research problem.

According to the findings of the exploratory study in the organisations sampled, it was identified that reporting, communication, and awareness efforts within Information Security Incident Management were largely uncoordinated. Moreover, digital systems to support information security communication were limited. The findings from the exploratory data (i.e., Phase I) prompted the basis for the proposal of a conceptual model designated a **C**oordinated **C**ommunication and **A**wareness approach towards enhancing **I**nformation **S**ecurity **I**ncident **M**anagement (CCA^{ISIM}) in order to address the core research problem (i.e., the basis of Phase II).

The CCA^{ISIM} model unifies and subsumes a dyad of theories of situational awareness and the Interactive Model of Communication towards enhancing the coordination of awareness and communication efforts in Information Security Incident Management. The proof-of-concept of the conceptual model was verified via a simulated interface prototype in Phase II. The model and the proof-of-concept prototype were evaluated by a selection of experts and end-users from Ethiopian organisations. The sampling frame of participants for Phase II of the study was recalibrated as the original sample was deemed unsuitable for the subsequent phase. The evaluation necessitated the inclusion of expertise in information security. Therefore, the sampling frame for Phase II considered more mature organisations within the information security domain. The model and prototype were evaluated based on the established constructs of information systems acceptance proffered by the Technology Acceptance Model (TAM). Generally, the model and prototype achieved a good acceptability rating and can potentially be applied in organisations that are vulnerable to information security incidents.

The CCA^{ISIM} model derived in this study has implications for both theory and practice, including underscoring the importance of the theories of Shared Situational Awareness and the Interactive Model of Communication with respect to unifying diverse stakeholders (including end-users) in order to promote a proactive and participatory approach in managing information security incidents. The application of the dyad concepts improves the reporting capacity of users in a coordinated manner in a continuum from individual to shared levels which aids in developing a unified understanding of the processes involved in an information security incident response. The research design also allowed for new empirical data to be captured with respect to Information Security Incident Management practices within several contexts.

Moreover, this empirical evidence may assist organisations in evaluating their information security practices. The findings and recommendations may not be generalisable to all contexts. There is a need for further case studies to evaluate the model within a real-world context.

Keywords

Information Security, Information Security Incident Management, Communication, Awareness, Situational Awareness, Shared Situational Awareness, Interactive Model of Communication, Incident Management, Socio-technical Solution, Information Security Incident Response Teams, Incident Response.

Table of Contents

List of Figures

List of Tables

Definition of Key Terms

Asset is “any resource that has value to the organisation” (ISO/IEC, 2005, p. 2).

Cyber security is “the protection of the interests of a person, society or nation, including their information and non-information-based assets that need protection from the risks relating to their interaction with cyberspace” (Reid & Van Niekerk, 2014, p. 1).

Information is “assets or data that should be documented and that has value or potential value” which contains “a message, usually in the form of a document or an audible or visible communication” (Oppenheim et al., 2004, p. 159).

Information Security is “the preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved” (ISO/IEC, 2005, p. 2).

Information Security Event is “an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant” (ISO/IEC, 2005, p. 2).

Information Security Forensics is “an application of investigation and analysis techniques to capture records and analyse information security incidents” (ISO/IEC, 2016, p. 1).

Information Security Incident is “an incident which is a violation of computer security policies, acceptable use policies, or standard computer security practices” (Cichonski et.al, 2012, p. 65). An incident “is indicated by a single or a sequences of unwanted or unanticipated information security events that have a significant probability of compromising business operations and risking information security” (ISO/IEC, 2016, p. 2).

Information Security Incident Management (ISIM) encompasses the management of both information security incidents and information security vulnerabilities (ISO/IEC, 2016, p. VI). ISIM is a management program that plans and prepares for security incidents. It involves the allocation of resources required for incident control.

Information Security Incident Response Team (ISIRT) is “a group of properly trained and trusted members of the organisation that handles information security incidents during their lifecycle” (ISO/IEC, 2016, p.1). The ISIRT is accountable for “providing incident response services to part or all of an organisation. The team receives information on possible incidents, investigates them, and takes action to ensure that the damage caused by the incidents is minimised” (Cichonski et.al, 2012, p. 65).

Information Security Management Systems (ISMS) represents a “part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security” (ISO/IEC, 2005, p. 2).

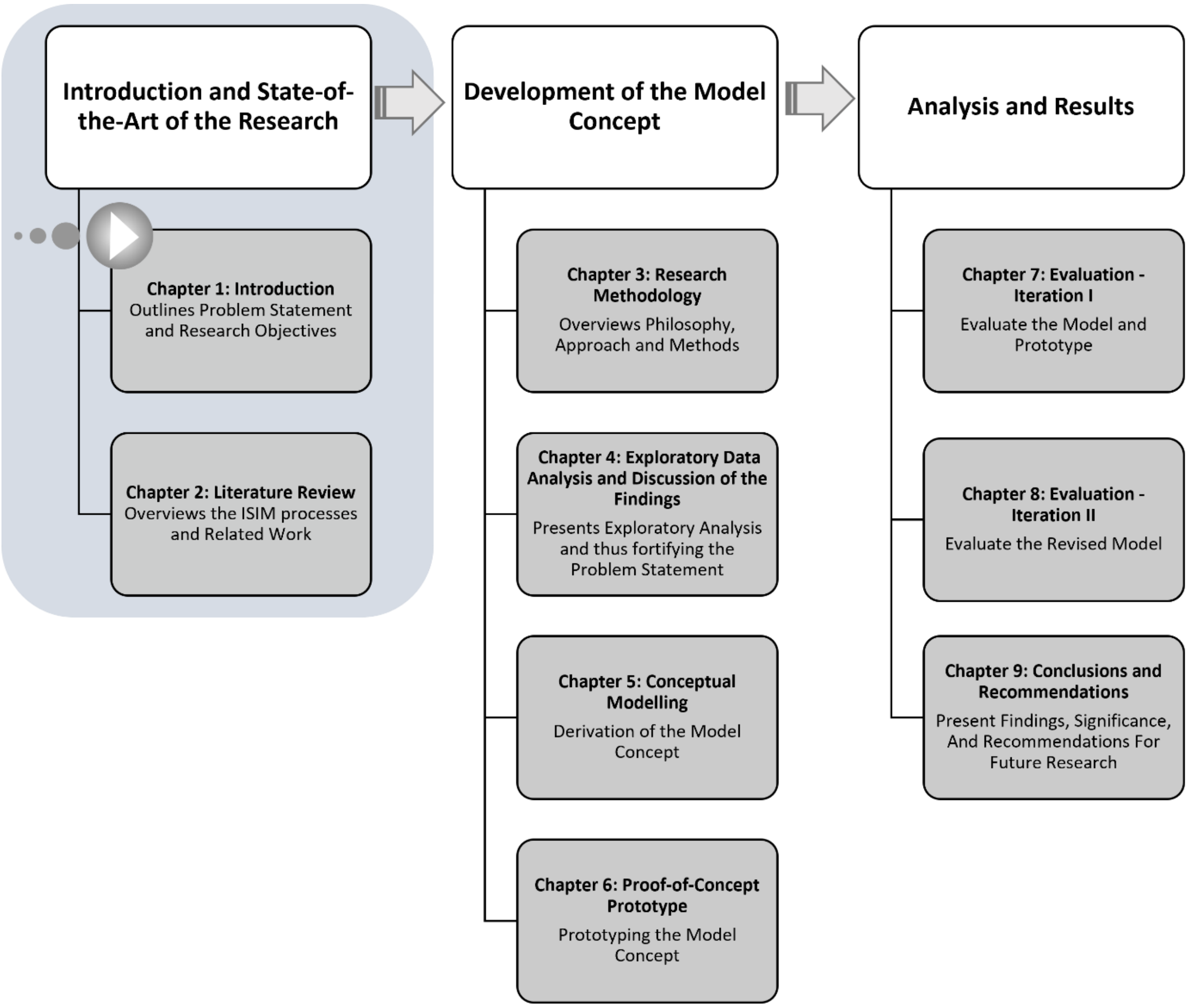
Organisational Communication as is “the study of sending and receiving messages that create and maintain a system of consciously coordinated activities or forces of two or more persons” (Tompkins, 1984, pp. 662-663).

Acronyms

- **CCA^{ISIM}**: **C**oordinated **C**ommunication and **A**wareness approach towards enhancing **I**nformation **S**ecurity **I**ncident **M**anagement
- **CISID:** Central Information Security Incident Database
- **COBIT:** Control Objectives for Information and Related Technologies
- **DOS:** Denial of Service
- **DSR:** Design Science Research
- **ENISA:** European Union Agency for Cyber security
- **HCI:** Human Computer Interaction
- **ICT:** Information and Communications Technology
- **IDP:** Intrusion Detection and Prevention
- **IDS:** Intrusion Detection System
- **IEC:** International Electro technical Commission
- **INSA:** Information Network Security Agency
- **IMC:** Interactive Model of Communication
- **IT:** Information Technology
- **ITIL:** Information Technology Infrastructure Library
- **IOT:** Internet of Things
- **IS:** Information Security
- **ISIM:** Information Security Incident Management
- **ISIRT:** Information Security Incident Response Team
- **ISP:** Internet Service Provider
- **ISO:** International Organisation for Standardisation
- **MCIT:** Ministry of Communication and Information Technology in Ethiopia
- **MINT:** Ministry of Innovation and Technology
- **POC:** Point of Contact
- **POS:** Point of Sale
- **SA:** Situational Awareness
- **TAM:** Technology Acceptance Model
- **UML**: Unified Modelling Language
- **VPN:** Virtual Private Network

CHAPTER ONE

RESEARCH ROAD MAP


Introduction and State-of-the-Art of the Research
Chapter 1: Introduction
Outlines Problem Statement and Research Objectives
Chapter 2: Literature Review
Overviews the ISIM processes and Related Work
Development of the Model Concept
Chapter 3: Research Methodology
Overviews Philosophy, Approach and Methods
Chapter 4: Exploratory Data Analysis and Discussion of the Findings
Presents Exploratory Analysis and thus fortifying the Problem Statement
Chapter 5: Conceptual Modelling
Derivation of the Model Concept
Chapter 6: Proof-of-Concept Prototype
Prototyping the Model Concept
Analysis and Results
Chapter 7: Evaluation - Iteration I
Evaluate the Model and Prototype
Chapter 8: Evaluation - Iteration II
Evaluate the Revised Model
Chapter 9: Conclusions and Recommendations
Present Findings, Significance, And Recommendations For Future Research

CHAPTER 1: INTRODUCTION

1.1. Background

The prevalence of information security incidents has been a critical concern for many organisations; particularly for those operating in the Information and Communication Technology (ICT) sector, as it requires a substantial capital investment in terms of both technology and human expenditures (Khando, Gao, Islam, & Salman, 2021). Furthermore, the sector develops large scale technologies that transform society and economies (Holtgrewe, 2014). These concerns strongly require proactive mitigation and information security strategies to counter information security incidents. Information security threats could arise from various sources either externally or internally (Syahrial, Prabowo, Budiastuti, & Gaol, 2019). According to a recent report by International Business Machines (IBM), the number of information security incidents escalated by 33% in 2021, compared with 2020 (IBM Security, 2022). The world is on the brink of a new technological revolution—the 4th industrial revolution—in that processes, technology, products, and information are evolving swiftly (Rapanyane & Sethole, 2020). These large-scale interconnections of computers, cyber-data, and information exchange across the globe have triggered vast potential threats to the protection of information and the occurrence of information security incidents is increasing (Jang-Jaccard & Nepal, 2014; Li & Liu, 2021). Technologies such as smartphones, laptops, and Internet of Things (IoT) are ubiquitous and have made information security a necessity (Kaufhold et al., 2021; Perera, Zaslavsky, Christen & Georgakopoulos, 2013). These new technologies pose new attack vectors for information security incidents. Although most organisations have state-of-the-art information security systems, the installation by itself does not guarantee organisations that they can operate in a vacuum without the threat of vulnerabilities (Ahmad, Hadgkiss & Ruighaver, 2012; Siponen, Pahnila & Mahammod, 2007). Therefore, it is an essential requirement for organisations to proffer proactive and strategic approaches to manage information security incidents effectively.

As organisations are highly dependent on ICT, information security incidents could be either intentional or unplanned, unsolicited, or unforeseen which may compromise information systems security (Miloslavskaya & Tolstoy, 2020; Mirtsch et al., 2021). Information Security Incident Management (ISIM) enables organisations to systematically identify, respond and manage information security incidents (ISO/IEC, 2016). Planning, detection, reporting, assessment, and response processes are critical steps towards preventing information security incidents in a proactive approach (Miloslavskaya & Tolstoy, 2020). The coordination of communication and awareness approaches within ISIM positively supports the process of mitigation of either existing or future incidents in organisations (Ahmad et al., 2021). However, the process of ISIM within organisations is beset with several challenges. These include lack of training, lack of documentation, lack of planning, lack of post-incident monitoring, poor coordination between the security and control personnel, lack of management commitment, lack of applicable tools for incident management, and poor collaboration (Line & Albrechtsen, 2016). The variation in perspectives and priorities for ISIM between managers and technical personnel is also a contributory challenge (Line, Moe, & Heegaard, 2016). Consequently, these issues call for further studies to be conducted with the aim of engendering a coordinated, collaborative and proactive mechanism within the realm of ISIM (Ahmad et al., 2021; Nyman & Große, 2019). Accordingly, this study attempted to explore the veracity and prevalence of these claims such as the lack of collaboration and awareness.

Line et al. (2016) stressed that further studies should be undertaken to examine the role of communication and participation among stakeholders within the practice of ISIM. While collaborative-based incident management benefits organisations, the lack of coordinated approaches hinders organisations in managing incidents effectively (Oriola, Adeyemo, Papadaki & Kotzé, 2021). Likewise Ahmad et al. (2015) asserts that there are limited studies that contemplates how the practices of incident response teams can be utilised for security process improvement and that most researchers pay more attention to the response process of ISIM instead of the “lessons learnt” from information security incidents. There has been a call for further studies to evaluate the comprehensive organisational factors involved in order to understand the impact on learning and ISIM aside from threat management tasks (Thangavelu et al., 2021). The study at hand proffered that enhancing the awareness and communication efforts within the context of ISIM may be a strategy for addressing some of the challenges articulated. In the study at hand, communication refers to information sharing, reporting and mutual understanding of information security incidents that occur within organisations. Awareness of information security incidents refers to attaining a shared or mutual understanding of information security incidents among stakeholders (Metzger et al., 2011).

Awareness refers to knowledge, attitude, and skill that may be leveraged to protect the information assets of organisations (Ahmad et al., 2021). This study attempts to couple communication and awareness efforts in an integrated modality towards improving stakeholder engagement within an information security incident scenario.

The study at hand is significant as there is a consideration of information security from a socio-technical approach which involves an examination of the participation of all stakeholders rather than a purely technical viewpoint. The Design Science Research (DSR) methodology was applied to address the problem of poor coordination of awareness and communication efforts among stakeholders in ISIM. Initially, an exploratory study was conducted to confirm the problem statement. Moreover, a model and an interface prototype were developed as a proof-of-concept approach to address the problem statement. Then an evaluation was conducted to assess the fitness for purpose of the model and prototype. Thus, the study contributes to the ISIM processes in improving the coordination of awareness and communication protocols and accordingly the cooperation among stakeholders towards minimising the impact of information security incidents.

1.2. Motivation for the Study

The motivation for this study emanated from an overview of the related work conducted within ISIM where the practice of information security incident standards is inconsistent, lacks diverse organisational context and limited empirical validity which requires further study (Alshaikh et al., 2018; Tøndel, Line & Jaatun, 2014). Thus, this study considers the human-centric factors such as communication and awareness relative to security incidents within the empirically studied organisations. The aim was to address the gap with an empirical investigation considering the facets of reporting, communication, and awareness of security incidents among organisational users to enhance the management of information security incidents in a comprehensive, proactive, and collaborative approach. Despite the efforts by some organisations to utilise ISIM standards, the integration of awareness and communication components was not adequately addressed towards proactive ISIM. Managing information security incidents is challenging and Information Security Incident Response Teams (ISIRT) work towards swiftly restoring operations back to their default state; however, poor communication and awareness strategies can thwart that process. Therefore, this study aims to contribute to finding a solution space to apply awareness and communication strategies in an effective manner thus enabling organisations to cope with information incidents expeditiously.

1.3. Problem Statement

The increasing interconnectedness of the digital world coupled with threats to information security and the lack of organisational preparation for ISIM is a significant concern (Johnson, 2006; Miloslavskaya & Tolstoy, 2020). Although organisational investment and efforts in the prevention of information security incidents exist, encountered incidents are escalating which indicates a gap within organisational incident management processes (Thangavelu, Krishnaswamy, & Sharma, 2021).

ISIM is particularly challenging as it involves both technical and sociological dimensions (Ahmad, Hadgkiss, & Ruighaver, 2012). Although most organisations attempt to combat incidents, the existing organisational process lacks the all-inclusive awareness of threats among stakeholders which is considered to be a limiting factor (Thangavelu et al., 2021). Thus, while some information system concerns are related to behavioural factors (Bariff & Ginzberg, 1982), a comprehensive approach that integrates human, system, organisational, behavioural, and technical factors in ISIM is crucial to containing information security incidents in a coordinated manner (Ahmad et al., 2012).

While these requirements are essential, it is not clear how the elements of communication and awareness can be further enhanced where all stakeholders have a shared understanding within an information security incident scenario. Extant ISIM reporting and awareness schemes do not integrate information security policies, processes and active incidents particularly with the participation of stakeholders and end-users (O’Brien et al., 2020). Some studies have explored ISIM from a socio-technical (Charitoudi, 2013), governance (Da Veiga & Eloff, 2007) and a risk management perspective (Humphreys, 2008), but further studies are required to empirically examine the contextual situations of information security awareness from diverse organisational settings (Alshaikh et al., 2018).

To manage incidents properly, enhancing the communication and analytical skills of users has a significant value for advancing understanding and proactive protection (Werlinger et al., 2010). However, the practice of awareness and threat management is conducted in a disjointed manner without due consideration of metacognitive awareness (Padayachee & Worku, 2020; Thangavelu et al., 2021). Despite the existence of a few studies (Ahmad et al., 2015; Bulgurcu et al., 2010; Padayachee, 2017) that examine the coordination of awareness and communication efforts within the ISIM process, it is important to explore and empirically study how the role of communication, coordination, and information sharing influence the information security incident response task (Ioannou et al., 2019; Nyre-Yu et al., 2019). A coordinated approach to information security communication and awareness efforts in organisations requires further studies to be conducted within a real-world context (Padayachee & Worku, 2020).

From an awareness perspective, the situational awareness model has been recognised as an appropriate framework towards enhancing ISIM processes (Ahmad et al., 2021). Padayachee and Worku (2017) attempted to include situational awareness within ISIM but the integration of communication and reporting components was limited. In a related study, Padayachee and Worku (2020) considered the application of situational awareness within ISIM from an organisational perspective, however, the model advanced was not empirically tested. Husák et al. (2022) developed a visually enabled web-based system by applying the situational awareness model to address the lack of procedures that manage situational awareness and decision-making; however, the submission fails to consider the reporting and communication of incidents. Similarly, Ahmad et al. (2021) proposed a model based on situational awareness for incident handling; however, this study focused on the management perspective by using past incidents with no involvement of end-users such as non-IT personnel and junior personnel in the study. Thus, related studies are limited in terms of incorporating end-users, examining ISIM from a collaborative perspective and integrating communication mechanisms within the processes of ISIM.

Accordingly, this study will consider the problem of involving all stakeholders including end-users within the processes of ISIM. Consequently, the study aims to examine the nuances of ISIM processes via the lens of awareness and communication formation to improve the understanding of incident information among all stakeholders thereby improving the responsiveness to information security incidents. As the prevalence of internet connectivity grows in Africa so too will the rate of cybercrimes (Van Niekerk, 2017). Yohannes et al., (2019) who studied the case of institutions working within the finance sector in Ethiopia from the lens of ISIM, confirmed that the lack of coordination, lack of standards, and collaboration are critical challenges. Consequently, the context of Ethiopia was selected as the study area as this setting can be seen as a proxy for organisations with a low advancement of ISIM. This setting provided an ideal opportunity to examine the problems associated with poor ISIM practices. Furthermore, there was a need for empirical explorations of this nature to be undertaken within the Ethiopian context.

1.4. Research Questions

The main research question is: *How can the coordination of awareness and communication efforts be enhanced to support the processes of ISIM?*

The minor research questions that guided the study are:

- **RQ1**: To what extent are strategies for awareness and communication efforts integrated into organisational ISIM practices?
- **RQ2**: How do organisations integrate communication and awareness efforts into their ISIM processes and practices?
- **RQ3**: To what extent is the integration of stakeholders' and end-users' participation instigated within the processes of incident awareness and communication efforts within ISIM practices?
- **RQ4**: How should organisations enhance the coordination of awareness and communication efforts within the processes of ISIM practices?

1.5. Research Objectives

The main objective of this study is to explore and develop a conceptual model towards the enhancement of coordination awareness and communication efforts to support the processes of ISIM.

The specific objectives that guided the main research objective are:

1. To assess the integration of strategies for communication and awareness efforts within ISIM practices.
2. To identify the strategies leveraged by organisations to integrate communication and awareness efforts within their ISIM processes and practices.
3. To assess the integration of stakeholders' and end-users' participation within the processes of incident awareness and communication efforts within ISIM practices.
4. To develop and evaluate a conceptual model to enhance the coordination of communication and awareness efforts within the processes of ISIM practices.

The aim of this research involves the exploration and derivation of a solution space to navigate the complex issues of ensuring effective awareness and communication efforts within ISIM practices. The coordination of communication and awareness efforts is achieved through an inclusive nexus of users to meet the objectives of ISIM processes.

1.6. Significance of the Study

This study will have both theoretical and practical implications for the ISIM discipline. The study will propose a novel conceptual model to enhance the communication and awareness efforts to support the ISIM processes and practices.

Since there existed limited synthesised knowledge about integrated methods for enhancing information security incident awareness in a more systematic approach (Khando et al., 2021), the study will contribute significantly by indicating appropriate approaches that depict the awareness and communication efforts for ISIM in organisations. Studies from this perspective will have a substantial impact on enhancing the information security management behaviour of employees in organisations regarding information security threats (Jang-Jaccard & Nepal, 2014; Li & Liu, 2021). The study at hand will assist in framing the theoretical underpinning related to awareness and communication efforts within an organisational context.

The planned and coordinated communication of information security incidents in organisations supports the proactive management of incidents which enhances effective routine operations (Posthumus & Von Solms, 2004). In addition, the strategy supports executives and decision-makers in the development of all-encompassing policies for ISIM through the integration of communication and awareness components by instigating the participation of all users.

Typically, organisations practice information security awareness efforts in a largely uncoordinated manner without due consideration to standards (Ab Rahman & Choo, 2015; Yohannes et al., 2019). In the organisational dimension depicted in the study by Siponen, (2000), stakeholders in the organisation (end-users, management, decision-makers, technical experts) can play a significant role in the process of awareness creation and communication of incidents. The approach proposed by this research supports the stakeholders' awareness in an organisation by instigating participation in the process of awareness and communication efforts.

1.7. Purpose of the Study

Refining the process of reporting, planning, and responding to incident events can make a significant contribution towards enhancing the management of incident information in organisations. This study purports that improving the communication and awareness formation within organisations is an important vector towards improving the management of incident information. Thus, the purpose of this study is to explore the nuances of communication and awareness efforts of incident information in organisations. Furthermore, the study aims to derive an approach to improve the coordination of communication and awareness efforts of incident information. To achieve this purpose and address the research problems, the study employs the DSR methodology. The first phase, Phase I of the study, aims to explore the extent of the problem while the second phase, Phase II, derives a solution to the problem identified in Phase I with the purpose of improving the coordination of awareness and communication efforts during an information security incident scenario. Both phases of the study involve purposively selected organisations from Ethiopia.

1.8. Research Design

The research approach for this study is framed within the context of the DSR approach. The DSR approach was applied to conceptually develop a model and a prototype for the problem identified. The study is comprised of two phases. Phase I involved conducting an exploratory study to define the problem domain and establish the significance of the problem domain in response to research questions, **RQ1**, **RQ2**, and **RQ3**. Phase II involved designing and evaluating the model and prototype designed in response to the problem identified in Phase I, thereby responding to research question **RQ4**. Research questions **RQ1**, **RQ2** and **RQ3** are addressed through the exploratory study which aimed to confirm the problem statement and to identify the objectives of the study. Research question four (**RQ4**) was addressed using modelling and prototyping techniques. The developed model and prototype were evaluated by security experts and end-users.

The study employed various methods for data collection – surveys, interviews, and document analysis. Recruitment of participants involved purposive sampling of respondents from organisations based in Ethiopia. The selection of participants was based on proximity to the research study. In Phase I, organisations from an array of technology-oriented industries were purposively selected where respondents such as information security experts and end-users working in various positions within the organisations were interviewed. Phase II considered a similar domain of organisations; however, the participants selected were unrelated to the first sample, which provided a broader perspective and representation. The nature of the organisations involved consisted of technology-oriented organisations including the banking sector, security, aviation, insurance, media, and software companies.

1.9. Theoretical Framework

The discipline of information security intersects both the technical and sociological domains. Therefore, a solution space in this domain requires an appropriate exploration from a social science perspective. The framing of information systems and security from a social and technical perspective is important to explore the relationship to solve a research problem (Sarker et al., 2019). The study utilised appropriate awareness and communication theories from sociology. The study employed a situational awareness theory as a lens for developing the conceptual model. Situational awareness emphasises the processes of perception, comprehension, and projection of future incidents which is a formal approach to awareness (Endsley, 1988). As integrated organisational communication is important in all sectors (Barker & Angelopulo, 2005), the study also utilised the Interactive Model of Communication (IMC) as a protocol for communication to increase awareness. The IMC works with the exchange of messages from the sender to the receiver and vice versa in which the field of experience of both parties results in better communication (Wood, 2014). The IMC is applied because the model deals with the interaction of various stakeholders in the communication of a given message in a certain channel that allows for multi-approach communication and with the possibility of the provision of space to share the field of experience between the sender and the receiver.

1.10. Ethical Considerations

Ethical clearance was requested and provided by the ethics review committee of the College of Science, Engineering and Technology (CSET) office of the University of South Africa (UNISA) before conducting any data collection. The study involves two phases. The process of data collection for Phase I (Clearance Number: 182/EWW/2014) and Phase II (Clearance Number: 2021/CSET/SOC/025) was conducted by acquiring appropriate ethical clearance from the School of Computing Research Ethics Committee (CSET (UNISA) (See Appendix H, Appendix I and Appendix J). All participants were given consent and were given the right to withdraw without penalty. The rights to confidentiality and anonymity were also maintained. No sensitive personally identifiable information was collected. The responses were not directly associated with the participant’s identity. Phase I of the study was conducted before the COVID-19 pandemic. The data collection mechanism was conducted physically. Since Phase II was conducted during the Covid pandemic, appropriate Covid-19 protocols were maintained. To achieve that, the data collection mechanism utilised was entirely online.

1.11. The Information Security Landscape in Ethiopia

Ethiopia was selected for this study as it epitomises regions where the level of cyber security development is limited (Adane, 2022; Manyazewal, Woldeamanuel, Blumberg, Fekadu, & Marconi, 2021). This choice increases the contribution of the research as conducting an empirical study within a limited cyber security development context would provide an opportunity of gaining further insight in the issues of communication and awareness rather than a consideration of a context where the coordination of information security protocols is well-established.

In addition, the researcher as an Ethiopian national could provide deeper insight into the research context in terms of identifying and contacting organisational officers. Although Ethiopia is characterised by low internet penetration, access to ICT, digital and other internet applications has been increasing over time. According to the digital Ethiopian data portal, the country is characterised by 20.6% internet penetration (Kemp, 2021). As a result of the proliferation of ICTs, digital technologies, and the increasing application of such technologies in the business and service sectors, the demand to introduce new ICT policies and information security policies has grown significantly. In response, the Ethiopian government introduced the first information security policy in 2011, which was re-established and revised in 2013 and prepared by the Information Network Security Agency (INSA), which is the state-based security agency to control the overall ICT infrastructure and information security operations of the country. INSA is the legal governmental agency, which was established and granted authority based on an approved proclamation by the government. The agency has been responsible for controlling and protecting the overall ICT-based, digital, and internet security issues that the country has encountered since the approval of its mandate (INSA, 2013).

1.12. Limitations and Delimitations of the Study

The scope of the study is to explore how communication and awareness efforts can be systematically integrated to support ISIM processes. Although ISIM encompasses many aspects, the study is specifically focused on the enhancement of the processes of ISIM through an integration of communication and awareness practices. Although most of the theoretical and problem statements are derived in a standardised way, the study selected organisations and participants from the Ethiopian context (6 organisations and 32 participants in Phase I and 5 organisations and 37 participants in Phase II). Given the limited sample size and the context, the findings and data may not be generalisable to all organisations.

1.13. Research Contribution

This study will contribute to the ISIM domain by exploring and magnifying the awareness and communication efforts required in order to support the processes of ISIM. Given the limited number of related studies that consider communication and awareness efforts, the study will contribute substantially to systemising communication and awareness protocols within organisations. The study will also provide support for improved information security through augmenting the processes of ISIM such as planning, detection, response, and lesson learning by enhancing the collaboration of users for incident communication in an interactive manner in order to achieve a shared understanding of organisational incident patterns. The exploratory study followed by the development of a model and prototype will have tremendous significance for organisations to consider in their information security policies and practices. Since the gap between standardised procedures and uncoordinated communication of incident information is considered a challenge, the study aims to address this gap from both a theoretical and practical perspective.

The study will contribute to both research and practice. A conceptual model will be proposed and designated – A **C**oordinated **C**ommunication and **A**wareness approach towards enhancing **I**nformation **S**ecurity **I**ncident **M**anagement (**CCA**$^{\text{ISIM}}$) which contributes to integrating the communication and awareness efforts for enhancing the users' ability to proactively enable and participate in the processes of ISIM. Moreover, the model enables the enhancement of the planning, detection, response and lesson learning functions through interactive collaboration, incident information sharing and shared understanding for improved awareness of incidents.

1.14. Thesis Structure

As shown in figure 1-1, the thesis structure is composed of nine (9) chapters.

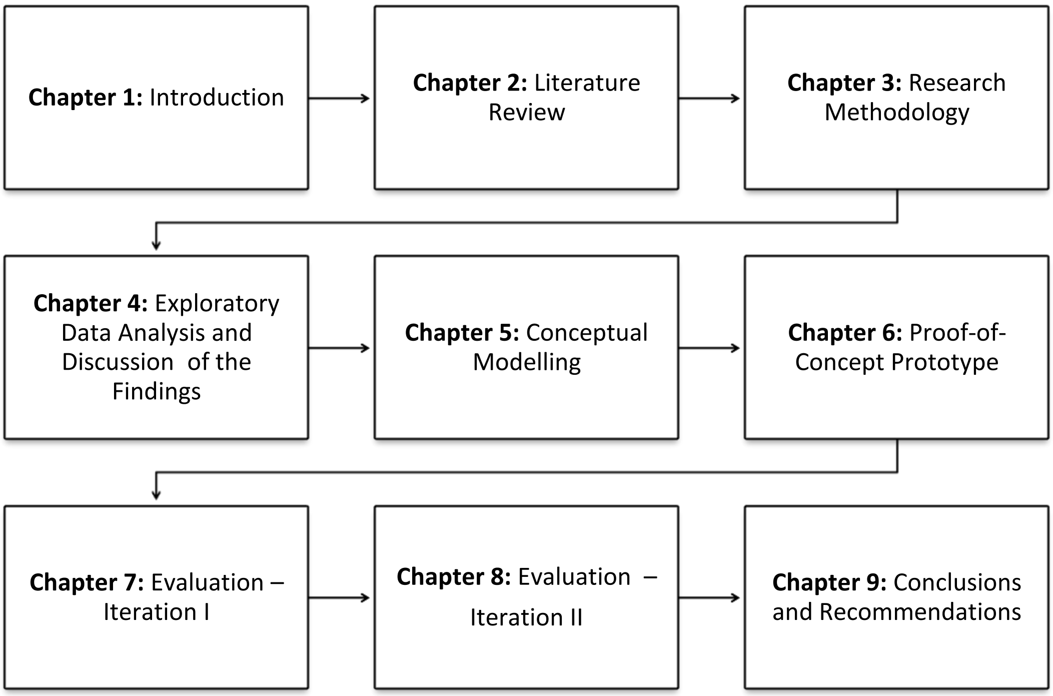

Chapter 1: Introduction
Chapter 2: Literature Review
Chapter 3: Research Methodology
Chapter 4: Exploratory Data Analysis and Discussion of the Findings
Chapter 5: Conceptual Modelling
Chapter 6: Proof-of-Concept Prototype
Chapter 7: Evaluation – Iteration I
Chapter 8: Evaluation – Iteration II
Chapter 9: Conclusions and Recommendations

Figure 1-1: Organisation of Research Chapters

The content to be covered in the research will include the following:

Chapter 1 (Introduction): This chapter introduces the topic and the problem statement. Additionally, this chapter provides the motivation, research questions, research objectives, the contribution, significance, purpose, research design, framing, and the ethical considerations of the study.

Chapter 2 (Literature Review): This chapter overviews the ISIM processes and related work. This chapter also synopses the various applicable standards and the challenges associated with ISIM, which underpins the problem statement.

Chapter 3 (Research Methodology): This chapter details the philosophy, approach, method, strategy, sampling, data analysis and collection procedures, validity and reliability measures that are applied in the research.

Chapter 4 (Exploratory Data Analysis and Discussion of the Findings): This chapter presents and analyses the collected data with respect to the preliminary research questions.

Chapter 5 (Conceptual Modelling): This chapter provisioned the derivation of the model that is the **C**oordinated **C**ommunication and **A**wareness approach towards enhancing **I**nformation **S**ecurity **I**ncident **M**anagement (CCA^{ISIM}).

Chapter 6 (Proof–Of–Concept Prototype): This chapter will implement the derived conceptual model into a simulated prototype. The interface prototype will demonstrate visually how the conceptual model may function under specific settings.

Chapter 7 (Evaluation–Iteration I): This chapter will evaluate the model and the prototype in tandem that was implemented in Chapter 6.

Chapter 8 (Evaluation–Iteration II): This chapter will evaluate the revised model based on feedback from Iteration I.

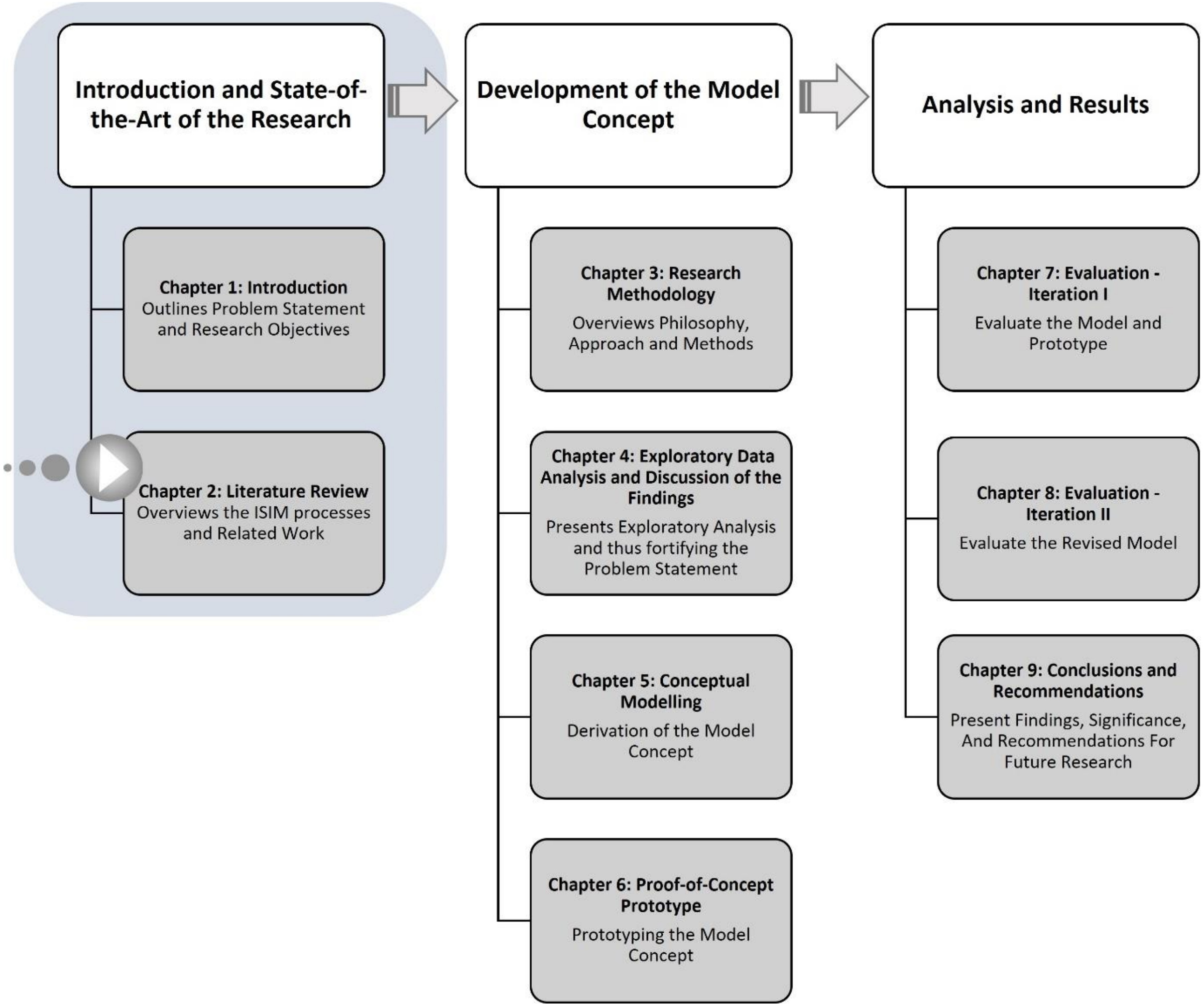
Chapter 9 (Conclusions and Recommendations): This chapter will discuss the executive summary of the research findings, its contribution, recommendations, implications for theory and practice, limitations and highlights future research endeavours to be undertaken.

1.15. Chapter Summary

The systematic coordination of communication and awareness efforts in enhancing the processes of ISIM is recognised as a crucial mechanism for containing information security incidents. The objective of this research is to explore and develop an appropriate model by integrating aspects of awareness and communication through end-users' participation to support the processes of ISIM. This chapter provided an overview of the problem statement, research questions, research objectives, and the contribution of the study. The study will contribute to the ISIM domain in identifying a solution space for enhancing awareness and communication protocols that were found to be wanting. Furthermore, the study is couched within a socio-technical perspective where the human is central to containing information security incidents which may activate a proactive approach to ISIM. Chapter 2 will provide an overview of ISIM processes, standards, and practices.

CHAPTER TWO

RESEARCH ROADMAP



Introduction and State-of-the-Art of the Research

Chapter 1: Introduction
Outlines Problem Statement and Research Objectives

Chapter 2: Literature Review
Overviews the ISIM processes and Related Work

Development of the Model Concept

Chapter 3: Research Methodology
Overviews Philosophy, Approach and Methods

Chapter 4: Exploratory Data Analysis and Discussion of the Findings
Presents Exploratory Analysis and thus fortifying the Problem Statement

Chapter 5: Conceptual Modelling
Derivation of the Model Concept

Chapter 6: Proof-of-Concept Prototype
Prototyping the Model Concept

Analysis and Results

Chapter 7: Evaluation - Iteration I
Evaluate the Model and Prototype

Chapter 8: Evaluation - Iteration II
Evaluate the Revised Model

Chapter 9: Conclusions and Recommendations
Present Findings, Significance, And Recommendations For Future Research

CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

The purpose of the literature review is to explore extant related works in order to unpack the core research problem and address the research questions by emphasising the importance of awareness formation and communication protocols toward enhancing Information Security Incident Management (ISIM). This chapter synopses the practices, processes, and standards apropos ISIM. The underlying concepts of ISIM are explored within an orientation of the background of the study (Section 2.2), an exposition of the related work (Section 2.3) and an elucidation of the recognised standards and frameworks (Section 2.4) such as the ISO/IEC 27035 standard (Section 2.5). The processes that are involved in managing information security incidents are discussed in Section 2.6. The challenges associated with ISIM within the context of communication and awareness formation, which may arise from the lack of formalised processes, lack of stakeholder involvement and poor coordination of ISIM processes, are discussed in Section 2.7. This chapter concludes in Section 2.8 by highlighting the theoretical gap which may suggest the coordination of awareness and communication efforts warranting further exploration.

2.2. Background

The social order in the current milieu is highly reliant on complex interconnected information systems which are characterised by information security threats (Mirtsch et al., 2021). Both public and private sector entities have been subjected to information security incident threats and events (Riebe et al., 2021). Evidently, leaders of both sectors are increasingly susceptible to uncertainties concerning cyber vulnerabilities and threats (Miloslavskaya & Tolstoy, 2020). According to a research study, conducted by the Identity Theft Resource Centre (ITRC), the sum of data breaches in 2021 surpassed the total sum of breaches in 2020 by 17%, which is 1,291 data breaches in 2021, in comparison to 1,108 data breaches in 2020 (Henriquez, 2021). The 2022 Annual Data Breach Report, specified that more than ten (10) million people were impacted by supply chain attacks targeting 1,743 entities (ITRC, 2023). According to the 2021 Interpol African Cyber-threat Assessment Report, African organisations have shown the highest increases (34%) of cyber-attacks from January to April, 2021 – mainly related to ransomware in which government organisations were the main target of the incident (Interpol, 2021). Similarly, according to the Deloitte 2021 study in Nigeria, even financial institutions, who have invested much in cyber security, which involves collaboration with insiders and threat actors, are vulnerable to high profile attacks (Aladenusi, 2022).

“A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems” (Sarker et al., 2020, p. 28). An information security incident is defined as a one-time or repeated occurrence of unforeseen events or incidents that have a substantial likelihood of damaging routine business operations or risking organisational information assets (ISO/ IEC, 2016). Information security threats could arise from a myriad of sources with varying damage impacts on organisations (Olav Sveen et al., 2007). The European Union Agency for Network and Information Security (ENISA) attempted to classify the attack vectors which, by their own admission, was an onerous task and the list is by no means exhaustive (Marinos & Lourenço, 2018). However, the attack vectors range from abusive content (e.g. spam), malicious code (e.g. viruses, worms, trojan, spyware), information gathering (i.e. attempts to gather information about hosts, services and accounts to identify vulnerable points, e.g. sniffing, scanning, social engineering), intrusion attempts (e.g. exploiting vulnerabilities, login attempts), intrusions (i.e. compromising accounts via unauthorised access, application compromise, bots), compromising availability (e.g. denial of service, sabotage), information content security (e.g. unauthorised access and modification of information), fraud (e.g. unauthorised use of resources, copyright infringements, masquerading, phishing) to exploitation of vulnerabilities (e.g. outdated virus signatures). Jouini et al. (2014) classified the sources of information security incidents as malicious human threats (i.e. insiders or external threats), non-malicious human actions, environmental incidents (i.e. natural disasters) and technological factors (i.e. physical processes). Palmqvist (2022) who conducted a systematic review of information security incidents found that over the past five years, most incidents were attributed to human errors while system failures were sparse, and no reported incidents were attributed to environmental concerns.

ISIM is one of the core mechanisms to control information security incidents in organisations (Dodson, 2001; Humphreys, 2008). According to ISO/IEC (2016), ISIM encompasses the management of both information security incidents and information security vulnerabilities. An event is an apparent alteration to the normal behaviour of one of an organisational system’s components (i.e., workflow, data, and person). An incident is a given event associated with a human entity and is administered by an incident response coordinator and managed by an information security incident response team (ISIRT) (ISO/IEC, 2016). The aim of ISIM practices is to mitigate and respond to the incidents while minimising the harm caused by the damage (Tøndel et al., 2014). Dodson (2001) explained that the ISIRT contributes to the protection of organisational resources through appropriate support such as identification, risk analysis, evidence collection and follow-up to reduce escalation. While frameworks for ISIM are useful, research is limited regarding effective awareness delivery methods, which can theoretically influence the employer's behaviour which in turn improves the management of incidents (Wang et al., 2022).

Evidently internal stakeholders (i.e. employees) are a key threat to information systems security management when they do not comply with existing organisational information security policies and guidelines (Son, 2011). As information resources may be secured by various approaches through non-technical or technical means, hitherto the preponderance of efforts supports the technical perspective (Ifinedo, 2012; Son, 2011). However, protecting information assets from the non-technical and human-centric dimensions is gaining momentum as the exploitation of employees (i.e. internal stakeholders) is viewed as one of the key vectors in organisational information security challenges (Khando et al., 2021). Thus, insiders who are not enculturated to safeguard the availability, confidentiality, and integrity of an organisation's IT assets, may expose their organisations to external threats.

External threats emanate from individuals or organisations that are peripheral to an organisation and they do not have legitimate access to the organisation's IT infrastructure (Jouini et al., 2014). Internal employees (i.e. insiders) can be considered as a threat to the organisation as they have legitimate access to organisational infrastructures and systems (Padayachee, 2021). An insider threat is defined as any individual who has legitimate access to an organisation's IT assets but acts maliciously for personal gains (Van Niekerk, 2017). Non-compliance with information security policies from an insider is termed as an "insider threat" (Balozian & Leidner, 2017). Insiders have the potential to damage the information assets of the organisation (Son, 2011) either intentionally (e.g. data destruction, theft) or unintentionally (e.g. negligence to change passwords or log off, failure to update systems).

As internal threats, which include all stakeholders that have access to an organisation's assets, have been advanced as a significant threat to an organisation's information infrastructure (Ahmad, Hadgkiss, & Ruighaver, 2012; Son, 2011), it is clear that information security concerns must be addressed by a consideration of both non-technical and technical means (Stanton, Stam, Mastrangelo, & Jolton, 2005; Vroom & Von Solms, 2004). However, given the human-centric nature of an insider threat, the non-technical dimension of information security should be considered as a critical means to safeguarding organisational information resources (Leach, 2003; Son, 2011). Ensuring an insider submission to security procedures and policies via non-technical means involves promoting ethical use, policy, awareness, legislation, compliance, corporate governance and auditing (Vroom & Von Solms, 2004).

Clearly considering the human-centric activities of communication, collaboration and promoting awareness may be a means of improving the disjointed processes of ISIM (i.e., planning and preparation, detection and report, assessment, response, and lesson learning). The awareness and communication efforts made by organisations for enhancing ISIM processes are identified as a critical means to ensure routine business operations (Ahmad et al., 2021; O'Brien et al., 2020), which specifically supports the response phase of ISIM (Tøndel et al., 2014). Padayachee and Worku (2017) emphasised the significance of collaboration among users for incident response to enhance ISIM processes. Organisations need to shift towards the collaborative impact of response teams in incident analysis and standardised threat exchange format through transparent reporting (Riebe et al., 2021). The potential impact of information security incidents could affect the revelation, alteration, and destruction of organisational informational assets, and it will be difficult to investigate the incident and control it if the incident is not reported initially and recognised by the organisation (Miloslavskaya & Tolstoy, 2020).

According to Vroom (2002), it is critical to view information security from diverse perspectives (i.e., human, technical and physical) in that all employees are required to be trained in terms of the implementation of information security standards in their organisation. To demonstrate the human integration, the collaborative organisational model depicted by Werlinger et al. (2010) coordinates various users of an organisation (i.e., executives, management, end-users and experts) in the process of incident management. However, despite the coordination of stakeholders, the model specifically engages expert users in communicating analysed incidents. End-users are only involved in the process of notification. In this study, the communication and awareness efforts will be extended to all categories of users. Figure 2-1 depicts the model of collaboration among stakeholders for incident response adapted from Werlinger et al. (2010).

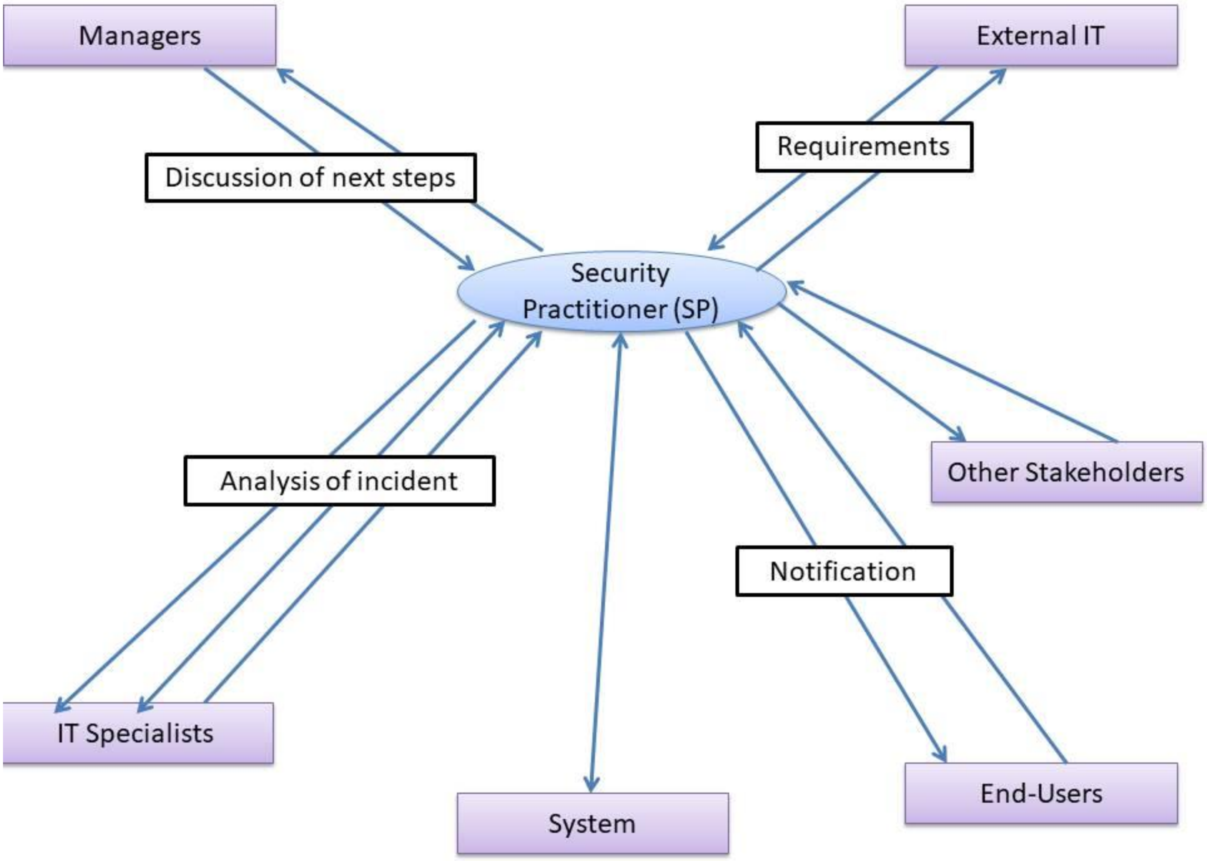


Figure 2-1: Collaboration among Stakeholders for Incident Response (adapted from Werlinger et al. (2010))

Clearly organisations cannot combat organised, sophisticated and persistent information security threats by focusing only on technical controls; rather they need to consider coordinating and mobilising their employees (Ahmad et al., 2021). ISIM is not only a technical, human or behavioural concern but also an organisational, management and communication concern (Kraemer et al., 2009). Therefore, the application of effective communication protocols among stakeholders of the organisation (i.e., executives, experts, end-users) is crucial to safeguarding informational assets (Knight & Nurse, 2020). Policies could be established to promote the communication of information security incidents, thus expediting the corrective actions that need to be undertaken (Cheung, 2014). This underscores the importance of communication and awareness formation within ISIM processes owing to the human dimension, which warrants further study.

2.3. Related Work

The practice of ISIM is largely uncoordinated, and organisations need to consider cultivating the awareness of users to combat persistent information security threats (Line et al., 2016). Most of the literature reviewed from the awareness perspective focuses on the technological outlook with a comparatively lesser emphasis on the humanistic standpoint (Ahmad et al., 2021). Although several mechanisms were suggested to improve the processes of ISIM, the essence of cohesion of socio-technical characteristics has not been given due consideration in recent studies (Sarker et al., 2019). Moreover, Hove et al. (2014) found that the tacit knowledge of users was disregarded and that employees have difficulties in reporting incidents, which requires users to comprehend and communicate the right incident information to the right people without compromising the confidentiality of the information. Thus, while users are an important source of incident information, the disjointed practices of ISIM processes (i.e., planning, detection, assessment, response, and lesson learning) have impeded the collation and distribution of incident information.

Various models and tools were proposed to address the problem of awareness and collaboration regarding ISIM. For instance, Metzger et al. (2011) introduced a comprehensive process-based approach to ISIM which enables the ISIRT to associate existing incidents across various means to support the classification of incidents and to assume appropriate actions either in a manual or an automated manner. Similarly, the model suggested by Jeong et al. (2008) involves investigating real-time incidents and reporting to only authorised personnel. Imamverdiyev (2013) considered fuzzy analytics as a means to address the challenges of prioritising the large volumes of incidents which could serve as a technical solution for ISIM. Baskerville et al. (2014) suggested an approach that keeps the balance between prevention (i.e., planned threat management) and incident response (i.e., unexpected threat management) through the application of three elements (i.e., planning, situational analysis, and operation) in both the response and prevention paradigm with a careful balance between the two (i.e., prevention and response). The advantage of the model is that it attempts to prioritise the management of incidents via the incorporation of the “lessons learnt” phase as a core element between prevention and response. The model developed by Padayachee and Worku (2017) was based on the notion that the processes of ISIM iterate from individual situational awareness (i.e. “knowing what is going on around you”) to a shared situational awareness thereby enhancing the responsiveness and collaboration of stakeholders when an incident occurs.

Husák et al. (2022) developed a new tool set (named CRUSOE) for enabling situational awareness in order to address the lack of procedures that manage situational awareness and decision-making in incident handling. The authors claim that the processes of situational awareness are not adequately managed. The aforementioned authors designed a visually enabled web-based system from the OODA (observe, orient, decide and act) to support decision making within the incident response phases, however the system focuses primarily on awareness for decision-making without a consideration of reporting and communication of incidents. Similarly, the model developed by Ahmad et al. (2021) also demonstrates the application of situational awareness from a management perspective by designing a process model within the incident response process. However, there was no real participation by end-users because initial requirements elicitation excluded them. Thangavelu et al. (2021) also proposed an empirically validated model for information security professionals to demonstrate the link between metacognitive awareness and self-efficacy, but with limited emphasis on communication and instigating the participation of end-users. Likewise Thangavelu and Krishnaswamy (2020) developed a conceptual model for incident management by using the National Institute of Standards and Technology Special Publication (NIST-SP-800-16) to depict the effects of Comprehensive Information Security Awareness (CISA) on threat management from a system and situational awareness perspective without due consideration to the communication perspective, which the current study attempts to incorporate.

Existing models to support ISIM are limited in some respects. For instance, although the model proposed by Metzger et al. (2011) was successfully implemented, the reporting process is limited to specific users such as Computer Security Incident Response Teams (CSIRT) and network administrators. Additionally, some security incidents are not reported at all, which limits situational awareness and hinders users from reporting incidents comprehensively. The model proposed by Imamverdiyev (2013) does not consider the socio-technical perspective and focused only on the prioritisation of incidents with a limited focus on post-incident prioritisation. Moreover, the model proposed by Baskerville et al. (2014) does not address the elements of communication and awareness efforts required in the practice of ISIM. The model proffered by Padayachee and Worku (2020) did not incorporate communication protocols as a fundamental element within the processes of ISIM. The model by Husák et al. (2022) does not instigate the participation by end-users because initial requirements elicitation excluded them.

Organisational studies show that incident reporting, collaboration, incident detection, post-incident experience sharing, and rehearsals were not given the required attention (Tøndel et al., 2014; Yohannes et al., 2019). According to Ahmad et al. (2015), who conducted a study on the financial sector (Australia), the lack of formal structures has negatively impacted the "lessons learnt" component of ISIM. This implied that the lessons learnt from previous incidents in an organisation could not be effectively used to resolve future incidents. According to Bartnes et al. (2016), who conducted a study on an electric power organisation (Norway) to assess the practice of ISIM, the coordination of the processes was limited. Similarly Line (2013) found that in power industries, ISIM processes were relatively unsystematic and that the coordination among organisational users was poorly managed. Correspondingly, Yohannes et al. (2019) who conducted a study involving Ethiopian banks, found that although the banks were compliant with the Information Technology Infrastructure Library (ITIL) and the International Organisation for Standardisation (ISO) standards, there were no formal means of ISIM practices in these entities. Jaatun et al. (2009) who conducted a study on the ISIM practices within the petroleum industry (Norway) by interviewing nine experts, found several issues of concern. Their study revealed the following issues: information security measures were mostly technical (not human-centric), mutual plans for responding to incidents were largely absent, scenario training opportunities were not considered, learning from previous incidents was unpublished, root causes of incidents were not identified, openness and awareness of incidents were marginal, and reporting systems were incompatible. Thus, incident reporting, collaboration, incident detection, post-incident experience sharing, and rehearsals were not given the required attention.

Various recommendations have been suggested to address the challenges concerning the management of ISIM. Metzger et al. (2011) recommends automatic, scheduled reporting functions and the opportunity to configure thresholds for mail monitoring and quarantining of compromised systems and sub networks in a formally specified incident response process. Padayachee and Worku (2017) recommended the involvement and active engagement of all users (end-users and management) within routine incident management processes. Husák et al. (2022) posited that the cyber security community should embrace the concepts of cyber-situational awareness and the tools that facilitate it. A comprehensive and unified approach for ISIM was recommended by Line et al. (2014). Correspondingly, Jaatun et al. (2009) rationalised that it is essential to inculcate a reporting culture in organisations for the unification of ISIM processes. Suggestions include enhancing the communication capacity of stakeholders through individual training and organisational learning in order to unify situational understanding. The recommended approach involves learning lessons from incidents (both reactive and proactive), as the organisation can learn from previous and real-time incidents by accentuating the importance of organisational learning (Jaatun et al., 2009). van Wyk, Van Biljon, and Schoeman (2020) also recommend that future research should examine how the evolutionary processes of reformulation, technology advancements and design improvements including considerations of how the solution (including the knowledge visualisation criteria and incident management system) can be generalised to solve similar problems in other contexts.

From an organisational perspective, ISIM can be supported by means of automated incident reporting. For instance the use of incident tracking systems could be advantageous (Metzger et al., 2011; Tøndel et al., 2014). It is advisable for organisations to maintain a structured approach in information security awareness programs in order to measure their effect and effectiveness towards empowering end-users to ensure safety and security online (Kruger & Kearney, 2006). The ISO/IEC 27035 standard promotes training, awareness and up-to-date incident information reporting and sharing; however, ISIM is marred by poor cooperation and insufficient incident communication efforts (Tøndel et al., 2014). Thus, organisations should leverage an integrated and standardised format for incident response (Schlette et al., 2021). In this regard, organisational stakeholders (external or internal) may be the weakest information link or potential threat to the organisation (Johnson, 2006). Therefore, it is imperative that the employees of an organisation are required to work in a collaborative, dynamic and coordinated manner in order to manage these challenges (Line et al., 2016). Consequently, since effective communication mechanisms are critical to obtain relevant situational awareness (Linderoth et al., 2015), this research study aims to explore how organisations manage and harmonise awareness and communication efforts in ISIM as a foundation for suggesting a conceptual model to respond to these core challenges.

2.4. Information Security Incident Management Standards Framework

Various ISIM approaches exist, and organisations can choose specific and appropriate information security management standards according to their internal systems. ISIM standards can assist in managing information security incidents in a systematic manner. According to Manley and McIntire (2020), the National Institute of Standards and Technology (NIST) and the Forum of Incident Response and Security Team (FIRST) framework address the role of communication both in normal business operations and in crisis times. The System Admin, Audit, Network and Security (SANS) also provides information security incident handling through various phases including training and certifications (Brown et al., 2019). Although various organisations adopt existing frameworks such as Computer Emergency Response Team (CERT) and (NIST), there exists a gap of empirical studies on how information security is addressed in an integrated approach from both a user and component aspect (Goodall et al., 2004; Werlinger et al., 2010). ISIM standards aim to collaborate and consider the management of incidents from an organisational perspective through appropriate planning, implementation and mobilisation of resources (Oriola et al., 2021). ISIM involves not only technical solutions but also solutions comprehensive to organisational context such as people and resources (Ahmad et al., 2012). ISIM specifies the essential components for the management of security information in collaboration with other parties such as business partners, customers, and suppliers. Although the standards differ and evolve, the applications of the standards are intended to enhance the proactive management of incident handling in organisations.

According to Cichonski et.al., (2012), ISIM consists of the following phases:

- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post-incident activity
- Coordination and information sharing

Table 2-1 shows the standards and the associated processes applied to ISIM. The NIST standard has four overarching processes such as preparation, detection and analysis, containment, eradication and recovery and post-incident activity. The ISO/IEC 27001 standard applies the PDCA approach to plan, do, check, and act in the management of information security incidents. The COBIT framework "requires a great deal of knowledge to understand its framework before it could be applied as a tool to support IT governance" (Zhang & Lefever, 2013, p.391). The ISO/IEC 27035 framework, one of the contemporary standards in ISIM, involves five processes to properly manage incidents in organisations. The ITIL standard focuses on standardisation and IT services.

Table 2-1: ISIM Standards, Aims, Processes and Characteristics.

Standards for ISIM	**Description**	**Processes for the Standard**	**References**
NIST	"The standard considers the process of containment, eradication and recovery"	-Preparation -Detection and Analysis -Containment, Eradication and Recovery -Post-incident activity	(Cichonski et al., 2012).
ISO/IEC 27001	-The standard enables organisations to manage security incidents - "The standard is generic and the assessment and handling of information security risks are tailored to the requirements of the organisation".	-Plan (Establish ISIM) -Do (Maintain -Check (Monitor and review) -Act (Implement & Operate)	(ISO/IEC, 2005)
ISO/IEC 27035	-The ISIM processes are defined based on structured approach from planning to implementation. -Each ISIM process is distinct - "The standard presents basic theories and stages of information security incident	-Planning and Preparation -Detection and Reporting -Assessment -Response -Lessons Learnt	(ISO/IEC, 2016)

Standards for ISIM	Description	Processes for the Standard	References
	management and incorporates these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt".		
COBIT	-Support separate IT governance from the management -Focus on regulatory compliance and risk management and management of IT assets	-Planning & Organisation -Delivering and Support -Acquiring & Implementation -Monitoring & Evaluating	(ISACA, 2012)
ITIL	"The framework outlines best practices for delivering IT services". ITIL is a systematic approach to manage risk, strengthen customer relations, establish cost-effective practice and build stable IT environment.	-Plan -Implement -Evaluate -Maintain	(Zhang & Lefever, 2013)

The NIST (National Institute of Standards and Technology) "comprises of the phases of preparation, detection and analysis, containment, eradication and recovery and post-incident activity" (Cichonski et al., 2012, p.21). The NIST guideline is comparable to the ISO/IEC standard and NIST Special Publication 800-61 "Computer Security Incident Handling Guide" (Scarfone et al., 2008).

ISO/IEC 27001

According to the ISO/IEC 27001 family of standards (ISO/IEC, 2005), ISIM is crucial for improved compliance, senior management involvement, improved effectiveness and staff responsibility in the proactive management of information security incidents in organisations. The ISO/IEC 27001 family of standards framework applies a Plan, Do, Check and Act (PDCA) model, taking into consideration the requirements of the organisation and the interested parties, through required processes and actions, to meet the requirements and expectations from the stakeholders (ISO/IEC, 2005; Proença & Borbinha, 2018).

ISO/IEC 27035

There is an information security incident standard (ISO/IEC, 2016) that is a well-recognised information security standard applied by organisations to manage, report and handle security incidents. The standards have the option to structurally manage incidents in terms of planning, preparation for incident report, actions to take when incidents arises and learning from previous incidents as part of lesson learning (Tøndel et al., 2014). This standard will be discussed in more detail in Section 2.5 as it underpins the conceptual model presented in the study at hand.

COBIT (Control Objectives for Information and Related Technologies)

The COBIT framework was created by the Information Systems Audit and Control Association (ISACA, 2012). The framework was developed as an assistive guideline for organisational managers which can potentially address critical issues such as business risks, technical issues and controlling requirements. It is a standard framework that can be adapted in any organisational context. Thus, COBIT can ensure that organisations retain their reliability, quality and control of information systems which is a critical business aspect of organisations (ISACA, 2012). The COBIT incident framework enables organisations to ensure effective incident management and governance through its processes.

The ITIL (Information Technology Infrastructure Library) aims to standardise the selection, planning and maintenance of IT services and focuses more on the technical standardisation and collaboration of stakeholders (Hunnebeck & ITIL, 2011). It is one of the applied standards in organisations to promote quality service management and computing services, and is utilised in the implementation of security incidents. ITIL is a standard guideline framework for providing Information Technology services which can support organisations in managing business risk, enhancing customer relations and developing an Information and Communication Technology (ICT) environment aimed at growth and transformation (Potgieter et al., 2005).

2.5. The ISO/IEC 27035 Standard

The ISO/IEC 27035 standard, one of the most recognised ISIM standards, frames the processes for the management of information security incidents threats and vulnerabilities (Tøndel et al., 2014). The ISO/IEC 27035 standard, which is a contemporary standard, is taken into consideration in this study as it deals with the management of incidents continuously from planning to lesson learning. The process of ISIM assumes a cyclic process: planning and preparation; detection and reporting; assessment and decision; response (prevent, reduce, recover); and lessons learnt (Figure 2-2). The steps require proactive planning, assigning the right people to manage the incident, proper identification, and reporting of the incident, assessing, and responding to the incident, and making decisions on the incident. It also requires users to contain and resolve the incident, learn from the existing incidents and prepare for future incidents for improved security (ISO/ IEC, 2016).

ISIM should be supported by skilled and trained employees who have the requisite awareness to achieve the objectives of the management of incidents (ISO/IEC, 2016). The ISO/IEC 27035 information security umbrella covers the framework for managing information security threats in that it provides the format, template and standard to report encountered information security incidents in a well-organised and collaborative manner (ISO/IEC, 2016).

According to the policy document (ISO/IEC, 2016), the participation and collaborative awareness and communication of incidents is critical for structured incident management. Users are less likely to participate in the management of information security unless they are aware of and know how their participation enhances the business operation of the organisation. Further, the efficacy of the structured incident management and operational efficiency of the organisation to manage incidents is dependent on the quality of the notifications, the obligation to notify, ease of use and the training of employees. The effective management of incidents is also related to the value of information that users have access to in order to motivate them to report incidents in a structured approach which may benefit organisations (Bulgurcu et al., 2010). Thus, the ISO/IEC 27035 standard enables users to collaborate in such a manner in order to further improve the management of incidents. In line with ISIM processes, the ISO/IEC 27035 standard consists of five processes - plan and prepare, detection and reporting, assessment and decision, responses and lessons learned. These steps which were used to frame the theoretical and practical vectors of the research problem are discussed next.

2.6. Information Security Incident Management (ISIM) Processes

According to Kossakowski et al. (1999) and Ahmad et al. (2012), the processes of ISIM include broadly preparing, handling and following up information security incidents. Preparation involves the priming of policies and procedures for responding to intrusions. The handling process involves the collection, analysis, communication, and awareness of information security incidents and its progress among all stakeholders. Further handling involves the application of short-term solutions, eliminating intruder access and returning the system to normal operation. Then the follow-up process deals with the identification and implementation of lessons learnt from the experience. The aim of these processes is to restore the system back to its standard operative state (Dodson, 2001). ISIM addresses various processes, planning and communication of incidents among employees of organisations (ISO, 2016). To achieve that, it requires awareness, training and equipping all stakeholders including end-users (Ahmad et al., 2021). ISIM involves the resource coordination for the management of incidents, as well as formulating and reporting the formal detection and response processes (Khando et al., 2021). As depicted in Figure 2-2, ISIM event flow diagrams consist of the processes of plan and prepare, detection and reporting, assessment and decision, response and lessons learnt. These are discussed in detail from Section 2.6.1 to Section 2.6.5 in relation to this study.

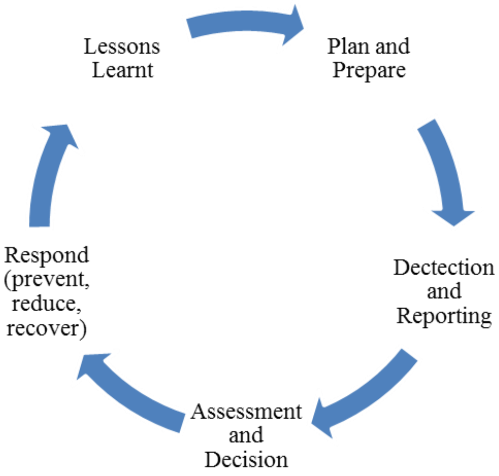


Figure 2-2: An Information Security Incident Management (ISIM) Event Flow Diagram (adapted from (ISO/IEC 27035, 2016))

Although the practice differs within organisations, the following are recommended processes in the information security incident management practices (Hove et al., 2014):

- Planning and Preparation
- Detection and Reporting
- Assessment and Decision
- Response to Incidents
- Lessons Learnt

The details of the processes of ISIM are discussed in the next sections (Section 2.6.1 to Section 2.6.5).

2.6.1. Planning and Preparation

This step deals with the preparation of ISIM policy and procedure and creates a proficient team to deal with incidents. The process of planning and preparation for ISIM is often inadequate, however, ISIM requires proactive and effective forward planning (Line et al., 2016). In order for organisations to succeed in the management of incident events and vulnerabilities for operational use, an organisation must complete several fundamental activities after the necessary planning. Planning and preparation involve allocation of resources, recruitment of a skilled workforce and establishing a formal reporting scheme for incident detection and response process. According to ISO/IEC (2016), some of the especially important operations that organisations should consider in the planning and preparation phase include:

- Commitment of senior management.
- Updating the ISIM policies at corporate and system, service, and network level.
- Establishing an ISIRT team for technical support.
- Briefings, training, and awareness creation sessions.

While it is vital to plan and prepare for incidents, the current strategies for this phase are poorly managed (Line et al., 2016).

2.6.2. Detection and Reporting

Information security incident detection and reporting anomalies exist in organisations in that users sometimes depend on their own tacit knowledge (Werlinger et al., 2010). The detection and reporting of incidents by users in organisations is also limited and is usually conducted by technical means and consequently end-users do not typically detect and report incidents (Ahmad et al., 2012; Metzger et al., 2011). Information security vulnerabilities can be detected by individuals directly or indirectly that trigger an alarming concern which could be either at physical, technical, or procedural levels. Detection could be, for example, directly from computerised systems, notification of system change, or other reports that appear from individuals or groups (ISO/IEC, 2016). Incidents can be detected either by automated machines or by human experts. Automatic means of information security incident event detection include: audit trail analysis, firewall, intrusion detection systems, and anti-malicious code tools (Hove et al., 2014).

Although the balance between openness and protection of incidents should be maintained, it is important to communicate the incident event to various media outlets for recognition (Manley & McIntire, 2020). According to ISO/IEC (2016), potential information security incident event identification sources include the following: system users, executives, security managers, line managers, suppliers and customers, ICT Department, ICT help desk, service providers such as Internet Service Providers (ISPs), telecom operators, ISIRTs, media such as mass media (newspaper, television, etc.), and websites and social media channels.

The individual who is notified of the source of the incident through either manual or automated means is responsible for initiating the process of detection and reporting of incidents. The individual may be any member or stakeholder of the organisation who could be in either a contract or a permanent position (Varga et al., 2021). During the reporting process, the individual must follow the established organisational reporting policies, use the standard reporting forms and report in the incident event to get the attention of the respective officers such as the ISIRT, management or executives. Accordingly, it is important for all employees to be aware of the existence of such established manuals and guidelines to report the information security incident vulnerabilities (Tøndel et al., 2014). The awareness includes the detailed format of the incident reporting schemes, the person who is reporting it and other associated elements of the incident. In some instances, conventional reporting mechanisms such as fixed telephone, mobile telephone and cordless phone may not be safe. Further safeguarding should be applied when communicating confidential or secret incident information. While the detection and reporting of information security incidents will be more wide-ranging if all users are involved, it is also important to maintain confidentiality by adhering to access control privileges.

2.6.3. Assessment and Decision

The third phase of ISIM is the assessment and decision phase that deals with occurrences of incident events and their assessment and the decisions taken (ISO/IEC, 2016). The process deals with how incidents are encountered, analysed, business restoration, collection of forensic evidence if necessary and decision-making (ISO/IEC, 2005). Each information security incident is assessed to determine its severity and its impact so that it enables decision makers to determine incident classification, to distribute responsibility and take appropriate follow-up action (Line et al., 2014). Shortcomings in the practice of incident responses contribute to limited strategic concern for security protection in organisations (Ahmad et al., 2012). The assessment and decision of information security incidents is not a trivial process and requires the expertise of the ISIRT (Tøndel et al., 2014).

2.6.4. Response to Incidents

The fourth crucial phase of ISIM is to respond to incident vulnerabilities according to the decisions taken in the previous phase (Ani & Agbanusi, 2014; ISO/IEC, 2016). The decisions undertaken could involve conducting full scale forensic investigations, collecting further incident information, responding to information security vulnerabilities and communicating incidents (ISO/IEC, 2005). Furthermore, decisions for incidents could be right or wrong in which wrong decisions could exacerbate the occurrence of incidents (Line et al., 2016). Since the process of information security incident response is at an emerging stage, Humphreys (2008) also supports the proposal that organisations are required to introduce an integrated and coordinated approach for the management of incidents to enhance compliance towards better management of encountered incidents. This phase involves containing, investigating, and resolving incidents. Information security incident response remains challenging for organisations. The lack of established checklists and proactive response reporting to users requires further empirical studies (Tøndel et al., 2014). Depending on the decisions, the response could be done in real time, or it could be delayed, or it could involve further forensic analysis. The response phase outlines the actions to be taken to restore or prevent further consequences of escalation (Line, 2015).

2.6.5. Lessons Learnt

The fifth phase of ISIM is to learn from previous incidents – the analysis, response and the decisions undertaken (ISO/IEC, 2005). The “Lessons Learnt” phase involves making real changes to improve the process instead of focussing solely on the positive achievements (ISO/IEC, 2005). Some of the processes that organisations should consider in this phase include – undertaking further forensic analysis, documentation of “lessons learnt”, and improving ISIM processes, risk assessment and policy schemes (ISO/IEC, 2016; Tøndel et al., 2014). Although there is limited research on the link between ISIRT and organisational environments, lesson learning is an important phase of ISIM (Ahmad et al., 2012). Olav Sveen et al. (2007) indicated that the most prioritised incidents are reported to learn and build knowledge to minimise future incidents. In addition, it is a requirement for organisations to report information security incidents according to their severity to concerned users and stakeholders. For instance, it is mandatory to report high-level security incidents to multiple concerned stakeholders outside of the organisations such as ISPs and media to obtain appropriate support (ISO/IEC, 2016). The lack of willingness to share incident information with external parties could be a major impediment to learning lessons from prior incidents (Hove & Tarnes, 2013; Jaatun et al., 2009). Thus, the lack of documentation and unreported incidents has negatively impacted the shared awareness among users and the "lesson learning" phase from previous incidents.

2.7. Information Security Incident Management Challenges

The disjointed management of information security incidents contributes to the lack of awareness among users (Thangavelu et al., 2021). The lack of documentation, lack of training, lack of post-incident evaluation and lack of communication between management and end-users are some of the challenges encountered by organisations within ISIM processes (Line et al., 2016). Other challenges include limited managerial commitment to ISIM processes, lack of awareness of technical usability tools and uncoordinated reporting of incidents (Line & Albrechtsen, 2016). The lack of communication strategies (internal communication and external communication) in ISIM has a significant impact on achieving compliance (Tøndel et al., 2014). Extant studies also indicate that there is poor participation of end-users in information security practices, fragmented approaches to information security management and lack of formalised communication means to report incidents in organisations (Kossakowski et al., 1999; Line & Albrechtsen, 2016; Rasmussen, 1997). The lower the quality of the participation and communication among stakeholders, the lower the capacity of the awareness and the shared understanding of incident knowledge in organisations.

The active participation of all users (end-users, executives and experts) in information security policies and procedures creates a sense of ownership and enhances compliance (Khando et al., 2021). ISIM requires the full participation of all users (Werlinger et al., 2010), however, the lack of participation of end-users in the process is a known challenge (Ahmad et al., 2012; Line & Albrechtsen, 2016). Thus, the problem can only be addressed through the active participation of all users (including end-users) in the process of ISIM policies and procedures of organisations (van der Kleij et al., 2022). Accordingly, all employees of an organisation must be trained, skilled and have awareness about information security reporting mechanisms, weaknesses and threats which includes mechanisms on how to report incidents, detect anomalies and escalate reporting appropriately (ISO/IEC, 2016). The information related to a security incident occurrence should identify both whom and when to communicate (ISO/IEC, 2016).

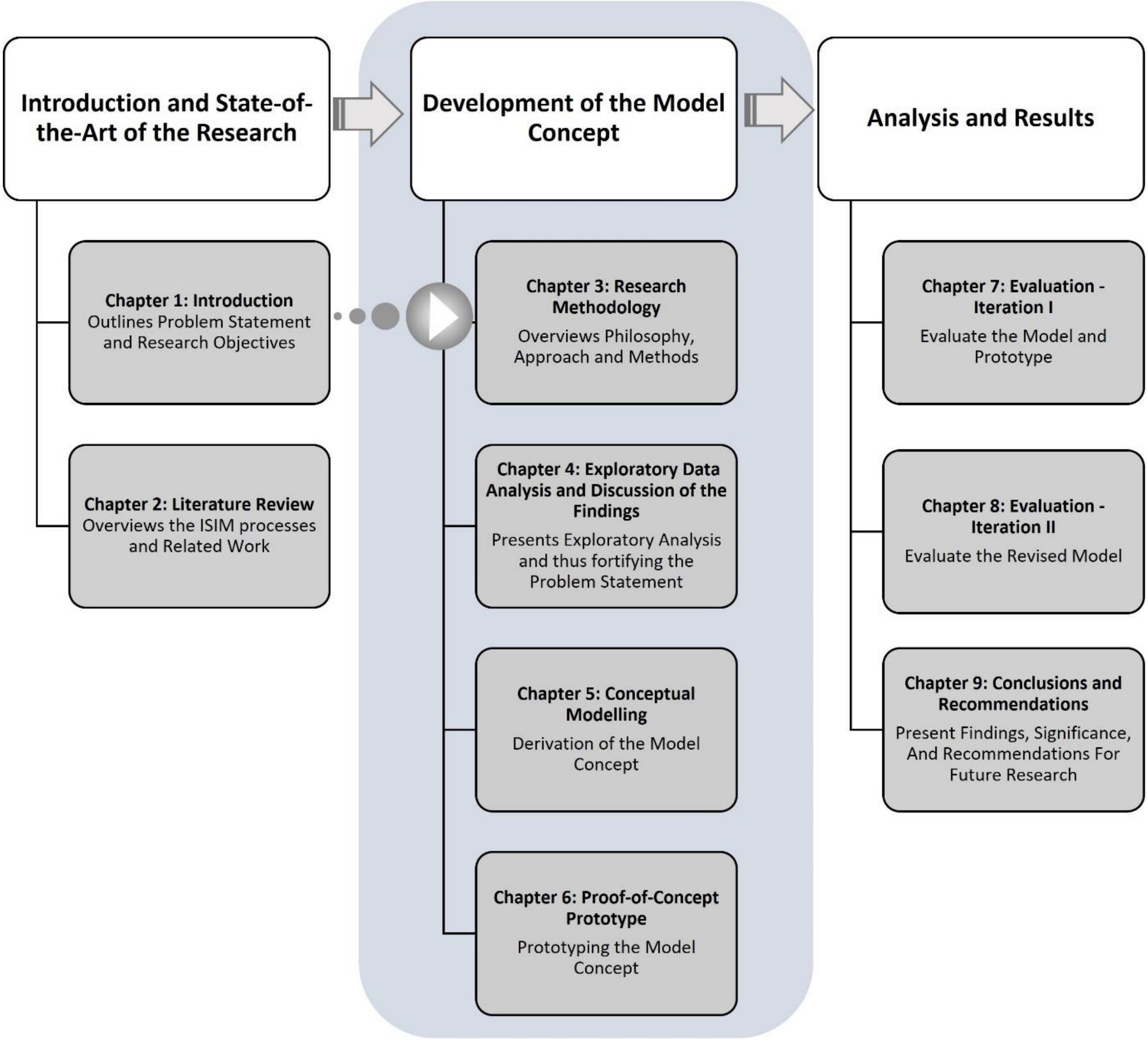
Despite the significance of information security awareness in the management of incidents (Ahmad et al., 2021; Vroom & Von Solms, 2004), a comprehensive and coordinated mechanism to streamline the incident cases to all users remains a challenge, which prompted calls for further research into exploring why ISIM is problematic (Tøndel et al., 2014). As communication is an essential element of every step in an information security incident response scenario, the lack of formalised reporting systems hinders the awareness process among users (Hove & Tarnes, 2013). The limited formalised and standardised reporting mechanisms such as digital and manual means would enable users to have a shared understanding of the contextual information in their organisations to control the communication pathway that all relevant information is communicated by appropriate senders and receivers to achieve authenticity (Ahlan et al., 2015; Miloslavskaya & Tolstoy, 2020).

2.8. Chapter Summary

This chapter explored the challenges associated with managing information security incidents in organisations. The uncoordinated and disjointed management of information security incidents as reported in the literature has possibly created inconsistencies and contributed to the increasing number of incidents in organisations. The lack of communication and awareness regarding information security incidents among stakeholders within organisations is a major concern. Furthermore, the participation of end-users within an information security incident scenario is limited. This chapter explored the various processes of ISIM, and the related challenges. These challenges contribute to the processes being disjointed and thus encumbering a collaborative and participatory approach to ISIM. Chapter 3 will propose a research approach to address some of the problems raised in this chapter.

CHAPTER THREE

RESEARCH ROADMAP


Introduction and State-of-the-Art of the Research
Development of the Model Concept
Analysis and Results
Chapter 1: Introduction
Outlines Problem Statement and Research Objectives
Chapter 2: Literature Review
Overviews the ISIM processes and Related Work
Chapter 3: Research Methodology
Overviews Philosophy, Approach and Methods
Chapter 4: Exploratory Data Analysis and Discussion of the Findings
Presents Exploratory Analysis and thus fortifying the Problem Statement
Chapter 5: Conceptual Modelling
Derivation of the Model Concept
Chapter 6: Proof-of-Concept Prototype
Prototyping the Model Concept
Chapter 7: Evaluation - Iteration I
Evaluate the Model and Prototype
Chapter 8: Evaluation - Iteration II
Evaluate the Revised Model
Chapter 9: Conclusions and Recommendations
Present Findings, Significance, And Recommendations For Future Research

CHAPTER 3: RESEARCH METHODOLOGY

3.1. Introduction

This chapter presents the research approach applied in this study. The research involves two phases of study (Phase I and Phase II). Phase I focuses on an exploratory examination in order to answer the core research questions through various data acquisition methods. Phase II focuses on evaluation of the model and interface prototype. This chapter explicates the research philosophy (Section 3.2), the research approach (Section 3.3), the research method (Section 3.4), and the sampling design (Section 3.5). The data collection mechanisms (Section 3.6), the data analysis mechanisms (Section 3.7) and the validity and reliability measures (Section 3.8) that are employed in this study are additionally presented. The approach, methods, and strategies establish the groundwork for the next phase on how to organise, design and collect data relevant to the problem. All the processes of the research methodology are discussed in relation to the application of the model developed in this research, namely the conceptual model designated the **C**oordinated **C**ommunication and **A**wareness approach towards enhancing **I**nformation **S**ecurity **I**ncident **M**anagement (CCA^{ISIM}). The research methodology and instruments are also validated and discussed in this chapter.

3.2. The Research Philosophy

The research philosophy refers to “a system of beliefs and assumptions about the development of knowledge” (Saunders et al., 2009, p.124). Within an interpretive research philosophy, the Design Science Research (DSR) paradigm was applied to study the problem. The interpretive approach allows knowledge construction from the participants actively involved in the research process and an in-depth observation of the use of a certain system can be achieved within an organisational setting. Moreover, the interpretive approach enables an interactive link between the researcher and the participants in which hermeneutical and contextual factors can be explicitly described (Gregg et al., 2001). Although the DSR method is pragmatic in its essence, it serves as a critical approach for producing new and innovative solutions for certain research problems (Weber, 2010).

The philosophy behind applying the DSR methodology is that it is a qualitative research approach in which the object of study is the design process which produces knowledge about the method applied to design a certain model or artefact (Carstensen & Bernhard, 2019). Moreover, the DSR approach allows for a design-based problem solving approach to address a given research question (Hevner, March, Park & Ram, 2008). There is currently a shift to the "generic qualitative studies" which do not pledge to the typical existing approaches that direct interpretive categories of research (i.e. grounded theory, phenomenological, narrative, case study and ethnographic) (Caelli et al., 2003).

Oates (2006, p. 292) suggests that interpretive research focuses on "the social context of an information system; the social processes by which it is constructed and developed by people through which it influences, and is influenced by its social setting". In other words, interpretive research is useful in understanding the context of an information system, specifically where a system influences and is influenced by the context in which the system is operating. Thus, qualitative data collection methods are required to fully understand this type of contextual information. The interpretive research paradigm in this research study can best answer the core research question through studying participants in a contextual manner (Berntsen et al., 2004). Accordingly, a relativist ontological position is taken considering constructed realities while the epistemological viewpoint (i.e. the "association between the 'knower' (the research participant) and the 'would-be knower' (the researcher)") is in the interpretivism context which advocates for a subjectivist stand point (Ponterotto, 2005, p. 131). Thus, an interpretive perspective enables the understanding of the ISIM domain in order to inductively reveal a solution space to resolve the identified challenges.

A research approach involves either an inductive or deductive approach (Leedy, 2005; Hassan et al., 2018). Deductive reasoning emerges from general theory to hypothesis testing and confirmation while inductive reasoning emerges from a question to data collection, to generalisations and eventually theory to explain 'what is going on' (O'Leary, 2007). In this study inductive reasoning was mainly applied to unpack the problem statement and to derive a solution to address the core research questions which are explained in Section 3.4.

The DSR methodology was applied as the research strategy of choice. Phase I of the research strategy involved an exploratory study to further understand the problem statement. Reiter

(2013) argues that exploratory studies offer more than just new factual data, they can be used to explain reality. Reiter (2013) also argues that researchers could not be impartial like in the positivistic approach; however, rigour can be achieved through transparency and honesty about the framing of the subject which requires explaining the ontological and epistemological position of the researcher of the study. Thus, considering the research problem, an interpretive research philosophy was employed to study the selected organisations in order to understand the practice of Information Security Incident Management (ISIM) within a real-world context. The interpretive research philosophy was employed to enable the researcher to interpret the problem from the data collected in order to address the research questions.

The methodical choice was multi-method which offers a wider selection of methods which was required to address the research questions. Phase I leveraged a semi-structured interview for the exploratory phase of the study, including both open-ended and close-ended question options. Further document analysis of information security policies, incident management systems and procedures were employed to gather data in a triangulated manner. Phase II involved developing a conceptual model and prototyping (a proof-of-concept), which was then evaluated via a survey method.

Figure 3-1 demonstrates the logical research approach applied in this investigation that is adapted from Saunders et al. (2009). Note the time horizons, which are not depicted in the figure, are cross-sectional.

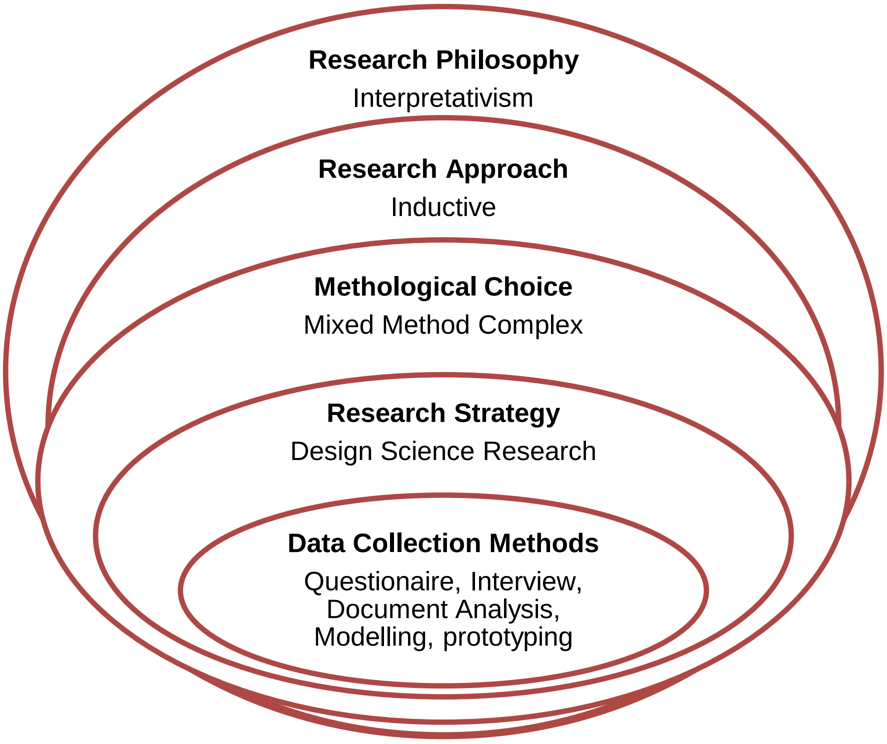


Figure 3-1: The Research Approach (adapted from Saunders et al. (2009))

3.3. Research Approach

In the framework of the interpretive philosophy and the DSR method, an inductive approach was applied to study the research problem. The study applied and benchmarked appropriate methodologies from established authors such as Oates (2006) and Saunders et al. (2009). In an inductive approach, the researcher starts by collecting data to explore a phenomenon and generate a conceptual framework (Saunders et al., 2019). Most of the research outputs or findings are derived from collected data. However, there are also inferences and relations to existing theories. As a result, although the study mainly utilised an inductive approach, some of the explanations of the data were made deductively through existing themes to then analyse data.

The DSR methodology was applied to this study as it involves building and evaluating artefacts to address the needs identified in industry and it assists in problem spaces that involves translating the reflections of people's ideas into developing feasible applications (Peffers et al., 2020). Scientific studies entail the evaluation of the models and artefacts based on the pre-specified research goals and appropriate methods applied for the research (Peffers et al., 2007). DSR involves the creation of an artefact, model and/or design theory as a mechanism to improve the current state of practice and the existing research knowledge (Kuechler & Vaishnavi, 2012). In DSR there exists various techniques proposed to validate a certain artefact, such as expert reviews, laboratory prototypes, simulation, and field experiments (Osterle et al., 2011).

The DSR methodology was applied in this study in order to understand and refine the problem, obtain data, develop the conceptual model and to evaluate the developed model. The research is delineated into two phases. The first phase (i.e., Phase I) deals with exploring awareness and communication efforts concerning ISIM within the studied organisations. Phase II deals with the subsequent phase of the study after the exploratory study which involves model evaluation, obtaining data from experts, improvement, and analysis. Each phase of the research methodology will be discussed in the following sections.

3.4. Research Method

The research study leverages the DSR approach to respond to the research questions. Phase I addresses **RQ1**, **RQ2**, and **RQ3** while Phase II specifically responds to research question **RQ4** (*How should organisations enhance the coordination of awareness and communication efforts within the processes of ISIM practices?).*

3.4.1. Phase I: Exploratory Study

The main objective of the research study is to explore how organisations strategise and harmonise the awareness and communication efforts in ISIM. An exploratory approach was employed to achieve the aim of the study which is an appropriate method to use when a problem context is not fully defined and requires further insight. An exploratory study is fundamentally evolving and does not necessarily suit a specific model (Munkvold & Bygstad, 2016). Thus, exploratory studies can serve as a means to investigate further methodologies to be employed in subsequent steps of a research project in order to obtain additional insight into the research context (Chawla & Sondhi, 2011). An exploratory research study is characterised by dynamism, pragmatism and continuous discovery which is difficult to associate distinctly to either quantitative or qualitative research designs (Jupp, 2006). Although the aim to identify trends recommends a quantitative alignment, the social engagements of the participants propose for a qualitative orientation (Ang, 2014).

From the inception, this study aimed to address the following research questions:

- **RQ1**: To what extent are strategies for awareness and communication efforts integrated into organisational ISIM practices?

- **RQ2**: How do organisations integrate communication and awareness efforts into their ISIM processes and practices?

- **RQ3**: To what extent is the integration of stakeholders' and end-users' participation instigated within the processes of incident awareness and communication efforts within ISIM practices?

- **RQ4**: How should organisations enhance the coordination of awareness and communication efforts within the processes of ISIM practices?

To address questions (RQ1 – RQ3) an exploratory study was conducted by combining qualitative and quantitative data collection methods. The qualitative responses were analysed according to themes and categories while descriptive statistics were used to analyse the quantitative data. The study identified two main problems in ISIM: poor coordination of awareness and communication efforts. These issues were also confirmed by the literature (Section 2.7). These key challenges negatively influence the reporting of information security incidents and hinder the synchronised and collaborative power of users acting in coordination within an ISIM framing. These challenges present a major threat to organisations as incident information will be limited resulting in an inadequate response. Research questions (RQ1 - RQ3) are addressed in Phase I as part of the identification of the problem and exploring empirical data from organisations. The link between the research questions, approach and the phases of research is demonstrated in Figure 3-2.

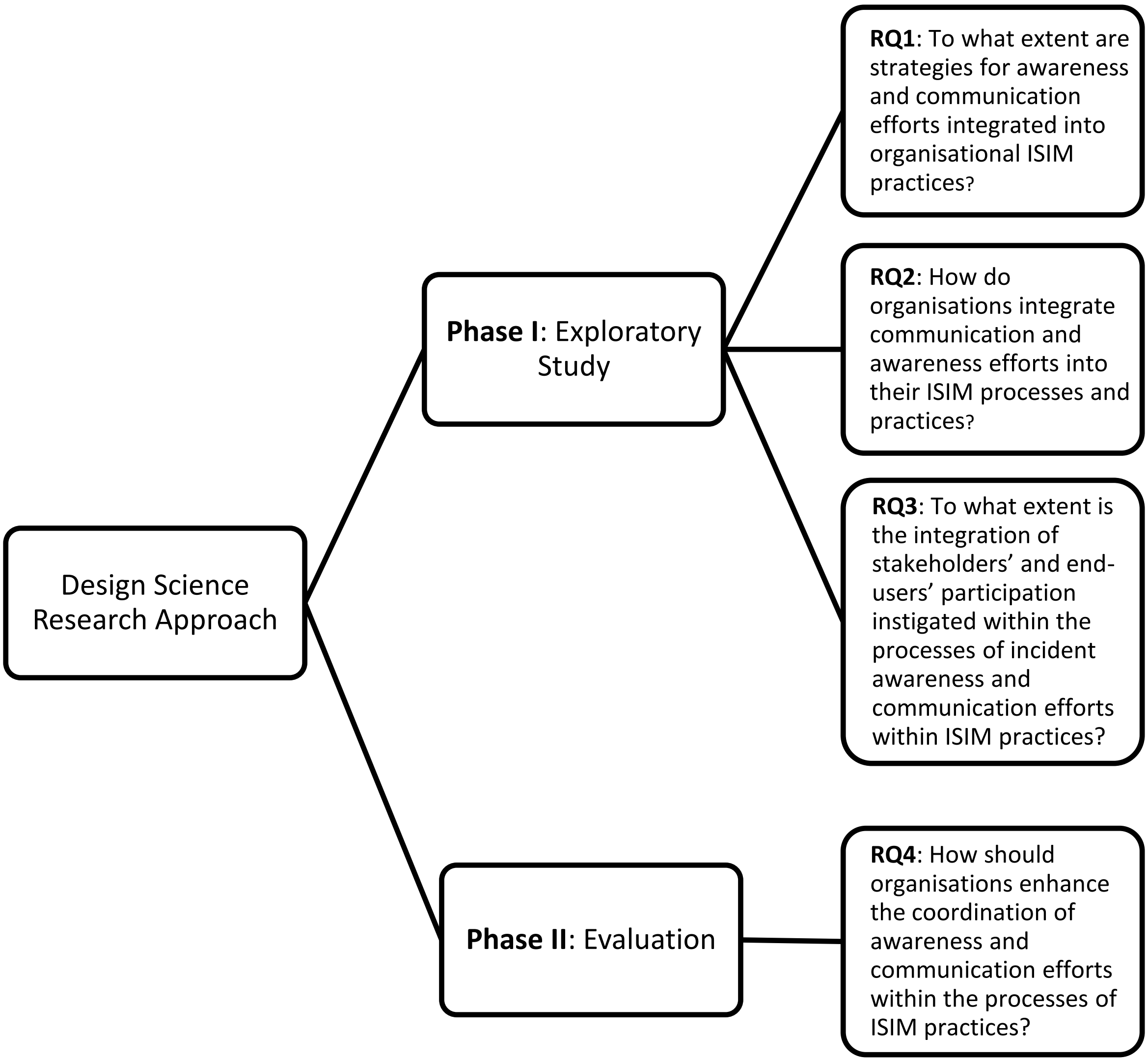

Design Science Research Approach
Phase I: Exploratory Study
Phase II: Evaluation
RQ1: To what extent are strategies for awareness and communication efforts integrated into organisational ISIM practices?
RQ2: How do organisations integrate communication and awareness efforts into their ISIM processes and practices?
RQ3: To what extent is the integration of stakeholders' and end-users' participation instigated within the processes of incident awareness and communication efforts within ISIM practices?
RQ4: How should organisations enhance the coordination of awareness and communication efforts within the processes of ISIM practices?

Figure 3-2: The Link between Research Questions and Research Phases

As shown in Figure 3-2, each research question was addressed using various methods of the research approach. **RQ1**, **RQ2** and **RQ3** were addressed by Phase I of the study (i.e., the exploratory survey). In addition, document analysis and interview techniques were employed. **RQ4** was addressed by Phase II of the research process or evaluation process. This phase involved gathering both quantitative and qualitative data using questionnaires. The application of the DSR methodology is discussed in Section 3.4.4.

3.4.2. Phase I: Semi-structured Interview

Phase I addressed **RQ1**, **RQ2** and **RQ3**. Specifically, a semi-structured interview was applied to gather both quantitative and qualitative data from experts and end-users. Data was collected via a semi-structured interview guideline from information security experts and end-users (Appendix A). The collected data was analysed using descriptive statistics, graphs, charts, and thematic analysis.

3.4.3. Phase I: Document Analysis

The data collected from the semi-structured interview was also supported with document analysis in order to triangulate the data collected. The documents included policy documents, information security procedures, Information Communication and Technology (ICT) policies and guidelines. The document analysis also included the proclamations related to information security and the ICT policy adopted in Ethiopia.

3.4.4. Phase II: Evaluation

The findings from the exploratory data (i.e., a component of Phase I) prompted the basis for the proposal of a conceptual model designated – **CCA$^{\mathbf{ISIM}}$** which was suitable to addressing the underlying research problem (Phase II). The **CCA$^{\mathbf{ISIM}}$** model unifies and subsumes theories of situational awareness and the Interactive Model of Communication (IMC) towards enhancing the coordination of awareness and communication efforts in ISIM. The models were applied to systematically explore the role of communication and awareness in a collaborative manner in order to proactively engage users for the practical management of incidents.

The model was framed based on the findings of the exploratory study and addressed the core research questions of the study. Phase II applied an expert review technique to evaluate the model and artefact (i.e., system prototype) developed as a demonstration of a solution to the problem identified in the preliminary exploratory study (Phase I). The experts involved in the expert review technique included Information Security Managers, Information Security Administrators, and Information Security Auditors.

The evaluation step is an especially important element of the DSR process as it provides critical feedback regarding the artefact or the model proposed (Peffers et al., 2012). The evaluation process, in Phase II, consisted of two iterations – Iteration I and Iteration II.

Data was collected via an online form from both information security experts and end-users for Phase II – Iteration I (Appendix B). Additionally, data was collected via an online form from information security experts only, for Phase II – Iteration II to evaluate the refinements of the model after Iteration I (Appendix C).

The exploratory study defined and established the problem domain. This was followed by designing and evaluating the model and prototype designed in response to the problem identified.

Figure 3-3 shows the DSR processes involved within the two phases of the study.

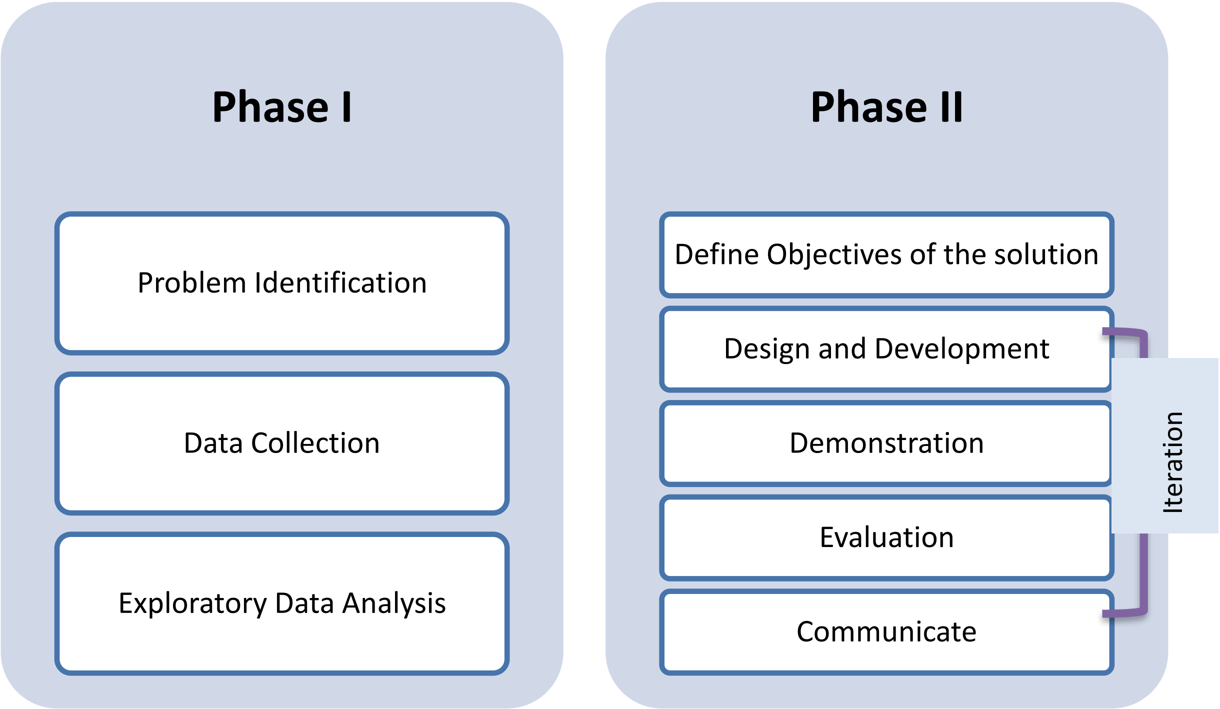


Figure 3-3: Design Science Process for Phases I and II (adapted from Peffers et al. (2020))

Phase II of the research methodology involves five processes (Peffers et al., 2007):

- Define the objectives of a solution
- Design and development
- Demonstration
- Evaluation
- Communicate

Define the Objectives of the Solution

The core objective is to develop an integrated conceptual model to improve stakeholder involvement in the awareness and communication efforts in ISIM processes. The proposed solution is intended to enhance awareness and communication tasks of ISIM to promote a shared mental model thereby resulting in proactive incident management. The poor coordination of users results in poor collaboration and poor reporting of incidents. As a result, the solution would involve creating a shared mental model which would promote proactive ISIM as all stakeholders will work in synchronicity.

Design and Development

The design and development of the conceptual model is the next step in the process. The definition of the problem statement frames the development. This step derives the CCA^{ISIM} conceptual model (see Chapter 5).

Demonstration

The prototype attempts to show how these components of communication and awareness efforts cooperate to demonstrate a coordinated awareness and communication model for ISIM. The core elements of the model (based on situational awareness and interactive models of communication) were mapped in the demonstration in a visualised manner. In addition to the presentation of the conceptual model, an interface prototype was demonstrated visually, and its prototype was provisioned online for evaluation purposes. The demonstration was undertaken in a simulated environment for the participants. Application test and model suitability was evaluated. The demonstration is available online for the participants to engage with the flows of the prototype (https://sites.google.com/view/ccamodel/home). The prototype design is an interface prototype and not a functional prototype. The interface prototype is discussed in Chapter 6 of the study.

Evaluation

This step involved an expert review technique including various stakeholders to evaluate the model and artefact (interface prototype) developed as a demonstration of a possible solution to the problem identified. The evaluation is undertaken in two iterations. Iteration I involved end-users and experts in the evaluation. The experts are qualified professionals in the organisation such as Information Security Managers, Information Security Administrators, IT Risk Analysis Officers, IT Response Team Members, and Information Security Auditors. Iteration II involved experts only as this phase focuses on the improvement of the conceptual model. The feedback provided by experts and end-users has prompted the improvement of the conceptual model in Iteration II.

Communication

The study findings will be published in the thesis and scholarly articles. The findings of the study will be forwarded to the participating organisations.

3.5. Sampling Design

Yohannes et al. (2019) conducted a case study on ISIM processes within a financial institution in Ethiopia in response to limited research within this context. Similarly, the issues of collaboration, communication and awareness were found to be concerning. They recommend that more studies ought to be conducted within various organisations in Ethiopia. Ethiopia was selected for this study as it typifies regions where the level of cyber security advancement is low and therefore a study in this context would be relevant to empirically study the problem (Adane, 2022; Manyazewal, Woldeamanuel, Blumberg, Fekadu, & Marconi, 2021).

The criterion for the selection of organisations to be considered in the study included: (i) a probable vulnerability to information security incidents (ii) engagement with large data sets (iii) a probable engagement in ISIM processes and (iv) proximity to the research context. This sampling methodology does introduce bias and decrease generalisability, however, the study included open-ended questions to assist in obtaining a nuanced picture of the subject domain.

The selection of organisations was from both government and private entities. The Information and Network Security Agency (INSA) is the sole security agency affiliated with the Ethiopian government and was also included in the study.

3.5.1. Sampling Design – Phase I

For the exploratory study (Phase I), a purposive sampling procedure was employed to select the participants from the targeted organisations. Six (6) organisations from Ethiopia were sampled. Large organisations were considered as they are more likely to have encountered information security incidents. Out of the identified organisations, 32 participants were included to be part of the study. A pilot test was employed for a group of information security experts (n=6) from each organisation to assess and validate the content validity of the interview guide. Only the most salient questions were piloted. Table 3-1 summarises the sampling design that was applied in Phase I.

Table 3-1: Sampling Design for the Exploratory Study (Phase I)

Participant	**No**	**Percentage**
Information Security Expert	7	22
Information Security Manager	6	19
Information Security Risk Analysis Officer	3	9
Information Security IT Auditing Officer	4	12
Operational Manager	5	16
End-User	7	22
Total	32	100%

3.5.2. Sampling Design – Phase II

For the evaluation of the model and prototype in Phase II, a purposive sampling strategy was applied to select organisations to be involved in the evaluation survey from various organisations (n=5) within Ethiopia. The set of participants involved in Phase II differed from the set of participants involved in Phase I. The study considered additional organisations within the information security domain in order to obtain a broader perspective. As the need for a new strategy for incident management would have more consideration in this developing context, the sample framing included five organisations (2 government, 2 private and 1 security agency (INSA)). The selected organisations within the government, private and security sectors tend to have large investments in data centres and information security, which makes them more vulnerable to security incidents. Moreover, these are organisations that may be in the process of introducing incident management standards.

The evaluation of the model and prototype involved both information security experts and end-users. The aim of the evaluation is to obtain critical feedback of the acceptability of the proposal to assure the fitness of purpose of the model concept and interface prototype. The evaluation process was planned to be undertaken in two iterations: Iteration I and Iteration II. For Iteration I, from the organisations identified, the planned target populations of this research were information security experts (n=10) (i.e. information security auditors, information security managers, information security administrators, information security incident handlers, etc.) and end-users (n=30). Nielsen (2010) suggested that five participants are sufficient for discovering 85% of evaluation of system usability problems. The optimal sample sizes of '10±2' can be used to a basic or general evaluation situation (Hwang & Salvendy, 2010). The limitation of 10 experts was deemed sufficient as this would lead to a more in-depth enquiry over the two iterations. Eisenhardt (1989) argued that for qualitative studies, theoretical saturation is reached when more cases add minimal value and specified that 4 – 10 cases may be sufficient as more cases may lead to additional complexity and copious data.

The sampling of participants per organisation for Iteration I is summarised in Table 3-2.

Table 3-2: Evaluation Sampling Plan Guideline for Iteration I (Phase II)

ORGANISATION	**Sector**	**Sample (Security Expert)**	**Sample (End-User)**	**Total**
Organisation A[2]	Government	2	6	8
Organisation B[2]	Private	2	6	8
Organisation C[2]	Corporate by Government	2	6	8
Organisation D[2]	Private	2	6	8
Organisation E[2]	Security Agency	2	6	8
	Total	**10**	**30**	**40**

This study involved an online survey, and there can be either probability or non-probability methods of accessing respondents (Couper, 2000). In Phase II, the sampling strategy uses a non-probability sampling technique to recruit the respondents from the organisations. Based on the number of respondents who are willing to participate, respondents may be selected randomly from the group depending on the size of the availability of experts or end-users. Respondents who are involved in roles such as IT Security Manager, IT Security Administrator, IT Security Consultant, IT security incident response team member, IT Security Incident Manager, IT Security Auditor, IT Risk Analysis Officer etc. are considered as experts.

Iteration II only involved information security experts (n=10) who provided feedback on the improvement of the model concept based on the feedback from Iteration I. These experts were selected from the same pool of experts that were involved in Iteration I. The aim of Iteration II is to request further feedback on the improved conceptual model.

3.6. Data Collection Methods

In line with the organisation of the study, the data collection involves two phases. Phase I is for the exploratory part of the study. Phase II is for conducting the evaluation of the model and prototype.

3.6.1. Data Collection Method – Phase I

For Phase I of the study, the data collection procedure employed a semi-structured interview method and a document review of information security policies. The data validity was kept reliable through the application of various means of data collection (i.e., a semi-structured interview and document analysis). Based on the collected data from the interview and document analysis, the problem statement was confirmed.

3.6.2. Data Collection Method – Phase II

The questionnaire was administered using Google forms and completed online for both iterations. Potential participants were approached via their organisations. Demonstration videos of the model and prototype using YouTube was provisioned to the participants to serve as an interaction between the researcher and the participant, which is available at https://sites.google.com/view/ccamodel/home. These videos ensured that the participants fully engaged with the model and prototype prior to responding to the questionnaire in Iteration I. Subsequently, the study incorporated the relevant suggestions proffered by the participants in Iteration I in order to refine the model (i.e., Iteration II). The same panel of information security experts were supplied with a summarised report regarding the outcome of Iteration I and a description of the refined model via email. Thereafter, the information security experts were invited to evaluate the refined model and they completed the questionnaire via an online link.

3.6.3. Instrumentation – Phase I

For Phase I of the study, a semi-structured interview guideline (see Appendix A) was employed to collect data. In exploratory studies, the application of a semi-structured interview guide helps to clarify data and find relevant thematic concepts (Bless et al., 2006). The semi-structured interview comprises both quantitative and qualitative questions that enable interpretative data reflection. Moreover, the study applied a confirmative descriptive interview (it allows respondents to provide confirmation of fit responses) since the semi-structured interview guide is based on various building blocks as a foundation (McIntosh & Morse, 2015) including the ISO/IEC 27035-1: (2016) standard.

The semi-structured interview guide is comprised of two parts. Part I was planned for the information security experts and end-users while Part II (which was self-developed) was planned for end-users only. Part I comprises of three sections. Section 1 was outlined to attain contextual information of the organisation. Section 2 and Section 3 were intended to explore the practice of communication and awareness efforts among information security experts and end-users. The idea for the frame of the questions was adapted from related literature. For instance, questions related to methods of communication for information security were adapted from Wooding et al. (2003). The framing regarding the protection of information security mechanisms (such as application, physical, technical and system) was adapted from Caballero (2013). In addition, the idea about information security governance framework such as corporate, IT and non-IT categories was adapted from Da Veiga and Eloff (2007).

Table 3-3 summarises the derivation of the interview guide for each question.

Table 3-3: Questionnaire Items for Phase I

Component	Question	Reference
Background	1.1-1.7	Da Veiga and Eloff (2007), Caballero (2013) and Wooding et al. (2003)
Responsibilities and Roles	2.1, 2.2, 2.3 and 2.4	Bernsmed and Tøndel (2013)
Standard Application	2.5, 2.6 and 2.7	Ab Rahman and Choo (2015) Tøndel et al. (2014)
Formalised Agreements	2.8. and 2.9	Johnson (2006)
Processes of ISIM	2.10	Ahmad, Hadgkiss, and Ruighaver (2012); Bernsmed and Tøndel (2013); Dodson (2001); Kossakowski et al. (1999) and Werlinger et al. (2010).
Level of Awareness	2.11	Bernsmed and Tøndel (2013).
Workflow	2.12 and 2.13	Belsis et al. (2005)
Efforts of Awareness	2.14	Johnson (2006)
Efforts of Communication	2.15, 2.17, 2.18	Baker (2002), Dodson (2001) and Wood (2014)
Experience with Communication	2.16	Werlinger et al. (2010)
Strategies in Involvement	2.19 and 2.21	Open-Ended Questions (Self-Developed)
Challenges	2.20	Open-Ended Question (Self-Developed)
Participation of End-users	3.1, 3.2, 3.3, 3.4 and 3.5	Johnson (2006)

3.6.4. Instrumentation – Phase II

The survey questionnaire is designed to collect discrete answers with close-ended survey questions supported by semi-structured qualitative questions. The survey-based instrument designed to evaluate the model concept and the prototype consists of three sections.

Section 1 of the questionnaire collects biographical data – gender, job category, age, years of experience, and the country of residence of the respondent.

Section 2 (which consists of 11 questions) was founded on the Technology Acceptance Model (TAM). Purao and Storey (2008) argued for using a modified version of TAM to evaluate design science outcomes especially in circumstances when the artefact is not immediately deployable as with the current artefact. They found that TAM is a useful alternative as it focuses on the “potential for adoption” (Purao & Storey, 2008). Thus, the constructs used for this study involved: “Intent to use”, “Perceived usefulness”, “Ease of use” and “Compatibility and Scalability”.

Table 3-4 shows the linkage between the research problem raised in Phase I: the constructs and specific questions derived about the constructs. Lack of awareness and coordination, poor reporting of incidents, lack of participation and collaboration, lack of awareness and coordination, lack of an organisational interactive reporting system, lack of a shared mental model, and lack of an adaptable, integrated, and harmonised incident reporting system were the general problem categories for the constructs.

Table 3-4: Questionnaire Items for Phase II

Problem Addressed	**Question**	**Construct**	**Adapted from**
Lack of awareness and coordination	**Question #1**: Assuming I had access to a system similar to the prototype, I **intend** to use it in an incident response scenario to assist in the coordination of communication and awareness efforts with respect to responding and resolving information security incidents.	Intent to Use	(Davis & Venkatesh, 2004)
	Question #2: Assuming I had access to a system similar to the prototype, I **intend** to use it to enhance my awareness about organisational information security incidents.	Intent to Use	(Davis & Venkatesh, 2004)
	Question #3: Given that I had access to the system, I predict that I would **use** the system of communication and awareness towards achieving collaborative and proactive information security incident reporting.	Intent to Use	(Davis & Venkatesh, 2004)
Poor reporting of incidents	**Question #4**: Using a system based on the model concept will increase my **effectiveness** in reporting an information security incident.	Perceived Usefulness	(Davis & Venkatesh, 2004)
Lack of participation or collaboration	**Question #5**: I would find a system based on the model concept **useful** towards achieving a shared, interactive and participatory platform for the coordination and management of information security incidents.	Perceived Usefulness	(Purao & Storey, 2008) and (Davis & Venkatesh, 2004)
Lack of awareness and coordination	**Question #6**: I would find a system based on the model concept valuable towards enhancing my **effectiveness** in an incident response scenario by maximising the coordination of communication and awareness efforts with respect to information security incidents.	Perceived Usefulness	(Purao & Storey, 2008) and (Davis & Venkatesh, 2004)

Problem Addressed	Question	Construct	Adapted from
Lack of interactive organisational reporting system	**Question #7**: I would find a system based on the model concept **easy to use** in an incident response scenario.	Ease of Use	(Purao & Storey, 2008), (Mujinga, Eloff, & Kroeze, 2018) and (Davis & Venkatesh, 2004)
Lack of interactive organisational reporting system	**Question #8**: Interacting with the system will not require **huge mental effort**.	Ease of Use	(Davis & Venkatesh, 2004)
Lack of a Shared Mental Model	**Question #9**: My interaction with a system based on the model concept will enable a shared mental model of an information security incident thereby **easing** the incident management process.	Ease of Use	(Davis & Venkatesh, 2004)
Lack of an adaptable, integrated & harmonised incident reporting system	**Question #10**: Using the system would be **compatible** with my own existing organisational system design.	Compatibility and Scalability	(Purao & Storey, 2008) and (Padayachee, 2015)
	Question #11: If the system is scalable, it will potentially be used by many users on a **wider scale** in an incident response scenario.	Compatibility and Scalability	Self-Developed based on (Albers & Lohmeyer, 2012) and (Padayachee, 2015)

In Section 2, the evaluation questions were scaled from 1 to 5 (strongly agree to strongly disagree).

Section 3 was founded on the principles of design-oriented information systems research (Osterle et al., 2011). Four constructs were used for this section: abstraction, originality, justification, and benefit. Open-ended questions based on these constructs were posed to the experts only, as this part of the questionnaire requires expert judgement. These questions also add to the rigour of the study (see Appendix B). These questions were posed to the experts in Iteration II as well. As the questions are open-ended, the responses may be revised after the model and prototype have been enhanced.

Section 2 of the questionnaire, which is based on the TAM, was a determinant of acceptance of the model concept. Davis (1989) proposed the TAM as a means of improving the understanding of user acceptance and to give designers a means of evaluating a new system.

The model considers two dimensions namely ‘perceived usefulness’ (i.e. the extent to which an application helps a user perform their job better) and ‘perceived ease of use’ (i.e. a system is easy to use) (Davis, 1989). The TAM has been extended in several ways, for instance Purao and Storey (2008) also used ‘compatibility’ to test if their reuse-based design approach increased the willingness of developers to adopt the approach. They included ‘compatibility’ as they felt that it was important to ensure their approach was compatible with current practice. This research also assumes that compatibility of the new model with existing ISIM practices is important to user acceptance of the model. As the model was also socio-technical and human-centric, that aside from system acceptance (i.e. accepted by all stakeholders), it is also important that it is correspondingly scalable (i.e. adaptable to a wider scope of problems) (Albers & Lohmeyer, 2012). Padayachee (2015), who also considered the DSR approach, purported that the following elements are valuable in determining the participant’s acceptability of the model concept – viability, utility (i.e. value), efficacy, usability and scalability (Nielsen, 2010). Thus, the TAM was also extended to include scalability (Padayachee, 2015). System acceptance evolves out of a wider scope, and it includes usability, broader social acceptability and practical acceptability which includes usefulness, cost and compatibility, and scalability.

Figure 3-4 depicts the adaption of the TAM framing, where the acceptance of the model concept is predicted by the intent to use the model concept which is in turn determined by the constructs of perceived usefulness, ease of use, scalability, and compatibility. This framing will evaluate if the model is indeed considered to be fit for purpose. The questions in the model acceptance section (Section 2) are more generic and are intended to be understood by all users.

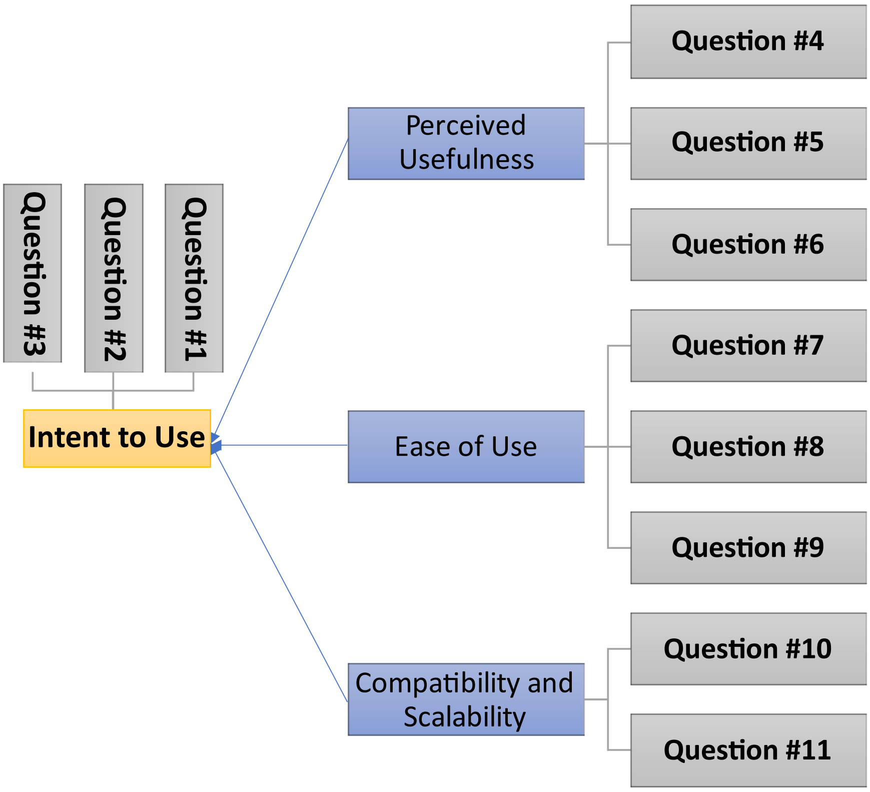


Figure 3-4: Research Framework (adapted from Purao & Storey (2008))

While the questions in Section 2 are generic, the questions in Section 3 are more suitable to experts. Section 3 was included to test the rigour of the model concept and prototype. Rigour in DSR is demonstrated by adhering to the following concepts: abstraction, originality, justification, and benefit as a means of distinction from typical development within a commercial organisation (Osterle et al., 2011). Each of these concepts were applied as follows as prescribed by Osterle et al. (2011).

- **Abstraction**: The artefact must be relevant to a set of problems. In this regard, the model and prototype attempt to resolve a subset of the socio-technical problems in the domain of ISIM, which were identified in Phase I, specifically the issues related to awareness and communication efforts.

- **Originality**: The artefact must contribute considerably to the evolution of the discipline or knowledge base. In this case the field in general is the Information Systems (IS) discipline and more specifically the Information Security discipline. The model and prototype are original and contribute to the body of knowledge in ISIM.

- J**ustification**: The artefact must be rationalised in a logical manner and should be validated. The rationale for the model was unpacked in Chapter 4 where the exploratory study showed that there is a need for such a model (i.e., Phase I). The validity and feasibility of the model concept was evaluated by domain experts and end-users.

- **Benefit**: The artefact should benefit its stakeholders. The design of the model concept is useful in demonstrating an approach to coordinating the management of information security incidents. However, it also provides a solution space to reason about including communication and awareness protocols within information security management.

3.7. Data Analysis Method

This section presents the data analysis procedures per phase. The tools used to collect data consisted of a semi-structured interview, a questionnaire (both structured and open-ended questions) and document reviews hence the data gathered were both qualitative and quantitative.

3.7.1. Data Analysis – Phase I

The quantitative data was clustered and analysed using descriptive statistics, graphs, and tabular data using Excel and SPSS (Statistical Package for the Social Sciences). The collected qualitative data was analysed via a case-by-case basis through frequent comparisons and inductive analysis which was based on themes and genres. More specifically, the qualitative data gathered from the interviews and document reviews which was analysed inductively using narrative and content analysis through themes was also triangulated to obtain a nuanced viewpoint of ISIM practices.

3.7.2. Data Analysis – Phase II

The analysis of the data for Phase II was conducted using various means. It includes descriptive statistics and inferential statistics for the quantitative data. The analysis for the qualitative data was achieved using thematic analysis. Atlas ti was used to analyse the qualitative data and SPSS was used to analyse the quantitative data.

3.8. Validity and Reliability

The validity and reliability of the study in both phases were achieved through various mechanisms. Although some qualitative researchers have argued that the term validity does not apply to qualitative research, the need for qualifying checks or measures has been recognised (Golfashani, 2003). Validity and reliability are conceptualised as rigour, trustworthiness, and quality in the qualitative paradigm (Bashir et al., 2008). Within the context of analysis, verification strategies that confirm both validity and reliability of data are activities such as confirming methodological consistency, and sampling validity and are supported with theoretical underpinnings (Morse, Barrett, Mayan, Olson, & Spiers, 2002).

For the qualitative data, validity can be achieved via four testing criteria – credibility, dependability, transferability, and confirmability. Lincoln and Guba (1986) provided the groundwork for these techniques as a substitute to achieving validity and reliability in qualitative studies. These techniques are comparative to the measures used by positivists. These criteria were used for Phase I of the study while the fifth criterion of ‘authenticity’ (Lincoln, 1995) was additionally applied in Phase II. Lincoln (1995) cautions that some criteria may be more applicable at some stages than at other stages of the research. It was assumed that validating the conceptual model in Phase II required an additional criterion to ensure that the model is considered useful.

3.8.1. Validity and Reliability – Phase I

The instrument was piloted among information security experts initially before the actual data collection was started. Only the most salient questions were tested. The pilot test involved six experts to verify the validity of the semi-structured interview guide. Table 3-5 describes how validity and reliability were achieved for Phase I of the study, where the criteria was applied by systematically considering the associated techniques. This framing was also used by previous studies (Persad & Padayachee, 2015).

Table 3-5: Validity and Reliability Criteria for Phase I (adapted from Bradley (1993))

Criteria	**Technique proposed to improve Validity and Reliability**	**Evidence of compliance**
Credibility ("Adequate representation of the constructions of the social world under study and can be assessed both in terms of the process used in eliciting those representations". (Bradley, 1993, p. 436).	-Protracted engagement -Peer debriefing -Member checking	-The engagement included semi-structured interviews. -Peer debriefing is attained through data submission, tools, and analysis to the secondary researcher for cross checking (in this case the supervisor of the study). -Member checking with the participants regarding their input.
Dependability "(i.e. consistency of the methods applied)" (Bradley, 1993).	-Maintaining an audit trail -Triangulation -Systematic association	-Dependability is attained by keeping a catalogue of data records, (paper and digital format). -The study depends on multiple sources of evidenced data to enhance validity (i.e., document analysis and interviews). -The dependability of the research instruments involved systematically associating the items on the questionnaire with commonly used standards and the literature for standardisation.
Transferability "(i.e. the level in which the 'working hypothesis' could be transferred to another context)" (Bradley, 1993, p. 436).	-Thick descriptions -Document analysis	-Transferability is attained via 'thick description' by acquiring richer inferences of the context through document analysis and background information on policies.
Confirmability "(i.e. the extent to which the characteristics of the data, as posited by the researcher, can be confirmed by others)" (Bradley, 1993, p. 437). It also implies achieving objectivity and impartiality.	-Data verification by a third party -Confirmation from participants	-Distribute interview transcripts to participants for confirmation. -The impartiality of the study was ensured through deployment of research assistants and data collectors to reduce bias.

3.8.2. Validity and Reliability – Phase II

The effectiveness of an artefact must be validated by the application of a standard heuristic evaluation process (Jaferian et al., 2014). These items on the evaluation survey were adapted from previously validated instruments. A similar survey instrument developed by Purao and Storey (2008) provided guidelines on evaluating the adoption potential of DSR efforts. This study used these guidelines and reviewed existing relevant literature to develop the items. The validity of the instrument was achieved by leveraging relevant existing knowledge and using the framing of the TAM which has been well validated by previous studies. The use of previously validated instruments provided a basis for face validity. To ensure content validity, a statistician and a language expert reviewed the instrument. The instrument was revised several times to ensure that the questions were clear and easy to understand. Cronbach's alpha α which is one of the most widely used measures of reliability in the social and organisational sciences was employed to measure internal consistency.

Table 3-6 describes how validity and reliability were ensured for Phase II of the study.

Table 3-6: Validity and Reliability Criteria for Phase II (adapted from Sikolia, Biros, Mason & Weiser (2013))

Criteria	Techniques proposed to improve Trustworthiness	Evidence of Compliance
Credibility - "how much the data collected correctly represents the multiple realities of the phenomenon." which relates to internal validity. (Sikolia et al., 2013, p. 2).	-Protracted engagement with participants -Data Triangulation -Thick descriptions -Participant guidance of the inquiry -Use of real participant words in the emerging theory -Peer debriefs -Negative Case analysis (extracted from (Sikolia et al., 2013)	-Two iterations of data gathering -Data triangulation using multi-methods -Provision of 'thick descriptions' in the analysis -Participants are directed with the outcomes of the study where the experts will assist in improving the artefacts. -Quotations from the participants is incorporated in the analysis -The statistician conducted peer analysis -Any descriptions that were inconsistent with the expectations of the researcher was considered
Transferability - "the application of one set of findings to another context which relates to external validity" (Sikolia et al., 2013, p. 2).	- 'Thick descriptions' of the research methods (extracted from (Sikolia et al., 2013)	Transferability is achieved by presenting clear accounts of the methodology to ensure repeatability. Provision of contextual information about how the data was collected, the organisational setting of the selected entities and the respondent's setting. The researcher provided existing situational analysis about the data collected such as organisational issues, information security culture of the organisation and the context of Ethiopia and the respondent's level.
Dependability - "the validation that the data represents the changing conditions of the	-Analysis of a detailed audit by an observer (extracted from (Sikolia et al., 2013)	An experienced statistician conducted an inquiry audit (external audit) on the integrity of the result outputs to maintain dependability.

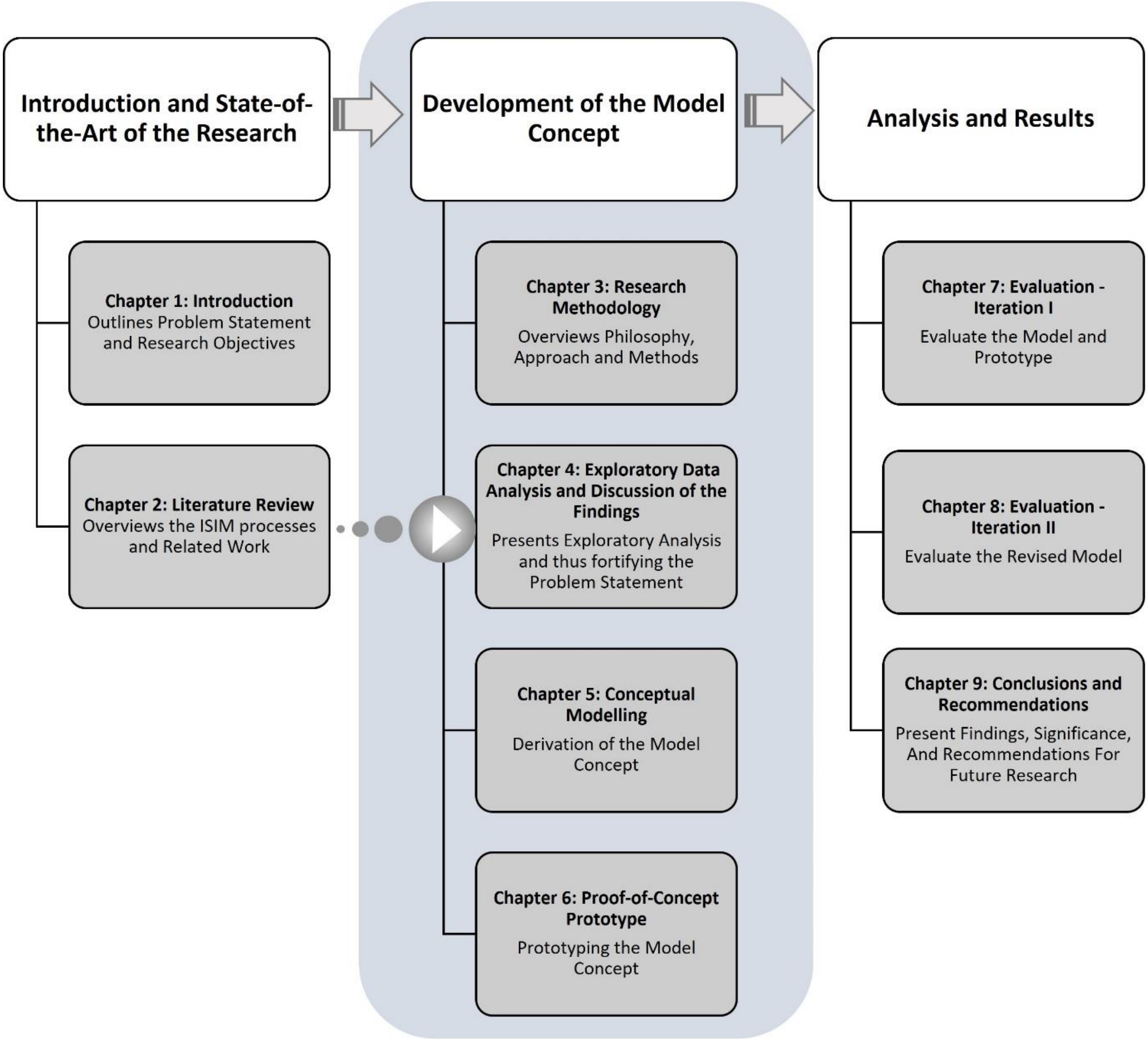
Criteria	Techniques proposed to improve Trustworthiness	Evidence of Compliance
phenomenon under study" (Sikolia et al., 2013, p. 3).		
Confirmability - "another researcher confirms the findings if presented with the same data" (Sikolia et al., 2013, p. 3).	-Investigation of a detailed audit by an observer (extracted from (Sikolia et al., 2013)	An audit trail is applied to ensure conformability. The researcher will detail the process of data collection, data analysis, and interpretation of the data. Moreover, confirmation bias and subjectivity will be overcome by using thematic analysis – data is coded in a justifiable manner so that it will provide meaningful analysis after categorisation using Atlas ti. The supervisor is not part of the data collection. Conformability is ensured by plotting existing literature that discussed findings related to the research undertaken.
Authenticity - "refers to the extent to which the research reflects the experiences of the respondents as they lived them and perceived them" (Fade, 2003, p. 144).	-member checking -freedom of the respondent to express themselves (Extracted from Fade, 2003).	The experts are allowed to review the aggregated responses for confirmation. The ethical procedures are ensured through confidentiality and anonymity which allow participants to express themselves truthfully.

3.9. Chapter Summary

This chapter defined the research approach utilised in the study. The study involved two phases – Phase I and Phase II to address the research questions. Phase I of the study involved an exploratory study to confirm the challenges of ISIM in organisations as articulated in the literature. Phase II of the study focused on the design and development of a conceptual model. Since the subject of the study is confined to the information security discipline, it required a specialised group of respondents. In both phases, various organisations were purposively selected for inclusion in the study. As a result, the sampling and selection of respondents were specifically and purposively selected from a pool of sectors related to ICT. Although the selection of the organisations was purposive, the study applied systematic and non-probability sampling to identify target study groups such as expert users and end-users. The data collection in Phase I was conducted in two Iterations, Iteration I and Iteration II, to obtain feedback from two rounds of data from information security experts and end-users. Chapter 4 will present the analysis of the data collected during Phase I of the study.

CHAPTER FOUR

RESEARCH ROADMAP



Introduction and State-of-the-Art of the Research
Development of the Model Concept
Analysis and Results
Chapter 1: Introduction
Outlines Problem Statement and Research Objectives
Chapter 2: Literature Review
Overviews the ISIM processes and Related Work
Chapter 3: Research Methodology
Overviews Philosophy, Approach and Methods
Chapter 4: Exploratory Data Analysis and Discussion of the Findings
Presents Exploratory Analysis and thus fortifying the Problem Statement
Chapter 5: Conceptual Modelling
Derivation of the Model Concept
Chapter 6: Proof-of-Concept Prototype
Prototyping the Model Concept
Chapter 7: Evaluation - Iteration I
Evaluate the Model and Prototype
Chapter 8: Evaluation - Iteration II
Evaluate the Revised Model
Chapter 9: Conclusions and Recommendations
Present Findings, Significance, And Recommendations For Future Research

CHAPTER 4: EXPLORATORY DATA ANALYSIS AND DISCUSSION OF THE FINDINGS

4.1. Introduction

The aim of this chapter is to present the results of the exploratory survey. The purpose of the exploratory study, which is a component of Phase I, is to determine how the efforts of communication and awareness issues are integrated towards the enhancement of Information Security Incident Management (ISIM) in organisations. The organisations were purposively selected from Ethiopia in order to address the paucity of empirical data as a result of low advancements in information security studies. The landscape of information security in Ethiopia is discussed in Section 4.2. This chapter also overviews the instrument used which was designed to collect rich data from the participants (Section 4.3), the profile of the organisations sampled (Section 4.4) and the profile and justification for the participants selected (Section 4.5). Thereafter the data analysis procedure (Section 4.5) and the data analysis of the data collected from the exploratory study (Section 4.7) are presented. Following that, the validity and reliability of the research process are examined to ensure rigour of the methods and the steps involved (Section 4.8). This chapter also considers the ethical procedures applied to protect the confidentiality and privacy of the participants (Section 4.9). The findings of the exploratory survey are compared against related studies for confirmation (Section 4.10) while the implication for a conceptual model is explicated in Section 4.11. The limitations of the methodology and concluding remarks are offered in Section 4.12.

4.2. The Information Security Management Landscape in Ethiopia

Most organisations and institutions have a limited capacity in ISIM. The Information and Network Security Agency (INSA) in Ethiopia aims to address those gaps. The agency assists in setting standards and provisioning training programs for information security (INSA, 2013). The approved proclamation law provided for INSA allows investigators of the agency to undertake ‘virtual’ forensic investigations without judicial permits (Adane, 2022). The Ethiopian Ministry of Communication and Information Technology (MCIT) is responsible for general Information Communication Technology (ICT) and telecommunication matters. Currently, the Ministry of Innovation and Technology (MINT) is responsible for policy formulation and designing strategies for innovation, entrepreneurship and technology related activities in Ethiopia (MINT - Ministry of Innovation and Technology, 2021).

Despite some cyber security frameworks being developed by local experts, a tested, workable and comprehensive cyber security policy and standard are non-existent (Adane, 2022). Information security ethics, law and relevant legislation and regulation concerning the management of information in an organisation were limited for several years (Reba, 2005 & Yilma, 2014). Despite some efforts to draft data protection proclamations, Ethiopia does not have a comprehensive legal instrument to regulate privacy and protect data (Eboibi, 2020). According to the draft National Cyber security Policy and Strategy developed by INSA (2021), there is a mandate to raise public awareness and bolster a national cyber security culture to reduce cyber security vulnerabilities. However, there is a need to provision virtual training opportunities by experts to various stakeholders to support the awareness of security threats (Adane, 2022).

4.3. Instrumentation

The instrumentation for Phase I of the study applied a semi-structured interview mechanism to collect data (Appendix A). The interview guides are consisting of quantitatively and qualitatively delineated questions for various users of organisations. The questions were derived from core research questions to probe respondents in providing rich data to the study. The questionnaire for the survey consists of two parts. Part I was designed for information security experts and end-users of various professions (information security managers, information security auditors and information security risk analysis officers). Part II of the interview guide was developed for organisational end-users that focus on their participation in information security processes, policies, and practices of their organisations. Part I comprises of three sections. Section 1 was devised to acquire background information about the organisations. Section 2 was devised to explore the efforts of coordination of awareness and communication from information security experts and end-users. Section 3 was designed for end-users to obtain data about end-user participation in the process of ISIM.

4.4. Profile of the Organisations Surveyed

The organisations that were included were selected purposively due to their large-scale engagement with information processing and vulnerability to security incidents than other types of organisations. There exists a direct dependence on computer-based and automated technologies for their data processing. The variety of organisations selected allowed the researcher to obtain multiple perspectives. The background and characteristics of organisations involved in the exploratory study are depicted in Table 4-1 (Note the superscript **1** denotes the organisations who participated in Phase I). The table presents the organisational type, organisational category, organisational employee size and the respondents (N) interviewed per organisation (sample) from the organisations.

Table 4-1: Background and Characteristics of the Studied Organisations

Organisation Code	Organisation Type	Organisation Function	Organisation Category	Number of Employees	N
Organisation A^1	Government	Aviation	Commercial	>8000	6
Organisation B^1	Government	Financial	Commercial	>10, 000	4
Organisation C^1	Private	Financial	Commercial	>300	5
Organisation D^1	Government	Media	Corporate (Non-Commercial)	>1500	5
Organisation E^1	Private	Financial	Commercial	>1500	5
Organisation F^1	Agency-Gov	Technology	Agency	>2500	7
				TOTAL	**32**

The details of the studied organisations are described next.

Organisation A^1

Organisation A^1 is a large Ethiopian governmental company, which has been involved in the aviation industry for more than 65 years and consists of more than 8000 employees. It is a pioneer organisation in the country that uses state-of-the-art ICT systems. The organisation uses these technologies to manage its customers' data in flight reservations, employee data and any day-to-day transaction processing operations of the organisation. The organisation deploys information systems to support its functions related to customer information systems, business, employee management, data and information security, telecommunication, and networking systems. Six (6) employees were included from Organisation A^1.

Organisation B^1

Organisation B^1 is a commercial banking organisation, which has been operating in the provision of financial and banking services for the public, personal and governmental institutions for more than 60 years. The organisation adopted an information security system from a South Korean company, which has adequate experience in serving well-known giant telecom organisations such as LG and SAMSUNG in managing and securing customer data and information security issues. This organisation adopted an Integrated Cyber-Security Solution to meet its requirements for cyber threat management, security evaluation and auditing services, information security management and information security awareness. Four (4) employees were included as a sample in the study from Organisation B^1.

Organisation C^1

Organisation C^1 is a private commercial banking institution in Ethiopia. This organisation utilises state-of-the-art ICT tools to automate most of the TPS (Transaction Processing System) and MIS (Management Information Systems) operations of the bank. The bank consists of few physical branches, with no more than 300 employees due to the application of automated technologies such as ATM (Automated Teller Machine) and POS (Point of Sale) for banking with the intent of minimising physical branches and employees. The bank has an information system deployed to facilitate business, commercial, data, telecom, and networking systems. The bank has been attempting to apply both technical and non-technical means of information security. However, the level of non-technical security mechanisms is limited to general corporate security, account usage and application installation. Five (5) employees were included as a sample in the study from Organisation C^1.

Organisation D^1

Organisation D^1 is the largest state-based media institution in the country with more than 1500 employees. The organisation has been involved in the production of news, documentaries and feature analysis for the public. In terms of its technology utilisation, the organisation has deployed versatile hardware and software systems that are being utilised by multiple users. The organisation utilises information systems technologies to administer employee management, customer handling, supplier management, data and information security matters. Although the organisation does not have specialised systems for ISIM, they have a generic system to manage information systems and their employees. Five (5) employees were included as a sample in the study from Organisation D^1.

Organisation E^1

Organisation E^1 is an emerging private bank in the country which has been provisioning banking and financial services for the community. The organisation consists of more than 2500 employees who are deployed in its various branches throughout the country. Most of the information systems that the organisation has been deploying include commercial and business information systems, data management and customer handling information systems. The organisation has an information system management facility. However, they are in the process of introducing an information security system in partnership with other agencies such as INSA. Five (5) employees were included as a sample in the study from Organisation E^1.

Organisation F^1

Organisation F^1 is a state-based security agency that has been working in controlling and safeguarding the national information security issues of the country since 2013. Seven (7) employees were included as a sample in the study from Organisation F^1. Owing to issues of confidentiality, relatively limited data was obtained from the respondents. Thus, additional data was collected though document analysis such as using proclamations, formal documents, printed newsletters, websites, and secondary data and research articles.

4.5. Profile of the Sample

The selection of the organisations for the study considered various criteria such as their alignment to the research problem, their affiliation to the information security incident issues, their willingness to be part of the study and their vulnerability to information security incidents. There were 32 participants involved in the study who provided comprehensive accounts of their experiences with ISIM practices. The sample comprised of information security experts (n=7), information security managers (n=6), information security IT auditors (n=4), operational managers (n=5), information security risk analysis officers (n=3) and end-users (n=7).

Table 4-2: Profile of the Participants

Respondent's Position	Number	Percentages
Information Security Expert	7	22 %
Information Security Manager	6	19 %
Operation Manager	5	16 %
Information Security IT Auditor	4	12 %
Information Security Risk Analysis Officer	3	9 %
End-User	7	22 %
Total	**32**	**100 %**

Most of the respondents in the sample have the basic education and an undergraduate degree. These qualifications are relative to their positions within the organisations. All the organisations indicated that they apply standard information security mechanisms. Most of the organisations have been utilising information systems to achieve their routine business operations such as customer handling, business support, and decision-making processes. The profile of participants involved in Phase I of the sample is depicted in Table 4-2.

4.6. Data Analysis Procedure

The data collected from both the semi-structured interview and document review were analysed systematically. (A link to the redacted raw data is referenced in Appendix G). The data collection in Phase I of the study was conducted using a paper-based questionnaire. Thereafter, the responses to the questions were transcribed and encoded to digital mechanisms. The quantitative data was analysed using Excel and SPSS (Statistical Package for the Social Sciences). The qualitative data was analysed inductively using narrative and content analysis through preformatted themes and genres that are based on the research questions and literature discussed in the preceding chapters. Moreover, the data from the document review was thematically analysed to support some of the data from the semi-structured questionnaire. Some of the findings (such as the Ethiopian contextual settings) were gathered from policy documents, legislations, websites, organisational information security policies etc. Thereafter both the interview and document review from the textual data were analysed in a triangulated manner.

4.7. Data Analysis – Presentation

The following sections present the results of data according to preformatted themes. The design of the questionnaire was separated into two parts:

- Part 1: For all respondents (n=32) (Section 4.7.1)
- Part 2: End-users only (n =7) (Section 4.7.2)

The analysis reported here was initially documented in a journal article authored by Padayachee and Worku (2020). However, this presentation is an extension of the original analysis.

4.7.1. Analysis of Data – Phase I: Part 1

This section discusses the findings of the data for Part 1 of the semi-structured interview questionnaire (Appendix A, Part 1).

Background

Table 4-3 summarises the responses to question #1.1 ("*How many employees currently work in your organisation*?"). The data was obtained from the information security experts only.

Table 4-3: Number of Employees within Sampled Organisations

Organisation	**Number of Employees**
Organisation A[1]	>8000
Organisation B[1]	>10, 000
Organisation C[1]	>300
Organisation D[1]	>1500
Organisation E[1]	>1500
Organisation F[1]	>2500

The responses to question #1.2, ("*To which of the following organisational category does your organisation belong?*") are depicted in Figure 4-1, which represents the organisational categories. The majority of respondents are affiliated with commercial organisations (62.5%; n = 20), while (15.63%; n = 5) are affiliated to corporate and (21.88%; n = 7) are affiliated with the security agency sector. None of the respondents selected the other categories of the organisation such as military, health or service provider.

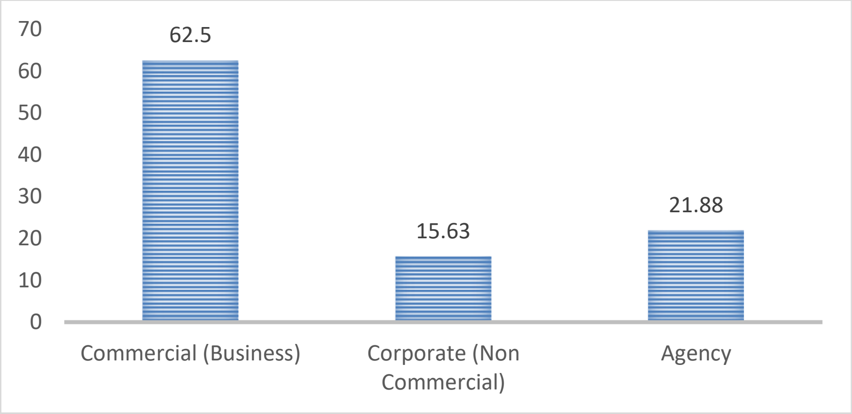


Figure 4-1: Responses across ISIM Parameters

In response to question #1.3, ("*Which of the following information systems does your organisation deploy and utilise?*"), the majority of respondents indicated that they deploy information systems to employee management (90.63%; n=29). While deployment of information systems for Business and Commercial purposes and Customer needs was ranked highly. The deployment of systems for data and information security is below average (46.88%; n=15). Few respondents indicated that their organisation deploys information systems for national security systems and telecom systems. The INSA is responsible for the deployment of information systems for national security. Table 4-4 shows the types of information systems which are deployed in the organisations sampled.

Table 4-4: Information System Deployment Types within the Organisations

Information System Type	**Number**	**Percentage**
Business and Commercial IS (Information Systems)	28	87.50
Customer Information System	25	78.13
Employee Management	29	90.63
Data and Information Security	15	46.88
National Security Systems	7	21.88
Telecom & Network Systems	11	34.38

In response to question #1.4 ("*Which type of information security mechanisms the organisation is utilising?*"), the participants expressed that their organisations have been utilising the basic security features such as antivirus and anti-spyware, firewall service, backup and restore systems and wireless security with some additional technologies. Most respondents indicated that the organisations utilise technical information security (93.75%; n=30), and physical information security (90.63%; n=29). For instance, Organisation A[1] deployed additional technical information security mechanisms such as anti-spyware and antivirus, firewall service, Virtual Private Network (VPN), encryption and decryption methods, Intrusion and Detection Systems (IDS), endpoint systems, restore backup systems and wireless security. The utilisation of non-technical information security (37.5%; n=12) and system and data security (59.38%; n=19) is lower. In Organisation D[1] they have users who interact from diverse areas; thus, they have introduced auto-scan systems for when users log in and use devices. Consequently, all users (i.e., end-users, management, producers, reporters, and directors) are expected to automatically scan any files whether downloading or uploading into the system. Figure 4-2 shows the types of information security mechanisms used by the organisations. As depicted in Table 3-3, the categories regarding the protection of information security mechanisms (in the background component such as technical information security, physical information security, system and data security and non-technical information security) is adapted from Caballero (2013) which is also similar to the ISO/IEC 27035 standard (ISO/IEC, 2016).

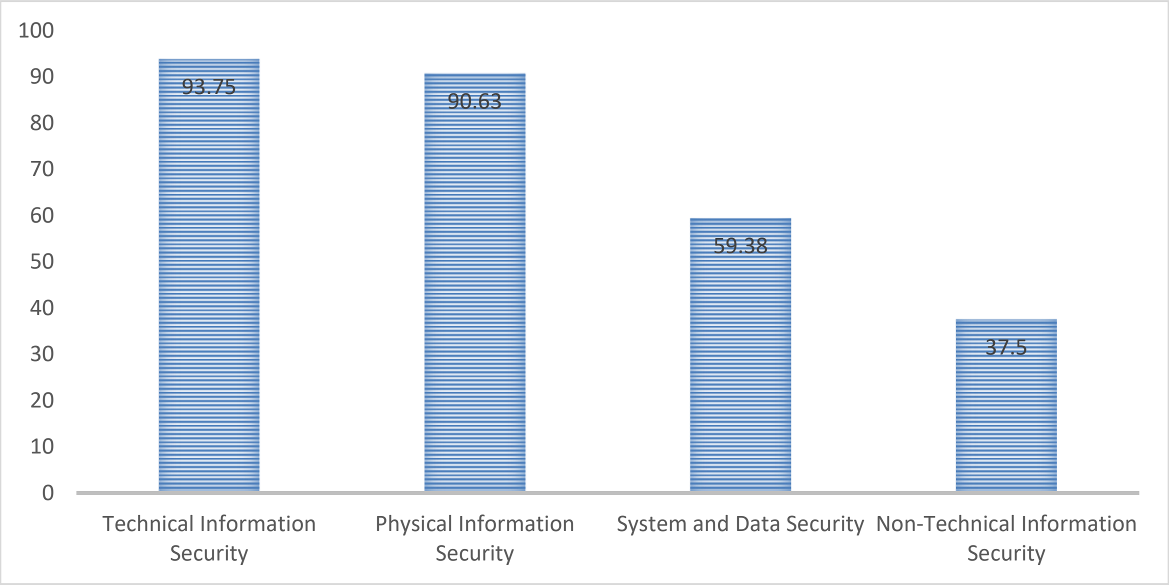


Figure 4-2: Information Security Mechanisms Utilised by the Organisations

In response to question #1.5 ("*Which of the following aspects of information security awareness issues are addressed in your organisational information security policy document?*"), most of the respondents indicated 'account usage'. The results show that most organisations integrate aspects of 'account usage' and 'anti-virus installation' more than any of the other information security management aspects. As most of the organisations focus on customer handling, they emphasise account management. Furthermore, organisations appear to be vulnerable to virus incidents from various sources. In contrast, information security incident handling and awareness issues (31.25%; n=10) are not given due consideration. According to the respondents, Figure 4-3 shows that the handling of information security and awareness to risk are less addressed in comparison to other aspects of information security awareness issues. The categories for the aspects of information security awareness issues integrated in organisations are adapted from Caballero (2013). The percentage is calculated by counting the number of positive responses ('yes' responses) out of the total number of respondents in the sample (32 respondents). The responses from the participants are as follows: security incident handling (31.25%; n=10); risk awareness (28.13%; n=9); account usage (username and password) (90.63%; n=29); internet application (email, downloading, and social media utilisation) (78.13%; n=25); software installation (62.50%; n=20) and antivirus installation and usage (90.63%; n=29).

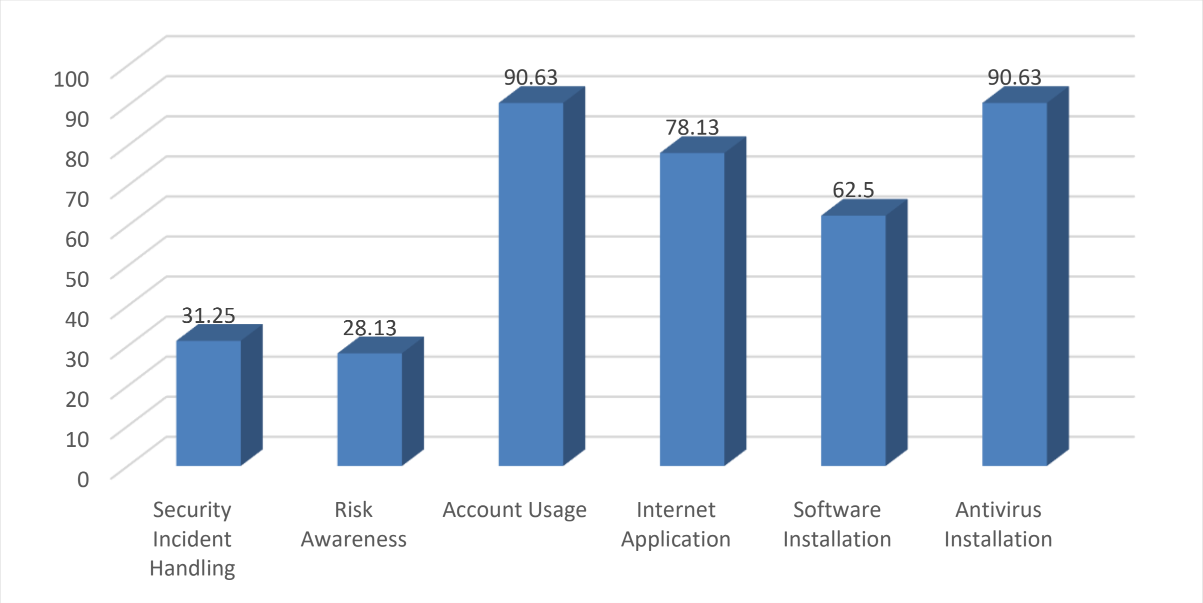


Figure 4-3: Aspects of Information Security Awareness Issues Integrated within Policy Documents

Some organisations (Organisation A[1] and Organisation B[1]) have also supported their information security protection by drafting an in-house information security policy via security experts and distributing it as a binding policy for employees. The ICT office or the Information Security Manager plans and develops information security incident policies and procedures with the support of middle-level management. The creation of awareness and communication aspects in the process of security incident management prevention strategies is also provided to these offices in consultation with the decision makers and management. Some authoritative role is also provided for a few concerned technical employees on some of the technical information security mechanisms.

From the responses to question #1.6 ("*Does your organisation have a specific policy document on information security incident management issues?*"), it was extrapolated that most organisations do not have a specific ISIM policy. However, some of the organisations studied do have a general ICT policy. Organisation A[1] and Organisation B[1] have a specific policy document for ISIM. Organisation C[1] has a generic document on information security policy. The remainder of the organisations do not have such policy documents, or they are still in the process of developing the policy document. Particularly, organisations belonging to the government have their own ISIM policy document, while most private organisations are in the process of developing an ISIM policy document. Table 4-5 shows the types of information security policies the organisations have introduced.

Table 4-5: Information Security Policy Availability

Organisation	**ISIM Policy Availability**
Organisation A[1]	ICT Policy + ISIM Policy
Organisation B[1]	ICT Policy + ISIM Policy
Organisation C[1]	Only Generic ICT Policy
Organisation D[1]	Generic ICT Policy, No ISIM Policy
Organisation E[1]	No ISIM Policy
Organisation F[1]	National Cyber Security Policy & Strategy, No ISIM Policy

It was found that the ISIM documents were initiated by technical ICT experts who had benchmarked from the available international ISO standards. In addition, the awareness aspects (policies and regulations) are also developed and forwarded by information security experts. In the event of an information security vulnerability, it is typically investigated by the information security expert and conveyed to the Chief Executive Officer (CEO) for decision-making. Participant #A1 from Organisation A[1] described how managers are involved in a limited manner in technical issues:

> *"Our management (especially the middle-level management) participate in the process of information security policy approval, security training and overall control of information security procedures. They usually do involve very minimally in technical security issues."* [Participant #A1_Expert User, Organisation A^1]

In response to question #1.7 ("*If your answer to the above question is 'NO', provide possible reasons for the lack of information security and incident management policies?"*), many of the respondents expressed their concern regarding managerial commitment to information security reporting and awareness issues of incidents occurring in the organisation. Some of the challenges reported by the respondents include up-to-date reporting, appropriate awareness protocols and lack of electronic or digital reporting systems. Although most organisations do not have a formal agreement for reporting incidents with their employees, they have endeavoured to provide information regarding incidents via various awareness and training mechanisms.

Information Incident Management Processes Role-Players

From the responses to question #2.1 ("*Which of the role players in your organisation is assigned the responsibility of developing incident management processes?*"), it was found that the national security agency (90.63%; n=29) and the ICT Office (84.38%; n=27) have the mandate and role to formulate information security policies. The majority of the respondents (84.38%; n=27.) indicated that information security policies are formulated and developed by information security experts and submitted to executives or management for approval purposes. Table 4-6 shows the percentage of responses for the role-players involved in ISIM policy formulation.

Table 4-6: Role Players involved in ISIM Policy Formulation

Role Players in ISIM Policy	Number	Percentage
ICT Office	27	84.38
Management or Executive Body	5	15.63
National Regulatory Body	29	90.63
Organisational Stakeholders	2	6.25

Based on the responses concerning how the management plays a role in ISIM policy formulation, it is identified that five organisations (Organisation A^1, Organisation B^1, Organisation D[1], Organisation E[1] and Organisation F[1]) are generally guided by the procedures provisioned by INSA concerning information security policy formulation and development. The information security personnel outline and frame the security policies in order to be approved by the management. The information security policies are initiated, framed and developed by the state affiliated INSA for most governmental organisations and some private organisations.

The role of Management in Information Security Awareness Efforts

In response to question #2.2 ("*Which of the following management levels plays an active role in awareness and communication regarding information security incident management?*"), the participants related that Lower-Level Management (81.25%) played the most active and direct role in the awareness efforts while Top-Level Management played the least active role (12.50%). The upper management are more involved in the administration and approval of the ISIM policy drafted by the information security experts.

The level of involvement per role is summarised in Table 4-7.

Table 4-7: Management Level and their Role in the ISIM Awareness

Management Level	Number	Percentage
Top-Level Management	4	12.50
Middle-Level Management	21	65.63
Low-Level Management	26	81.25

In response to question #2.3 ("*Describe the role that management currently plays/should play in information security incident awareness*"), most of the participants indicated that the awareness support is highly practised by lower managerial bodies. However, specific organisational security procedures (such as internal security manuals and low-level computer protection issues) are entrusted to respective internal employees. In all organisations, while the security personnel drafts and develops security policies, the management body (middle-level and executives) ensures their approval and resource and budget allocation. Case in point:

> *"The management is currently playing the role of approval of policies and initiates to introduce new policies in collaboration with information security technical staff"*
>
> [Participant A11_Expert User, Organisation D[1]]

It is notable that, in Organisation B^1, ISIM is categorised into two structures – information security program management and information security operation centre. The information security program deals with information security awareness, risk assessment, ICT information inventory, asset classification and information security plan and policy enforcement, whereas the information security operation centre is concerned with internal and external protection or defence mechanisms from attacks including physical attack protection. Although organisations (Organisation B^1, C^1, D^1, E^1) do not perform internal IT auditing, Organisation A^1 sometimes undertakes random ethical hacking of its users to control and check IT auditing. The IT auditing section works independently from other parallel ICT structures, which is centrally focused on policy contextualisation and customisation. The interview transcription from an information security expert from Organisation A^1 is a case in point:

> *"The IT auditing department also performs ethical hacking on users who has the account of the organisation."*

[Participant #A6 _Expert User, Organisation B^1]

Although most of the organisations have endeavoured to provide information security training and awareness packages to their employees, management has also faced significant challenges. These challenges arise from staff retention and the provision of security awareness training without disrupting the normal business operations. Lack of skill, awareness, managerial commitment, and adequate budget are raised as critical challenges which impede the effective implementation of communication and awareness practices regarding incident management. Case in point:

> *"Lack of knowledge and managerial commitment are some of the challenges and Training and awareness program on information system security are important for the management to be involved".*

[Participant # A9_ Information Security Manger, Organisation E^1]

Most of the policy design and formulation is prepared by the organisational information security experts in collaboration with INSA. However, most end-users were excluded from participating in the information security policy formulation and incident preparation.

Organisation C^1 does engage a few end-users on higher level security issues. In Organisation D^1, although most employees have normal access roles, specialised access roles also exist. For instance, the line management have an overall managerial administration role, whereas, the executive and boards have a role of task approval once done by other staff. Other stakeholders that are involved in the system also include reporters, editors, program owners, traffic controllers and directors who have their own access role and privileges. The other staff categories such as field staff and laptop users only access the system without any interaction to edit contents.

The role of Management in Information Security Communication Efforts

In response to question #2.4 ("*Describe the role that management currently plays/should play in information security incident communication*"), the participants related that the communication efforts by the managers are largely promising. There have been a few attempts by the management of the organisations to plan for information security reporting in their policy documents. As part of the information security incident reporting strategies, the management of only Organisation A^1, Organisation C^1 and Organisation E^1 have been highly committed to availing the utilisation of paper-based communication mechanisms and other forms of promotion (such as newsletters, postings, printed articles, and information security guides), usually when an incident has been encountered. It was revealed that the incident management reporting is well-articulated among information security experts. The communication among management and end-users is more limited. All organisations have been utilising conventional means of communication such as face-to-face meetings and internal letters for incident reporting.

In terms of information security incident communication, all levels of management have satisfactory levels of practice and experience of reporting incidents to their respective management bodies (low-level, middle-level and top-management), but the level of communication skills differs between the management and employee job categories, in that most information security experts and some low-level managers do report and communicate security incidents when encountered.

Participant #27 (Organisation F^1) suggested that there should be a plan for organised reporting on incident issues. Furthermore, organisations should provide mechanisms for clustering and categorising information security incidents to create a database of incidents to support decision-making:

> *"It would be good if organisations have plan for organized reporting/communication strategies that can raise the awareness of employees".*
>
> *"It would have been good also if our organisation can categorize and cluster information security incidents and create a knowledge base so that it can be retrieved and disseminated to the staff".*
>
> [Participant # A27_Expert User, Organisation F^1]

In Organisation E^1, only the line management and ICT staff are involved in the formulation and communication of information security incident policy matters with no involvement of end-users and other stakeholders. The reason mentioned for the lack of involvement is related to confidentiality and that organisations need to ensure that the information is accessible only to ICT experts and the relevant management body. Moreover, this organisation does not have instituted procedures and practices on ISIM guidelines to assist in engaging with end-users. They are also not part of the ISIM program; however, the organisation attempts to raise awareness and inform staff about the existing information security policies and how to manage and use them. Additionally, Organisation E^1 assumes that the best way to plan and raise awareness and communication skills among employees and stakeholders is through the provision of training and dispatching brochures about information security incidents and vulnerabilities when they occur.

Information Security Standard Utilisation

In response to question #2.5 ("*Which of the following standards does your organisation currently comply?*"), the majority of respondents indicated that their organisation does not adopt standards. Organisation A^1 is in the process of adopting the ISO/IEC 27035 standard. The existing organisational general ICT and information security policy documents do not inherit components from the international standards, but as written in their policy document, information security is defined as follows: *“Computer security is a branch of technology known as information security as applied to computers and networks”* (Information Security Policy Guideline Document, Organisation D[1]).

Table 4-8 depicts the responses for the various ISIM standards adopted in the studied organisations.

Table 4-8: ISIM Standard Utilisation in Organisations

ISIM Standards	**Number**	**Percentage**
ISO/IEC 27001	0	0.00
ISO/IEC 27002 Standard	0	0.00
ISO/IEC 27035 Standard	5	15.63
The ITIL Framework	0	0.00
NIST Special Publication 800-61	0	0.00
ENISA-Good Practice Guide for Incident Management	0	0.00
Nor SIS- Guide for Incident Management	0	0.00
SANS-Incident Handler's Handbook	0	0.00
COBIT 5	3	9.38
ISMM	0	0.00
IEEE 802.11	0	0.00
Other	0	0.00

Respondents indicated that the limited adoption rate was owing to limited awareness and commitment of the available standards. Cases in point:

> *“In the mean time, our organisation has developed an ad-hoc information security policy document by the technical group teams from ICT and management body. We also consult the national security regulatory body called INSA for advanced security matters. However, Lack of adequate knowledge on the availability of information security standards issues and lack of management commitment to use the existing standards are the factors which have been hindering our organisation to adapt the standards [sic]”.*
>
> [Participant # A6, Information security manager, Organisation B[1]]

> *"The management and information security personnel of the organisation have little understanding of the availability of such standards. However, we are planning to have a suitable standard after we study the relevant one".*
>
> [Participant #A11_Expert User, Organisation D^1]

> *"Lack of adequate knowledge on the availability of information security standards issues and lack of management commitment to use the existing standards are the factors which has been hindering our organisation to adapt the standards".*
>
> [Participant # A6, Information security manager, Organisation B^1]

From the responses to question #2.6 ("*If your organisation uses any of the above information security management standards, how does it implement this with respect to information security incident management processes?"*), it was extrapolated that only Organisation A^1 is partially complying with the ISO 27035 standard. While a few organisations have attempted to introduce information security standards, Organisation B^1 has endeavoured to use the COBIT standard with limited specification. However, the remaining organisations do not have practical applications of any of the international information security incident standards available.

Additionally, the participants implied that the adoption of such standards would be irrelevant for their organisational information security incident processes. This sentiment is shared by Organisation E^1, which means they have not adopted or used any internationally set information security standards. However, they have formulated internal guidelines for information security policies.

Formal Agreements for Information Security Incident Management

From the responses to question #2.8 ("*Does your organisation have any formal agreement with employees regarding information security incident management process issues?*"), it was found that the application of standardised agreements with employees concerning information security policies was limited. Most information security experts indicated that their organisations do not have a formal agreement with employees concerning information security policies.

In response to question #2.9 ("*If your answer to the above question is 'NO', provide possible reasons for the lack of such agreement between the organisation and the employees*"), the respondents cited lack of awareness as the main issue.

Participant #A24 (Organisation F^1) cites following the reason:

> *"The management and other staff do not have that much adequate knowledge on the existence of such standards."*

[Participant #A24_Expert User, Organisation F^1]

Also, an information security expert from Organisation F^1 contends that the lack of formal agreements is due to the organisational culture:

> *"There was not any form of organisational information security agreement due to policy and organisational culture".*

[Participant #A17_Expert User, Organisation F^1]

In considering the responses to question #2.10 ("*Assess your organisation's information security incident management processes"*), it was found that 'incident response' is the most formalised action while 'incident assessment and analysis' is the least formalised action. There is limited ICT support for many of the ISIM processes such as incident preparation and definition, incident detection, incident assessment and analysis, incident communication and incident policy efficiency. For instance, five respondents indicated that formal documentation in the process of incident preparation and definition does exist. Twenty-eight (28) respondents indicated that the incident preparation and definition phase of ISIM is supported by decision-makers. Table 4-9 summarises the assessment of ISIM parameters across various managerial factors.

Table 4-9: Assessment of ISIM Parameters Across Various Managerial Factors

Incident Management Processes	**Does it have a formal document?**	**Do they plan for it?**	**Is it supported by ICT systems?**	**Is it supported by Decision Makers?**	**% Affirmative responses**
Incident preparation and definition	5	11	5	28	**38%**
Incident identification/ detection	7	7	18	5	**29%**
Incident assessment and analysis	6	6	6	4	**17%**
Incident response	15	15	18	15	**49%**
Incident awareness and anticipation	11	14	3	9	**29%**
Incident communication and reporting	13	13	2	7	**27%**
Information security policy efficiency	6	6	2	10	**19%**

‘Incident response’ had the most affirmative responses for having formal documentation (15) and having a plan (15) in place. Both ‘incident identification/detection’ and ‘incident response’ had the largest number of affirmative responses (18) with respect to being supported by ICT systems. This suggests that there are technical controls for the detection and response of information security incidents. The most affirmative responses for ‘decision maker support’ was the process of ‘incident preparation and definition’ (28). The items ranked from the lower end of the scale included ‘incident identification/detection’ (29%), ‘incident awareness and anticipation’ (29%), ‘incident communication and reporting’ (27%), ‘information security policy efficiency’ (19%) and ‘incident assessment and analysis’ (17%).

Level of information security incident awareness and risk understanding

The responses to question # 2.11 (“*Rate the level of information security incident awareness and risk understanding of employees with respect to the following indicators? (Excellent, Very Good, Good, Satisfactory, Fair, Poor)*”), are summarised in Table 4-10. The awareness for ISIM evaluation matrix for indicators was calculated by applying the respondents’ score from ‘Poor’ to ‘Excellent’ which was encoded into Likert scales (from 1 to 6 respectively) for standardised analysis. For each category of management, the mean was calculated in order to cumulatively represent the overall response in the category. Although the generic results show a lower value to all management categories, the awareness matrix rate for the ISIRT category is much higher than the remainder of the categories.

Table 4-10: An ISIM Awareness Assessment Indicator Matrix

Awareness indicators	**Top-Level Management**	**Middle-Level Management**	**Low-Level Management**	**End-Users**	**ISIRT**
Knowledge about ICT systems and components	1.9	3.12	3.1	2.1	5
Information security competence	1.2	2	3.4	1.1	5.8
Reporting security incidents	1.1	2.8	2.3	1.9	5.7
Up-to-date knowledge about relevant threats	1.9	2.7	1.9	1.8	4.1
Learning from previous incidents	3.9	4.2	2.9	3.7	5.8
Mean Awareness Indicator	**2**	**2.9**	**2.7**	**2.1**	**5.3**

Although there is a general incident understanding and awareness of the existence of information security incident threats and vulnerabilities among all users, the level of specific awareness about such security incidents is not consistent among the employees' categories (end-user, security expert, and managerial levels). The level of awareness among the ISIRT or expert users is much higher (mean=5.3). Although this result was anticipated for experts, the level of awareness among the remaining stakeholders is below average. The awareness assessment indicator mean per category was as follows – Top-Level Management with (2) mean, Middle-Level Management with (2.9) mean, Low-Level Management with (2.7) mean and end-users with (2.1) mean.

However, in certain technologically penetrated organisations (Organisation A[1] and Organisation B[1]), the level of information security knowledge, competence and learning from previous incidents is higher among top-level and middle-level managers compared with those on lower levels. In Organisation A[1], a difference in the information security incident level of risk awareness and conceptualisation exists among different managerial groups and ISIRT experts in that the management has a lower level of basic awareness concerning security threats and vulnerabilities. This implies that the ICT personnel and information security experts have more in-depth awareness about security incidents and policy matters as compared with the management and end-users. Though most employees in each managerial category (top-level, middle-level, low-level) have a general understanding of information security issues, the level of competency in responding to incidents is much higher among ICT personnel and security experts, as anticipated. Information security incidents are generally reported back to information security experts and higher-level management. Although ISIRTs have no formal, automated, and documented learning system platforms, there have been efforts to learn from past incidents.

Workflow for Information Security Incident Management

In response to question #2.12 ("*Does your organisation have a specific workflow for information security incident management processes?"),* none of the organisations have been utilising formal or reputable workflow mechanisms that could enhance transparency and the incident reporting channelled to any unit or office in the organisation. There was also no evidence depicting the application of specific workflows in the process of ISIM practices. The organisations have never implemented any workflow for their security handling processes.

As the response to question #2.13 ("*If you have answered 'YES' to the previous question, comment on the following aspects:", a. How is it prepared and maintained? and b. How is it communicated to the members of the incident management team?*"), was negative, it was not possible to obtain any further responses on this issue.

Information Security Awareness Raising Methods among Management

Most of the practices utilised by organisations to raise the awareness about ISIM issues are through applying 'educational', 'promotional' and 'informational methods', in response to question # 2.14 ("*Which of the following methods support managers in increasing awareness of information security incident management policies in your organisation?"*). The awareness raising mechanisms utilised by the organisations in the study for ISIM are summarised in Table 4-11.

Table 4-11: ISIM Awareness-Raising Methods used by the Organisations

Awareness raising methods	Org A¹	Org B¹	Org C¹	Org D¹	Org E¹	Org F¹
Promotional methods	√	√	√	√	√	√
Enforcing methods	√	X	X	X	X	√
Educational methods	√	√	√	√	√	√
Informational methods (i.e., updates on information security)	√	√	√	√	√	√
Digital methods	X	X	X	X	X	√
Face-to-face guidance methods	√	√	X	√	X	√

Abbreviation: Org (Organisation)

Some of the mechanisms for ISIM awareness raising and training for the employees include paper-based presentations and interactive instructional methods. Only Organisation A^1 and Organisation F^1 use 'enforcing methods' that obligates employees to abide by the implemented information security policies and procedures. The organisations used enforcing mechanisms with respect to the account and system policies which are audited in the form of performance evaluations of the employee. The use of 'digital methods' to ensure information security awareness was limited. 'Digital methods' is practiced only by organisation F^1. Disciplinary measures incorporating responsibility, penalties and accountability were not given due consideration by the organisations under study.

Information security incident reporting mechanisms

From the responses to question #2.15 ("*Which of the following reporting mechanisms does your organisation use to communicate to the staff about information security incidents?"*), it was inferred that most of the organisations utilised the manual mechanisms of information security incident reporting. The application of the reporting mechanisms for ISIM is as follows: manual reporting (93.75%; n=30), face-to-face interaction (62.50%; n=20), electronic mechanism (46.88%; n=15), telephone reporting (43.75%; n=14), audio-visual mechanism (21.88%; n=7) and application software (customised) (15.63%; n=5). The use of specialised software and digital technologies was not given the due regard. The usage per reporting mechanism is summarised in Table 4-12.

Table 4-12: Information Security Incident Reporting Mechanisms

Reporting Mechanism	Number	Percentage
Telephone Reporting	14	43.75%
Manual/Paper Based Reporting	30	93.75%
Face-to-Face Contact or meeting	20	62.50%
Electronic Means (Email, social media, Mobile Phone)	15	46.88%
Audio-Visual/Multimedia format	7	21.88%
Special Software application for incident reporting	5	15.63%

Information Security Users' Communication Experience in Organisations

From the responses to question #2.16 ("*How would you assess the level of employees' communication experience with respect to information security incident management among different clusters of employees in your organisation*?"), it was deduced that the extent of an employee's communication experience concerning ISIM was found to be between a 'very poor' and 'fair' level across all managerial levels, except for ISIRTs. This indicates that peer-to-peer and vertical communication among end-users and managers was limited in comparison with peer-to-peer communication among ISIRTs.

In response to question #2.17 ("*How frequently does your organisation communicate information security incidents?*"), the data showed that the occurrence of communication concerning information security incidents is fundamentally unorganised and uncoordinated. It appears that information security incident communication efforts (both peer-to-peer and laterally) are reactive and occur after an incident is discovered.

Figure 4-4 depicts the frequency of information security incident communication among respondents. As shown in figure 4-4, the majority of the participants selected the "When an incident happens" option in response to the frequency of ISIM communication.

Case in point that demonstrates the infrequency of communiqués regarding information security incidents:

> "*I usually communicate among ourselves and security personnel when an incident arises on how to protect and mitigate current security issues without using any formal means of information security communication mechanism [sic]*".

[Participant #A11, _Expert User, Organisation D[1]]

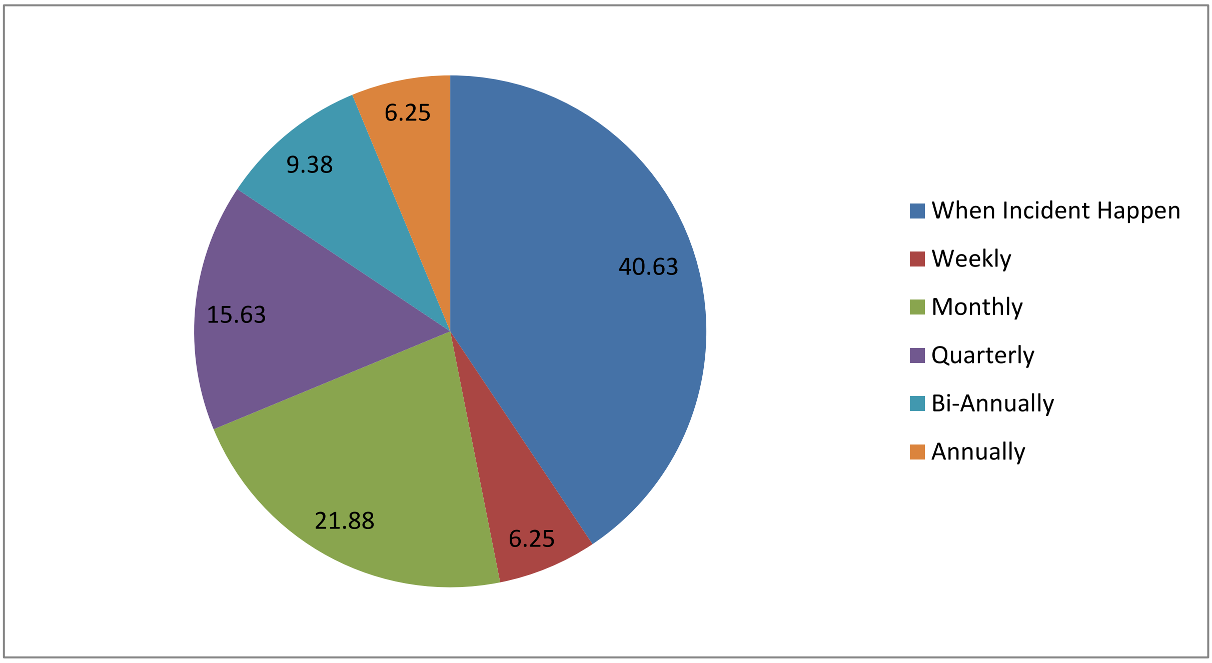


Figure 4-4: Frequency of ISIM Communications

Even though the organisations have endeavoured to introduce basic information security incident communication and awareness mechanisms, it is poorly coordinated. Numerous information security experts experienced unauthorised access by employees (i.e., insiders) who share their account privileges with other insiders despite their organisational information security policy that restricts sharing user privileges, which may expose the organisation to vulnerabilities.

Participant #A3 (Organisation B[1]), who is an information security expert, demonstrates another dimension to underreporting of information security incidents, where experts assume they have failed in preventing incidents.

A case in point:

> *"Our organisation provides basic training and awareness concepts to the staff both at the time of recruitment and during their job on some critical issues that they should do, especially training related to account (username and password) usage, software installation and anti-virus/malware issues. Regarding the communication of incidents, we are using some form of paper based reporting and face-to-face meetings in order to share information on the existing security incidents. Most of the communication and awareness aspects are done by the technical persons (information security office) of the organisation. However, we sometimes face that some information security experts do not report/communicate incidents because they think that they are responsible for the failure."*

[Participant #A3, Expert User, Organisation B^1]

Approaches to Information Security Incident Communication Efforts

In response to question #2.18 ("*How does your organisation communicate and report information security incidents to employees?*"), the data showed that the efforts of reporting and communication for information security incidents are highly disjointed. It was established that most organisations communicate through meetings (face-to-face). Only two organisations (Organisation A^1 and Organisation B^1) coordinate communication efforts electronically.

A case in point:

> "*The routine information security cases are not communicated to the operational staff, whereas the filtered or analysed information is not reported to decision-makers. We were also rarely communicated about information security incidents that were believed to be critical by the ICT staff and experts" [sic].*

[Participant #A17_Expert User, Organisation F^1]

In response to question #2.19 ("*In your opinion, what should be done to improve the awareness and communication and strategies among employees and stakeholders in order to enhance information security incident management in your organisation?*"), the majority of respondents (91%) recommended training, policy change, and analysed and categorised incident information based on their literacy level. A few of the suggestions raised by the respondents include specialised reporting mechanisms, categorisation of incidents based on the individual's knowledge base, analysed case histories, participatory incident reporting and awareness systems, policy revision and training. Some suggestions from the respondents are indicated as follows:

> *"We need a special reporting mechanism for information security incident that faces our organisation. Also we need some categorized information on information security incident pertaining to our literacy level."*
>
> *"We need information not only on incident cases, but also on analyzed information security incident information."*
>
> [Participant #A27_Expert User, Organisation F[1]]
>
> *"It would be very good if the organisation have implemented a participatory incident reporting and awareness mechanism."*
>
> [Participant #A11_Expert User, Organisation D[1]]
>
> *"Policy revision and training"*
>
> [Participant #A1_Expert User, Organisation A[1]]

Challenges of Communication and Awareness Efforts in Organisations

In response to question #2.20 ("*What kind of challenges does your organisation face regarding information security incident communication and awareness cases?*"), the respondents proffered several challenges. The following challenges were raised: lack of policies, planning and awareness and lack of managerial commitment, and lack of centres for information security training.

More specifically, the challenges submitted include:

- Lack of organised plan and policies.
- Lack of managerial commitment.
- Lack of established office or body for information security.
- Addressing all employees through training is difficult due to the business operation.
- Lack of awareness and communication regarding information security incident issues.
- Lack of personalised incident information according to roles and responsibilities.

Cases in point:

> *"Organized policies, Management commitment, Lack of awareness about information security incident issues"*
>
> [Participant # A12_Expert User, Organisation B[1]]
>
> *"Lack of plan and polices, Lack of managerial commitment, Lack of established office or body for information security".*
>
> [Participant #A14_Expert User, Organisation C[1]]
>
> *"...addressing all employees through training is difficult due to the business operation".*
>
> [Participant #A1_Expert User, Organisation A[1]]
>
> *"Employees use different external device without proper protection control against virus and spyware".*
>
> [Participant # A13_Expert User, Organisation D[1]]
>
> *"There is some staff that needs only pure information security incident information. There are also other staffs that need analyzed and summarized information about incidents such as managers and executives."*
>
> *"The routine information security cases are not communicated to the operational staff, whereas the filtered or analyzed information is not reported to decision makers. We*

> *were also rarely communicated about information security incidents that were believed to be critical by the ICT staff and experts."*

[Participant #A17_Expert User, Organisation F^1]

In response to the question #2.21 ("*In your opinion, how can communication with regard to information security incident management be effectively integrated into your organisational information security policy?*"), the participants proffered several improvements.

The respondents suggested the following improvements:

- Incorporation of reporting policies within ISIM.
- Information security incident training.
- Strong managerial commitment.
- Proactive information security incident planning.
- Enforcing automated information security incident communication (i.e., website or intranet).
- Constructive relationship between an organisation's ISIRT and public relations.
- Adoption of established information security standards (such as ISO/IEC standards).
- Building an information security database, where records are maintained by the ISIRT and shared with employees.
- Recruitment and deployment of ISIRTs to all branches.

Cases in point include:

> *"By preparing ICT Security Incident communication policy and procedure"*

[Participant #A1_Expert User, Organisation A^1]

> *"It will be integrated more with proactive planning, regular update of the training"*

[Participant # A12_Expert User, Organisation B^1]

"If the top-management take the issues as any other job and daily activity it will get more focus"

[Participant #A 13_Expert User, Organisation D[1]]

"It should be part and parcel of the ICT policy"

[Participant #A 15_Expert User, Organisation E[1]]

"It would be good if organisations have plan for organized reporting/communication strategies that can raise the awareness of employees"

[Participant # A27_Expert User, Organisation F[1]]

"Although we (the end-users) are the ultimate routine agents of the security system, policy and information, we have little awareness and understanding of the existing organisational information security policies and procedures. Even it would have been better if they can make it available on the organisational website or intranet system of the organisation."

[Participant # A29_Expert User, Organisation E[1]]

End-users' Engagement

The following analysis presents data findings from Part I (Section 3) of the questionnaire that mainly considers the role of end-users and participation in the process of information security incident communication and awareness practices (see Appendix A, Part I, Section 3). In response to question #3.1 ("*Identify the role and relation of the various stakeholders with regard to information security incident management issues in your organisation*"), the data showed that the participation of end-users is limited in information security policy formulation, implementation and ISIM processes. Both the development of ISIM training materials and the training activities are managed by the ISIRT for all employees with the support of management (middle-level management). Nevertheless, the participation of end-users in the policy and training process is limited. The main justifications provided for the limited involvement of end-users in the process include confidentiality of security incidents, work overload and the lack of expertise in information security. Only two organisations (Organisation A[1] and Organisation

B[1]) have made progress towards engaging end-users in the process of information security policy, planning and preparation practices. The organisations provide consultative training for the end-users of their units. In doing so, working time of the end-users and the training scheme were balanced.

In one of the studied organisations (Organisation D[1]), the implementation of access control was imposed as multiple users accessed the deployed systems. As a result of such multiple concurrent accesses, threats and vulnerabilities of information security exist. In this organisation, reporters only access the system to put or upload versatile program data (i.e., textual, image, sound, video, and multimedia) without the ability to duplicate, edit or transfer it to any other medium (i.e., disk, compact disk, or hard drives). Consequently, the role of the ICT personnel was to access the system directly either to enter or retrieve data. This role included operational control and data management with full support of help desks. To protect the informational assets of the organisation from any potential loss or damage, the existing policy document, which was developed in-house, restricted users from plugging any electronic devices into any of the available media production workstations. Any kind of data entry into the system by any user is registered in the system to be screened and overseen by the respective approval unit. The data will automatically be archived and recorded for two months once it has been uploaded by users, which then can be tracked by the ICT personnel.

In response to question #3.2 ("*Does your organisation involve end-users in the process of Information Security Communication and Awareness Matters*?"), the data showed that the majority of the respondents (93.75%; n=30) indicated that their organisations do not involve end-users in the process of information security practices (Figure 4-5). Thus, the level of engagement of end-users in all the processes of the information security practices is limited.

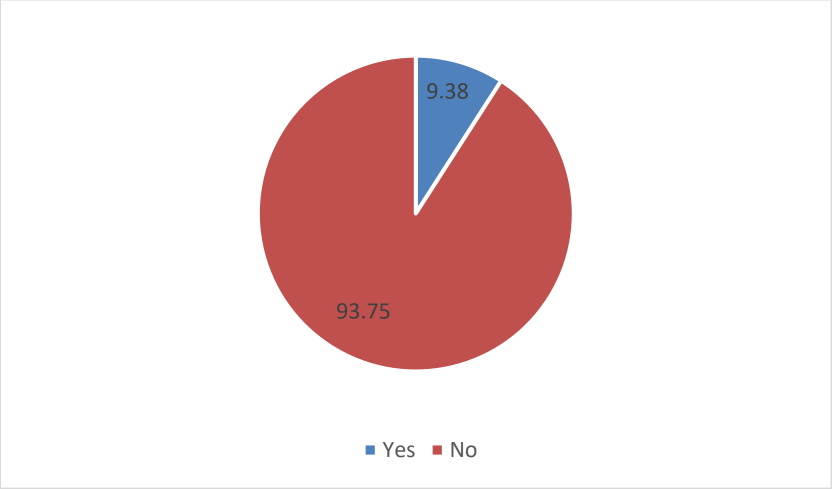


Figure 4-5: Participation of End-Users in Information Security Practices

In response to question #3.3 ("*If Yes, describe how your organisation involves end-users in the process of information security management and policy issues*"), the data showed that most users and employees were not actively participating in information security policy formulation. Furthermore, related information was not shared among users. In all the organisations, based on the gathered data from end-users, the participation of end-users in the process of information security incident planning and preparation processes is limited. Cases in point are:

"No, I was not part of any information security policy formulation or guideline."

[Participant #A2, End-user, Organisation B[1]]

"No, I was not involved in any of information security policy and guideline issues."

[Participant #A4_ End-user, Organisation D[1]]

Those organisations who engage end-users in the process of information security and incident management policy issues, indicated that they required it for feedback or opinion regarding the almost approved security policy documents.

Case in point:

> *"We only involve them to gather feedback about the information security encountering mechanisms"*

[Participant # A5_ End-user, Organisation D^1]

In response to question #3.4 ("*If No, Describe the reason why your organisation does not involve end-users in the process of information security management and policy issues*"), various reasons were proffered for the lack of engagement. For organisations which do not engage end-users in ISIM processes, respondents described that work overload and the lack of technical understanding among end-users are key factors. Information security experts claim that end-users have a poor understanding of policy and incident management issues. As a result, they tend to exclude them in ISIM processes. One reason cited by Participant #A22 is that end-users do not have detailed technical understanding about information security incident matters:

> *"Our organisation usually initiates policies by its ICT office and downwards for end-users for its implementation. End-users are only involved in executing the policy. We believe that they do not have the knowledge about detailed and technical information security incident matters".*

[Participant # A22_Expert User, Organisation B^1]

In response to question # 3.5 ("*Which information security incident cases regarding end-users are taken into account by the organisation?*"), the data revealed that 46.9% (n=15) of respondents are involved in 'only non-technical policy issues'. (Note: The percentage figure is derived out of the total respondents (n=32); however, not all respondents indicated a response on the options provided). None of the respondents indicated the involvement of end-users in technical aspects. 12.5% (n=4) of respondents indicated the participation of end-users for all security cases. This is attributed to the low level of engagement of end-users towards security issues. Table 4-13 shows the level of participation of end-users with its percentage.

Table 4-13: Participation of End-Users in ISIM Processes

End-User Participation Types	Number (N)	Percentage % (32)
All Security Cases	4	12.5%
Only Non-Technical Cases (Such as policy, procedure, compliance and enforcement)	15	46.9%
Only Technical Cases	0	0.00%
Higher-Level Policy Issues	1	3.1%

4.7.2. Analysis of Data – Phase I: Part 2

The end-users (n=7) were questioned regarding their level of engagement in a separate interview. Since the aim of the study is to explore the role of end-users in ISIM practices, Part 2 of the questionnaire was administered, coded, and analysed separately particularly for end-users.

The data collected in response to question #1 ("*Have you ever been involved in the setting of information incident security management guidelines in your organisation?*"), revealed that there is limited involvement of end-users in the ISIM processes — planning, preparation, and policy formulation. It appears that the majority of organisations do not have the culture of engaging all users including end-users in ISIM and awareness practices. A case in point by Participant # B5, end-user from organisation E[1], suggests that:

> *"We do the information security policy with the involvement of ICT staff only and also we have agreed to share information and draft polices with ICT concerned parties."*

[Participant # B5_End-user, Organisation E[1]]

As the previous response was negative, no further information was collected from question #2 *("If your answer to the above question is 'YES', describe your level of participation."*).

In response to question #3 ("*Have you ever participated in an information security incident awareness program?*"), the end-users indicated that they were not engaged in information security policy awareness and formulation.

An end-user Participant #B2, from organisation B[1] indicated the following:

> *"I was only participated in one training session organized by the organisation about general information security and how to protect ourselves".*

[Participant # B2_End-user, Organisation B[1]]

One end-user, Participant #B3, from organisation C[1], indicated the participation as the following:

> *"Yes, I have been part of the information security awareness and training sessions".*

[Participant # B3_End-user, Organisation C[1]]

In response to question #4 *("If your answer to the above question is 'YES', describe your role with regard to communication and awareness aspects to improve information security incident management in your organisation"),* one end-user from organisation C[1] (Participant B#3) described the general involvement level as the following:

> *"The ICT office with information security experts describes some aspects of contemporary security threats and they communicate us with papers and presentations. And they inform us how to protect and work in our routine operation"*

[Participant B #3_End-user, Organisation C[1]]

In response to question #5 ("*If your answer to the question 3 is 'NO', what should your organisation put into practice to involve end-users and stakeholders to become aware and communicate with them, in order to improve information security incident management?*"), the data revealed that an interest among end-users to be part of the processes of ISIM does exist. The end-users stressed that they prefer to be engaged in information security incident issues for a shared understanding and up-skilling. Information security policies are framed by the top management and ICT officers. The information security policies have been developed with information security experts and managers without the notification or consultation of end-users. End-users proposed that facets such as participation, up-to-date information on incidents, communication of incidents, incident handling and collaborative discussions with all stakeholders of the organisation are of importance to them. The following responses substantiate these propositions from the end-users. An end-user from Organisation A[1] indicated that the participation of end-users in the process of ISIM benefits not only the individual, but also the organisation. Cases in point:

> *"It would have been very good if our organisation would have provided me the opportunity to participate in information security issues that concern us to the benefit of the organisation"*
>
> [Participant B #1_ End-User, Organisation A[1]].
>
> *"I believe that end-users are part of the organisation and the primary vulnerable if incidents happen. So I believe the management should consider us in not only policy issues but also regular update information about incidents"*
>
> [Participant B #1, _End-User, Organisation A[1]].
>
> *"It is good if they can involve us and provide the necessary training and communication on up- to-date security issues"*
>
> [Participant B #4_ End-User, Organisation D[1]].
>
> *"Creating awareness regarding how to handle information security issues"*
>
> [Participant B #5_End-User, Organisation E[1]].
>
> *"It would be very good if our organisation could create a routine program on awareness raising issue. Creating awareness regarding how to handle information security issues"*
>
> [Participant B #6_End-User, Organisation F[1]].

> *"It is better if our organisation can create and organize different stakeholders of our organisation (end-users, managers, security experts and ICT personnel) so that they can discuss and solve information security incident problems"*
>
> [Participant B #6_ End-User, Organisation F^1].

> *"It is important to have up-to-date information on the existing organisational information security incident and policies"*
>
> [Participant B #3_End-User, Organisation C^1].

The responses to question #6 ("*In your opinion, how can your organisation plan and prepare better information security management through awareness and communication mechanisms?*") were incidental to the investigation. Despite some end-users stating opinions that were not directly related to the question raised, issues of participation, collaboration, communication, provision of awareness protocols and training were emphasised. The following cases in point also substantiate the requirement for end-user participation in ISIM:

> "*I think it will be good if the organisation frequently and consistently practice information security training and awareness to all employees irrespective of their position and role. And we also need a computer-based system that alarms us that we are under threat or to aware us [sic]*"
>
> [Participant B #3_End-user, Organisation C^1].

> *"It is good if organisation can keep update us on information security policies, current incidents, how to combat from their responses and to collaborate us in the operational activities of the security program"*
>
> [Participant B #4_End-user, Organisation D^1].

> *"Besides reporting on critical incidents of the organisation, it is important to have up-to-date information on the existing organisational information security incident and policies."*
>
> [Participant B #5_End-user, Organisation E^1].

> *"I think it would be improved if organisation could start working together with all concerned stakeholders of the organisation in terms of security threats orientation, security decisions taken and lessons learnt which can help us to learn and prevent from repeated mistakes"*
>
> [Participant B #6_End-user, Organisation F^1].
>
> *"I believe that the management and all staff should work in collaboration in order for the security policy and controls to work better"*
>
> [Participant B #2, End-user, Organisation B^1]
>
> *"It is good if they can involve us and provide the necessary training and communication on up- to-date security issues"*
>
> [Participant B #4_End-user, Organisation D^1]

Thus, it was gathered from the end-user perspective that the role of communication, participation and awareness for information security incident management is a critical convention within the organisations studied.

4.7.3. Document Analysis Synopsis

This section presents a synopsis of the document analysis undertaken. As most of the organisations (Organisation C^1, Organisation D^1 and Organisation E^1, Organisation F^1) do not own formal ISIM policy documents, related documents such as generic ICT policies, organisational user management documents and manuals were utilised to triangulate the responses from the end-users and the information security experts. The analysed documents included national ICT policies, information security policy documents, ICT proclamations, regulatory frameworks, organisational ICT policies and other supportive documents from websites. Some information security analysis documents were also considered in understanding the existing situations of the regulatory, management and administrative parameters of the organisational framework. Table 4-14 shows the documents analysed per organisation studied. Although Organisations A^1 and B^1 have general ICT and ISIM policy documents, it was not possible to obtain the documents, however, information about the content of the policy documents was triangulated through interviews with key information security experts.

Table 4-14: Summary of the Document Analysis

Organisation	Analysed Documents
National Level	-National Information and Communication Technology (ICT) Policy and Strategy (FDRE, 2016). -National Cyber Security Policy and Strategy (INSA, 2021) -Proclamation on Telecom and ICT Services
Organisation A^1	-ICT Policy – the ISIM policy was in process and confidential
Organisation B^1	-ICT Policy – the ISIM policy was in process
Organisation C^1	-Generic ICT Policy (Draft)
Organisation D^1	-ICT Directive and Guideline -Media and ICT Documents - Information Security Policy
Organisation E^1	-No ICT and ISIM Policy documents available
Organisation F^1	-Information Security Agency Establishment (Legislation) (A legislation that provides INSA the mandate to control the information security services of the country)

The document analysis of the information security policies revealed that most organisational information security documents do not inherit components from the international standards. Organisation D^1 has a generic ICT policy which includes ISIM as a section to describe the general framework of incident management in the organisation. Although the policy document does not specifically adopt an established ISO/IEC standard, the policy is constituted with general account utilisation, protection issues and some procedural issues on ISIM. As most of the organisations have been working with sensitive data, they have faced some challenges of information security threats emanating from various attack vectors.

4.8. Validity and Reliability of the Data

The *credibility* of the data was accomplished by applying the following techniques: protracted engagement, crosschecking, peer debriefing and member checking. Peer debriefing was accomplished by presenting the data and analysis to the secondary researcher (i.e., the supervisor) for cross checking. This also involved examining the data collection methods for content and face validity. Multiple sources of evidence were considered in the study such as information security procedures, policies, standards, and participant interviews. Transcripts of the interview notes was dispatched to the respondents for validation.

Dependability was realised by maintaining a list of data records, originally in paper format (manual), and subsequently transcribed into a digital format. This criterion was also fulfilled by the utilisation of multiple sources of information. The study involved occasionally utilising data collectors during data gathering to eliminate biasness thus maintaining impartiality. The items of the research instruments were systematically associated with existing standards and extant literature for standardisation.

Table 4-15 shows the validity and reliability mechanisms with techniques and evidence of compliance that were applied in the study.

Table 4-15: Evidence of Validity and Reliability Measures

Criteria	**Technique proposed to improve Validity and Reliability**	**Evidence of compliance**
Credibility	-Protracted engagement -Peer debriefing -Member checking	-The engagement included semi-structured interviews: ▪ quotations from all participants (Section 4.7.1). ▪ quotations from end-users (Section 4.7.2). -Peer debriefing was attained through data submission, tools, and analysis to the secondary researcher for cross checking (i.e., the supervisor). -Member checking was achieved by cross-checking the responses of the participants regarding their input.
Dependability	-Maintaining an audit trail -Triangulation -Systematic association	-Dependability was attained by keeping a catalogue of data records, originally in paper format (manual) and later transcribed into digital format. (See Appendix A & G) -The study was dependent on multiple sources of evidenced data to enhance validity (i.e., document analysis and participant interviews). -The dependability of the research instruments was ensured by systematically associating the items with extant standards and literature for standardisation (See Section 3.6.3).
Transferability	-Thick descriptions -Document analysis	-Transferability was attained through 'thick description' by gaining richer inferences of the information security landscape by means of document analysis and acquiring background information on policies. Thick descriptions (i.e., detailed accounts) of the context and the organisations were provided in Sections 4.2 and 4.4. The methodology was also clearly expressed in Chapter 3. The researcher detailed the process of data collection, data analysis, and interpretation of the data in this chapter
Confirmability	-Data verification by a third party -Confirmation from participants	-Transcripts of the interview notes were distributed to participants for confirmation. -The impartiality of the study was ensured through deployment of research assistants and data collectors to reduce bias.

Transferability was attained through appropriate methodological utilisation in all the processes of the research procedures. It applies contextual data and information to infer data from the organisations.

Confirmability infers maintaining impartiality and independence. The impartiality of the study was maintained by utilising data collectors to avoid bias. The researcher and research assistant systematically coded and analysed the data in order to keep neutrality and eliminate bias in the study. Moreover, participants were informed about their anonymity in order to get rich data without identifying their personal data, thus maintaining the authenticity of the data collected.

4.9. Ethical Procedures

The confidentiality of the participants was preserved by ensuring that no personally identifying information was requested during the interviews. In doing so, the respondents were requested to sign a consent form before the data collection. The consent form and the questionnaire were completed separately thus ensuring the confidentiality of the participants. Moreover, all respondents were notified that their responses would be used for the research purposes. Their details were not linked to their responses. The respondents were allowed to withdraw from the study without any penalty. No incentives were provided.

4.10. Discussion

Some of the challenges explored in this research correlated with similar studies conducted in other contextual settings. ISIM in organisations is confronted with various challenges such as lack of managerial commitment, disjointed efforts and lack of documentation of information security incidents (Jaatun et al., 2009; Line & Albrechtsen, 2016; Werlinger et al., 2010). With respect to research question **RQ-1** (*"To what extent are strategies for awareness and communication efforts integrated into organisational ISIM practices?*"), the findings indicate that the coordination of awareness and communication efforts are largely unstructured and unorganised and are stalled by limited managerial commitment and planning, however, there was an effort towards incorporating ISIM procedures in policy documents. These findings were comparable to the study by Yohannes et al. (2019). The requirement for effective communication of information security incidents is critical to enhancing the reporting of incidents in organisations (Knight & Nurse, 2020) which may assist in managing future incidents.

With respect to **RQ-2** (*"How do organisations integrate communication and awareness efforts into their ISIM processes and practices?"*), the lack of reporting mechanisms within the studied organisations reflect the low advancement of ISIM processes from a communication and awareness standpoint. Werlinger et al. (2010) established that organisations do not practice working in collaboration with stakeholders particularly with end-users with respect to communicating information security incidents. According to a case study in the banking sector in Ethiopia, the findings suggest that reporting or communicating information security incidents within organisations are limited (Yohannes et al., 2019). Moreover, Adane (2020), argued that the lack of awareness and reporting mechanisms in ISIM are core challenges within organisations, which is reflected in the findings of this research. Ahmad et al., (2012) and Khando et al., (2021) strongly stress the significance of all users sharing an information security incident awareness context. Information security incident reporting processes also play a significant role in ensuring proactive and immediate information sharing (Kossakowski, Allen, Alberts ,Cohen & Ford, 1999; Werlinger et al., 2010), which is one of the challenges identified in this research.

The significance of collaboration between internal and external stakeholders concerning incident reporting was also emphasised by previous studies (Hove et al., 2014). Nevertheless, as reported by Line et al. (2016) and Tøndel et al. (2014), the coordination or participation of users in organisations for shared incident reporting remains a significant challenge. The reflections of these findings are comparable to this study. With respect to **RQ-3** *("To what extent is the integration of stakeholders' and end-users' participation instigated within the processes of incident awareness and communication efforts within ISIM practices?"*), it was found that although the contribution of end-users in the ISIM process is deemed as important, the practical reality revealed that their involvement was limited. The engagement of end-users in the process of ISIM was largely discounted. Thus, most end-users have a limited understanding towards the reporting and processes of ISIM. However, it is possible to minimise the severity and magnitude of information security incidents through the engagement of end-users. Padayachee and Worku (2020) advocate the engagement of end-users in the processes of ISIM for two reasons. First, the incidents that occur via accidental and malicious end-users (i.e., insiders) can be circumvented, as ignorance will no longer be an excuse for maleficence. Second, end-users that can detect and communicate an incident more proficiently will be able to assist in reducing the severity of the incident.

The ISIM processes is a comparatively emergent concept for most organisations in Ethiopia. The organisations are characterised by inadequate ISIM policy guidelines and limited stakeholder participation, with a prominence on incident response instead of an initiative-taking strategy for incident protection. This indicates that organisations in Ethiopia are largely vulnerable to information security incidents. The majority of the organisations in the study highlighted general information security vulnerabilities and the technical information security installation of equipment, thus discounting the human-centric nature of ISIM. Organisations should strike a balance between prevention and response in order to combat information security incidents both retroactively and proactively (Baskerville et al., 2014). The absence of formal employee partnerships and plans in ISIM processes, could potentially also exacerbate the threat to organisations (Tøndel et al., 2014; Werlinger et al., 2010). Thus, it is clear that organisations must incorporate proactive planning, resource distribution and formal employee participation in all phases of ISIM (Ab Rahman and Choo, 2015).

4.11. Implications of the Findings for a New Conceptual Model

The findings of the study have advocated there is a need for a socio-technical solution to resolve the problem articulated in Section 4.10. The findings suggest exceptionally low integration of information security standards, fragmented information security communication efforts and lack of managerial commitment for information security incident mobilisation. These findings have a direct implication for a conceptual model to address the problems found. The findings of the exploratory study established poor communication and awareness as the core problem and call for a solution space in order to reason and address these issues. Thus, according to the findings, the culture of sharing and working in a coordinated means to report information security incidents is poor. Consequently, it can be justified that ISIM warrants a reconceptualisation of communication and awareness efforts into a collaborative, comprehensive and coordinated process. Recently, skilled ISIRTs have tended to adopt a proactive approach to detecting security threats before an incident happens (Ahmad et al., 2021). Thus, the advancement of a systematic approach to address the fragmented process of communication and awareness formation in ISIM will aid in the reactiveness entreated by ISIRTs in mitigating information security incidents. In response to the lack of coordinated and standardised mechanisms to enhance awareness formation and communication protocols in ISIM, this study proposed a conceptual model that will be based on a shared mental model of an information security incident scenario leveraging the concepts of shared situational awareness and the Interactive Model of Communication (IMC). This conceptual model will be discussed further in Chapter 5.

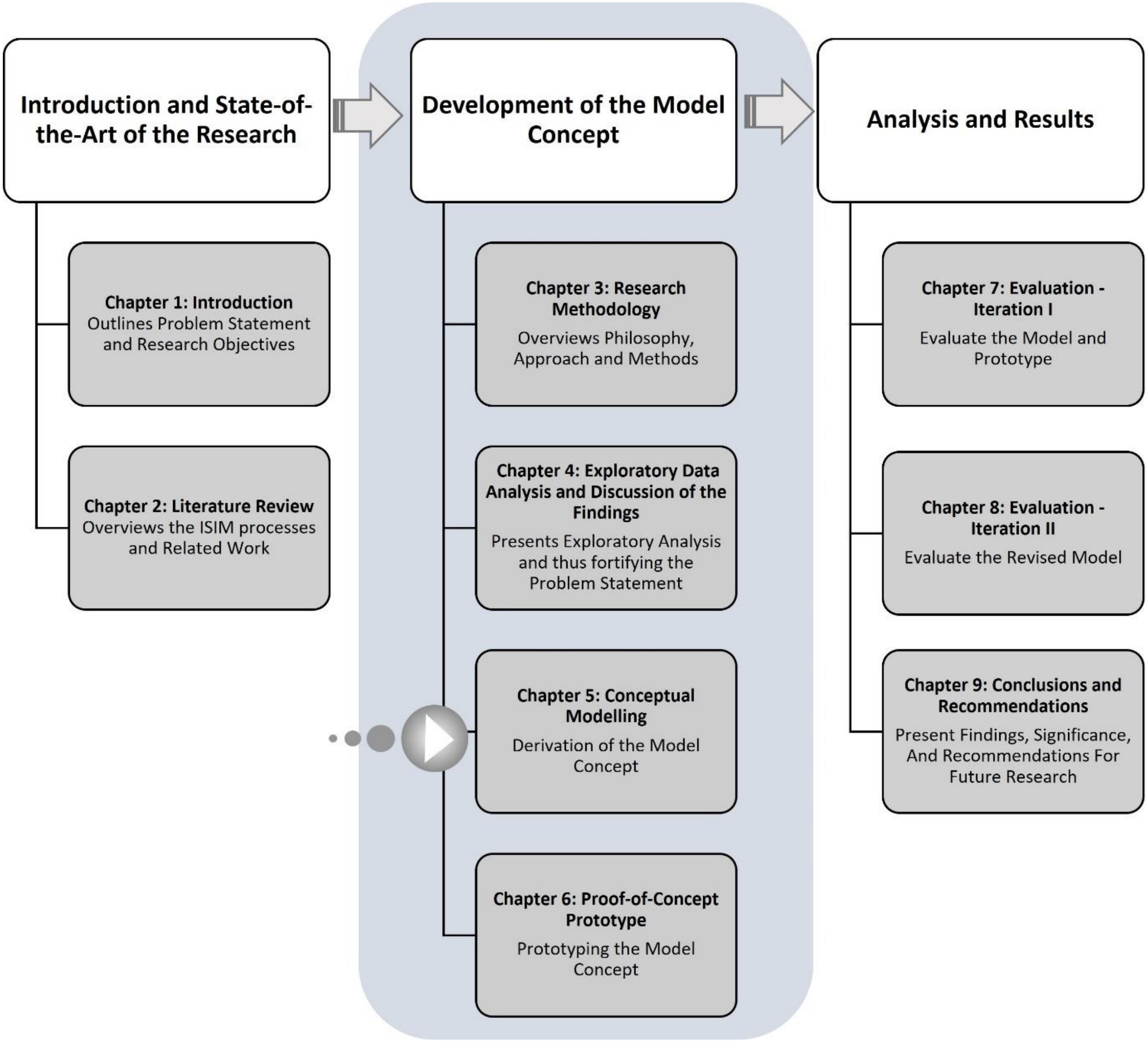
4.12. Chapter Summary

This chapter demonstrated the data analysis with respect to the exploratory study which is a component of Phase I of the study. Adequate data was collected from various respondents (information security experts and end-users) in the purposively selected organisations. The data shows a lack of collaboration, lack of communication and awareness appraisal systems in the organisations studied. Moreover, the participation of all users in organisations was limited to information security incidents and policy issues. In addition, the lack of integration and the lack of digital systems for incident communication were explored as being the main challenges in the studied organisations. The exploratory study assisted in confirming the literature and the basis for the problem statement.

The ensuing chapter, Chapter 5, will demonstrate the conceptual framework of the model for the study. The model exemplifies the core problems of the research study from various appropriate theoretical concepts and methods. Specifically, the model is intended to enhance the processes of ISIM leveraging the concepts of shared situational awareness and IMC in a coordinated manner.

CHAPTER FIVE:

RESEARCH ROADMAP



Introduction and State-of-the-Art of the Research

Chapter 1: Introduction
Outlines Problem Statement and Research Objectives

Chapter 2: Literature Review
Overviews the ISIM processes and Related Work

Development of the Model Concept

Chapter 3: Research Methodology
Overviews Philosophy, Approach and Methods

Chapter 4: Exploratory Data Analysis and Discussion of the Findings
Presents Exploratory Analysis and thus fortifying the Problem Statement

Chapter 5: Conceptual Modelling
Derivation of the Model Concept

Chapter 6: Proof-of-Concept Prototype
Prototyping the Model Concept

Analysis and Results

Chapter 7: Evaluation - Iteration I
Evaluate the Model and Prototype

Chapter 8: Evaluation - Iteration II
Evaluate the Revised Model

Chapter 9: Conclusions and Recommendations
Present Findings, Significance, And Recommendations For Future Research

CHAPTER 5: CONCEPTUAL MODELLING

5.1. Introduction

In Chapter 4, the exploratory study results were presented. The findings identified two key problems in information security incident management (ISIM) – poor awareness and communication efforts. These crucial challenges adversely affect the reporting of incidents and the coordinated power of users and stakeholders acting collaboratively and therefore present a risk to organisations. The scope of the problem identified undergirds the conceptual model proposed by this research undertaking and is espoused in this chapter (Section 5.2). The aim of this chapter is to theoretically respond to **RQ4** (i.e., "*How can organisations enhance the coordination of awareness and communication efforts in the process of information security incident management practices?"*). At this juncture, it is important to note that the exploratory study did not provide a solution to the problem identified but rather established that the processes of ISIM should be supported with mechanisms that enhance collaboration. Thus, the exploratory study amplified the problem statement. This chapter derives the model designated – A **C**oordinated **C**ommunication and **A**wareness approach towards enhancing **I**nformation **S**ecurity **I**ncident **M**anagement (**CCA$^{\mathbf{ISIM}}$**) – in Section 5.5 leveraging the concepts underpinning the situational awareness model and the Interactive Model of Communication (IMC). This study applied ISO/IECT 27035 which is a good starting point for organisations for handling ISIM (Tøndel et al., 2014). The applicability of the situational awareness model towards the IMC is discussed in Section 5.3 and Section 5.4 respectively. Section 5.5 explores the theoretical framing that underpins the conceptual model. A synopsis of the model is presented in Section 5.6. The closing section considers the limitations of the model (Section 5.7), the contribution of the model (Section 5.8) and the concluding remarks (Section 5.9).

5.2. Identification and Scope of the Problem

As discussed, in Section 2.2 and Section 2.7 (Chapter Two), the preliminary investigation showed that both the lack of collaboration and poor reporting of incidents are of concern to organisations. This was further confirmed by the exploratory study (Chapter 4). It is evident that it is challenging to achieve proactive ISIM without proper communication and awareness formation in organisations. Such uncoordinated approaches have been attributed to the absence of managerial commitment, lack of collaboration, the lack of appropriate systems in managing in incidents and lack of documentation which is supported by the findings of this study (Section 4.7).

The lack of collaboration and poor reporting of incident information minimises awareness and communication channels. Effective communication in ISIM processes (i.e., plan, detect, analyse, respond and lessons learnt) can play a substantial role in sharing incident information in a collaborative and coordinated approach. From the exploratory study, it was identified that the lack of appropriate reporting structures in organisations led to poor communication during an incident reporting scenario (Section 4.7.1).

Figure 5-1 shows the general demonstration of the problems of ISIM and a possible solution.

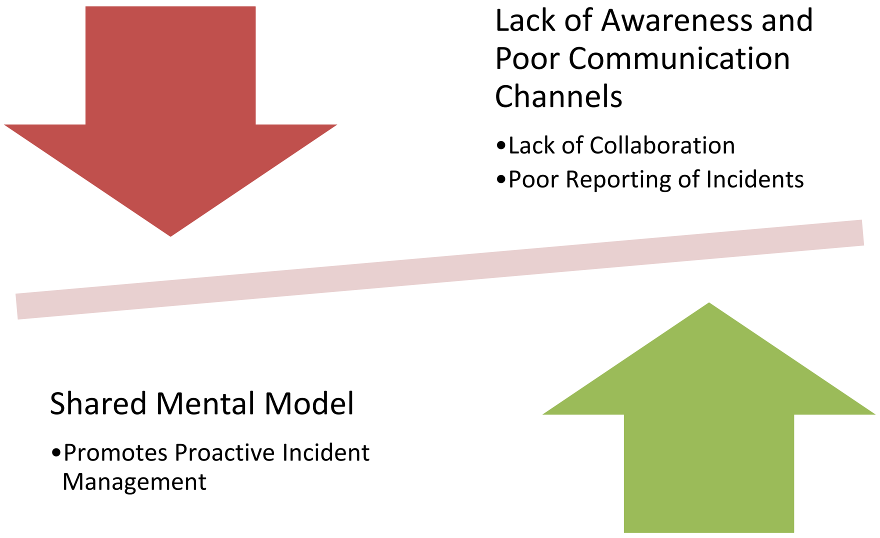

Lack of Awareness and Poor Communication Channels
•Lack of Collaboration
•Poor Reporting of Incidents
Shared Mental Model
•Promotes Proactive Incident Management

Figure 5-1: Identification and Scope of the Problem

Effective communication skills, collaborative learning, and coordinated mechanisms are particularly important for users in exchanging vast quantities of information of any kind in an organisational context (Leu & Kinzer, 2000). The greater the extent of communication flowing within an organisation, the better the levels of knowledge and awareness of security incident information is sustained (Hove & Tarnes, 2013). Indirectly, if users can get up-to-date information about incident information, this will reduce the probability of the breach occurring again (Knight & Nurse, 2020). In addition, users will have more awareness regarding existing security breaches and will be able to react more decisively if a similar incident arises.

This problem domain of awareness creation is fraught with difficulties as it crosscuts the technical and sociological domain. Studies related to information security awareness recommend training programmes for awareness formation among users (Hove et al., 2014; Tøndel et al., 2014; Yohannes et al., 2019). Grounded on the problems that originated from the exploratory study, a socio-technical solution could be useful in coordinating the efforts of awareness and communication. ISIM could benefit from socio-technical solutions to proactively minimise information security incident challenges in organisations (Werlinger et al., 2010). Sarker et al. (2013) identified socio-technical factors such as behavioural, organisational, communication and management issues as core factors for ISIM, which need to be addressed. Thus, in addressing this problem, the study considered a theoretical concept from social psychology that may offer a possible solution, which is a shared mental model. According to Jonker et al. (2011 p. 132), a shared mental model is defined as follows:

> *"Shared mental model theory as developed in social psychology, can be used as an inspiration for the development of techniques for improving team work in (human-) agent teams. Thus, it helps to improve team performance if team members have a shared understanding of the task that is to be performed and of the involved team work."*

Converse et al. (1993) contended that a shared mental model can help teams to collaborate effectively in decision making. Broadly speaking, a shared mental model which promotes a proactive ISIM approach is a possible resolution to the problems identified. A mental model can assist in problem-solving and it represents the knowledge of how various components affect other components and how components will act under the influence of numerous factors and stimuli (Floodeen et al., 2013).

Studies show that knowledge structure, team model and conducted cognitive tasks enhance the effectiveness of the team and that advanced analysts depend on prevailing mental models to map out threats and recognise gaps to better understand the operational picture (Chen et al., 2014; Maynard & Gilson, 2014). Entin and Entin (2000) concluded that mental models enable awareness creation, and the congruence and accuracy of these models can influence the level of situational awareness of teams. Floodeen et al. (2013) recommended the application of a shared mental model in security incident ticketing systems to enhance the efforts of communication. However, they did not validate the process of a shared mental model; they sensed that this could be the unaccounted component of the information in the incident ticketing system required by many experts and technicians.

However, mental models are difficult to define and Endsley (2001) points out that those mental models are more generic whereas a situational awareness model incorporates the system's parameters and the understanding of the dynamics, and provides a useful window on a generic mental model. Furthermore, a situational awareness model is a "current instantiation" of the mental model. Scarfone et al. (2008) proffered that in order to sustain situational awareness in incident management, the processes of preparation, documentation and the assignment of roles and responsibilities are critical issues. Situational awareness involves the informed and sensible dynamic contribution and reflection by an individual on a certain situation that provides a dynamic context to reflect on the past, present and potential future features of an incident (Stanton et al., 2001). The reflection dynamic can be constituted with conceptual-logical, ingenious, aware and unconscious elements which support activities of individuals to exercise mental models (Bendy et al., 1999). In the next section, the applicability of situational awareness to ISIM is considered.

5.3. Applicability of Situational Awareness to ISIM

Situational awareness reinforces further knowledge of "numerous pieces of data", as it demands an "advanced level of understanding a situation" and "a projection of future system states" (Endsley, 1995). Situational awareness considers the perception of a given situation, comprehension of its characteristics and projection of its status in the future (Endsley, 1988) which entails users' capability to instantly understand a situation, infer and decide based on better informed situations. Figure 5-2 demonstrates the levels of application of situational awareness to ISIM.

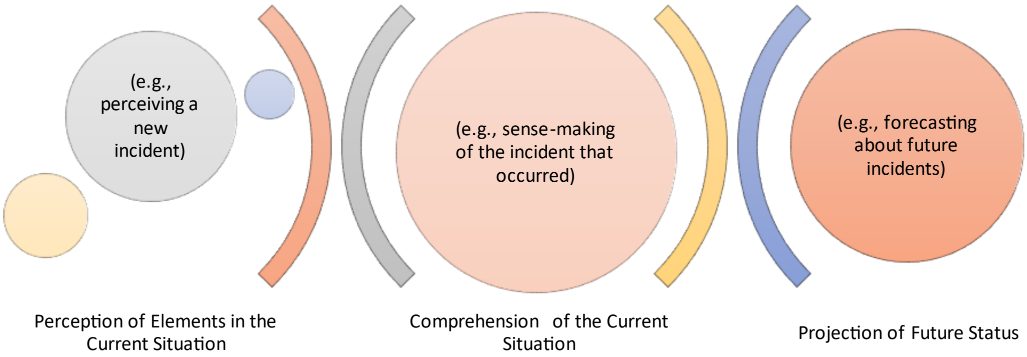

(e.g., perceiving a new incident)
(e.g., sense-making of the incident that occurred)
(e.g., forecasting about future incidents)
Perception of Elements in the Current Situation
Comprehension of the Current Situation
Projection of Future Status

Figure 5-2: Levels of Situational Awareness (from Endsley (1995)) redefined to encompass ISIM

The concepts of 'perception', 'comprehension', and 'projection' can be considered to symbolise progressively developing levels of awareness ranging from (i) basic perception of data, (ii) combination and interpretation of data, and (iii) aptitude to predict future events and their implications (Bendy et al., 1999; Franke & Brynielsson, 2014; Stanton et al., 2001). The situational awareness model is highly suited to organisational processes. The practice of situational awareness for incident response is lower in organisations which indicates the need for further empirical studies from the process perspective (Ahmad et al., 2021; O'Brien et al., 2020). In this regard, Webb et al., (2014) emphasised the importance of situational awareness to information security and risk management which have common problems with ISIM – (1) risk identification of information is perfunctory; (2) information security risks are projected without a consideration of situational awareness; (3) security risk evaluations are conducted irregularly without the consideration of previous data. The application of situational awareness is also extraordinarily complex and needs to consider other factors such as individual, team and environmental issues (Bolstad & Gonzalez, 2004).

In a previous study conducted by Line and Albrechtsen (2016), the application of situational adaption to ISIM was considered from an industrial perspective from theory as a management element for industrial safety. An analysis of incident data from organisational collaborative practices linked situational awareness to design and policy implications (Riebe et al., 2021). Section 2.3 of Chapter Two explored a study to develop a toolset for cyber-incident handling of decision support systems, which applied a situational awareness model within the OODA (Observe, Orient, Decide, Act) loop, however, the process was automated without human involvement (Husák et al., 2022). Situational awareness was also applied in sharing information for critical infrastructures to support decision making through operational and technical means (Pöyhönen et al., 2019). The model developed by Padayachee and Worku (2020) exemplified that the process of ISIM could progress from individual situational awareness to shared situational awareness thereby enhancing the collaborative power and responsiveness in the process. Nevertheless, the model does not accommodate the communication channels. Linderoth et al. (2015) who studied situational awareness within health care emergencies, which shares some parallels with incident response, revealed that communication, situational awareness, and attitude were the major problems and they specified that effective communication mechanisms are critical to obtaining acceptable and congruent situational awareness. The processes of information security incident planning, identification and communication are vital steps in ISIM processes, followed by assessment, response, decision and lessons learnt (Humphreys, 2008). Thus, communication pathways are a focal element within every phase in information security incident response (ISO/IEC, 2016; Tøndel, Line, & Jaatun, 2014).

Extant literature demonstrated the application of situational awareness within the context of information security and emphasised the key role of team work at every step of cyber security for a coordinated effect of situational awareness processes for improved response (Husák et al., 2022). While many studies relate security awareness to learning, organisations do not practically learn from earlier incidents within a real-world context and consequently neglect to implement strategic security issues (Ahmad et al., 2012). Thus, the application of the situational awareness model in information technology and other disciplines has been emphasised and used in a variety of contexts (Webb, Ahmad, Maynard, & Shanks, 2014). Although Yang, Byers, Holsopple, Argauer, and Fava (2008) considered the concept of projection from Intrusion Detection Systems (IDS), in the study at hand, the proposed model also considers a user-centred perspective in which it uses existing data directly obtained from the user to analyse, compare, decide and project incidents. The existing incident information from the previous steps (perceiving and comprehension) will serve as a mechanism to project the possibility and occurrence of incidents with detailed information about the previous incident.

Situational awareness has a significant role in understanding, perceiving, and projecting of imminent incidents to proactively address risks and vulnerabilities. Consistent with Barford et al., (2010), there are seven elements of situational awareness that is applicable to ISIM which were also promoted by Padayachee and Worku (2017). The seven aspects of situational awareness that could be used to support ISIM are listed as follows:

(i) Awareness of the existing situation which includes situation sensing (recognising that an incident attack is happening) and detection (i.e., type of attack), the source (who, what) and potential attack target.

(ii) Awareness of the attack impact (assessment and analysing vulnerability) which includes the existing impact and successive assessment.

(iii) Tracking the existing situation.

(iv) Adversary's behaviour awareness, patterns, intent, and trend analysis.

(v) Understanding why and how the current situation is occurring.

(vi) Understanding of the reliability of the gathered incident situation information.

(vii) Predicting future actions away from the adversary and limiting the adversary in the future, whereby the control involves knowing the motive, prospect, and ability.

However, a multi-actor engagement such as ISIM requires more than individual situational awareness; it requires shared situational awareness. According to Endsley (2001, p. 3), shared situational awareness is defined as "the degree to which team members possess the same SA (situational awareness) on shared SA (situational awareness) requirements". Shared situational awareness which is apt to organisational situations refers to "the degree of accuracy by which one's perception of his current environment mirrors reality and a number of individuals trying to create a common picture" (Nofi, 2000, p. 4). According to Kurapati et al. (2012, p. 48), research on shared situational awareness has "not dealt enough with the multi-stakeholder networks or organisations". Nofi (2000) proposes building shared situational awareness based on the following criteria. Initially, consider the individual's situational awareness within the structure of what needs to be undertaken. Secondly, form roles for other members of the organisation to properly share their mental models (awareness) using a given communication procedure. Thirdly, incorporate numerous individual mental models of the situation to produce a mutual understanding. Thus, Padayachee and Worku (2020) leveraged communication protocols of shared situational awareness, appropriating from Linderoth et al. (2015), in that their model considers communication and situational awareness to intervene as pathways for effective shared understanding.

Although there are various works on situational awareness concerning industrial control systems, IDSs and algorithms, less work is devoted to communication or information exchange (Franke & Brynielsson, 2014). The connexion of shared situational awareness relative to ISIM is illustrated in Figure 5-3.

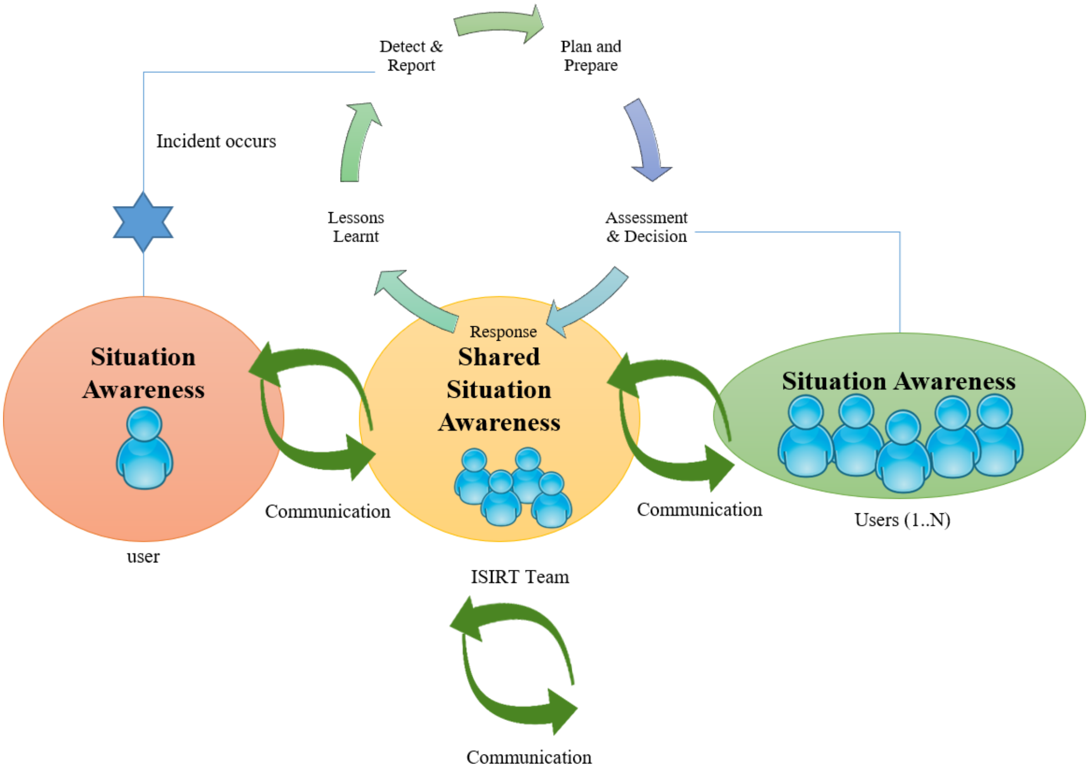


Figure 5-3: Shared Situational Awareness in ISIM (adapted from Padayachee and Worku (2020) and Linderoth et al. (2015))

In Figure 5-3, a user identifies an incident and is required to report the incident. The user reports it according to their perception about the incident (e.g., the type of incident, source of incident and potential target of the incident). The user will also attempt to ‘comprehend’ the information related to the incident from perceived and existing incidents. In addition, the user will create a ‘projection’ of the incident based on their perception and comprehension of the incident. In other words, they will forecast future incidents. The user will then *communicate* their incident report to the Information Security Incident Response Team (ISIRT) who will analyse and interpret the incident report. By applying the existing information and further tools (e.g., vulnerability analysis and impact assessment) and their perceptions and comprehension of the current situation, the ISIRT teams will also make a projection of succeeding incidents that will support the planning, preparation and lesson learning processes of ISIM. This is an internal *communication* between the team members within ISIRT. Thereafter, the ISIRT will *communicate* the assessments, responses and decisions made to the wider community in the system, thereby increasing the participation of all stakeholders. The framing shows that incident communication is possible among users thereby supporting a shared understanding of an information security incident.

While the application of situational awareness is useful in multi-actor contexts, the integration of communication mechanisms has been considered a critical factor in enhancing situational awareness in an interactive manner (Bolstad et al., 2004). The next subsections explore the coordination of communication efforts in tandem with situational awareness to address the key challenges identified by the exploratory study.

5.4. Applicability of Communication Protocols to ISIM

Communication “denotes various components such as a sender, a message, a channel, a receiver, a relationship between sender and receiver, an effect, a setting in which communication happens and a spectrum of things to which the actual 'messages' refer” (McQuail & Windahl, 2015, p. 5). In general terms, three communication models exist – the linear communication model, the interactive communication model and the transactional communication model (Sellnow, 2005).

The linear model considers communication as one-directional (Foulger, 2004). That means the message is disseminated in only one direction from the sender to the receiver. In the linear model of communication, there is no possibility of getting feedback as the receiver does not have the chance to respond or send a message back to the sender. The transactional model of communication supports non-verbal signals and “noise” as communication between senders and receivers which happens concurrently, which is more suited to cultural and contextual aspects (Barnlund, 2008). The interactive model was selected for this study as it is frequently used in cyberspace where individuals can react to mass communication (Businesstopia, 2018

& British Columbia Campus, 2020). It is out of the scope of this research to incorporate societal and cultural perspectives that may impact communication.

The IMC is an advanced system as it contemplates the setting of the communication which could affect the interaction through a shared field of experience (see Figure 5-4). The IMC by its nature is circular where it iterates from the sender to the receiver. Schramm (1954) embodied the idea that communication is a recursive process by nature in which the communication elements (sender, message, receiver and feedback) interact in an engaging manner. In the circular model, a certain message could be encoded and decoded by the sender and the receiver in a continuous cycle that enables a two-way interchange of messages to enhance communication (Janowitz, 1961).

The IMC was selected for this study as it is mostly applied in digital and internet-based communication where people can engage and provide feedback in the communication process (Businesstopia, 2018 & UOM, 2019). The IMC highlights that communication eventually creates an impact on the receiver’s side in terms of mutual sharing of information and assessment, and it supports two-way communication (Sapienza, Iyer, & Veenstra, 2015). Thus, consistent with the core research problem and the contextual factors, the IMC was integrated within the conceptual framework as a communication protocol.

Communication models such as the IMC were utilised and are functional within the context of information communication technologies (Lovászová & Michaličková, 2016; Noskova & et. al., 2016; Moise, 2008; Velten & Arif, 2016). Nonetheless, the application of communication models within teams is considered to be very poor (Chen et al., 2014). Valecha et al. (2012) applied the Schramm’s communication model to structure the communication reports of emergency services by introducing a model for a messaging system which defines the framework of a message and standardises the message format with the intention of sharing it with other departments.

Steinke et al. (2015) indicated that the performance of cyber security incident response teams may be enhanced with team adaption, communication, problem-solving, trust and shared knowledge. Effective communication is crucial, specifically during handoffs, during the response process. They go on to state that there are few directions to improving the communication process, except for checklists and mnemonics.

The fundamental reason in applying a communication model, particularly the IMC, (see Figure 5-4) is to improve the communication of information security incidents, practices and events in a collaborative approach. The model aims to demonstrate the interchange of information and messages that take place from sender to receiver and vice versa (Schramm, 1954). The IMC considers the communicators' fields of experience. The more their field of experience matches, the greater the shared interaction between the communicators (Wood, 2014). In IMC, "if everyone were to have the same experiences, all messages would be encoded, transmitted, and decoded alike" (Jossey, 1999, p. 2).

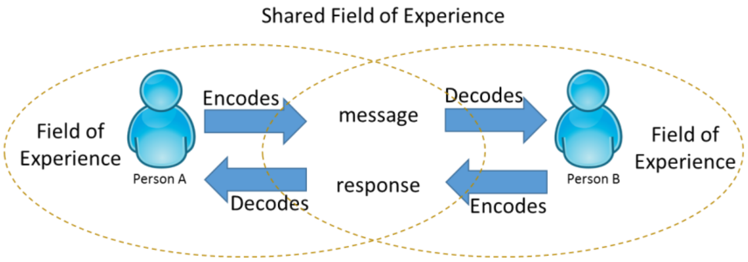


Figure 5-4: Interactive Model of Communication (adapted from Schramm, (1954))

Effective utilisation of the IMC model in ISIM is also dependent on the communication skills and technical capabilities of both the sender and the receiver and it is referred to as the 'field of experience'. There could also be hindrances to communication such as the physical, process, semantic and psychosocial barriers (Lunenburg, 2010). The model supports and eases exchange of information and management of incidents among stakeholders regarding encountered events, which can possibly answer the "What", "When" and "Who" aspects of an incident.

Users in organisations prefer to engage and report their routine operations using interactive or digital means of communication rather than conventional ways of communication (Nordby, 2011). The application of the IMC model in organisations for information security can also best fit the problem raised because IMC deals with sharing of experience and organisations are converging towards digital communication (Padayachee & Worku, 2020). The IMC model also enables users to iteratively share their experiences which enhances shared awareness among users (Lumen Learning, 2016).

In this study, the model encompasses the communication of incident information from one sender (user) to another (receiver) which will be encoded and stored in the system. Then, ISIRT will assess, evaluate, and disseminate the incident information. To support this interactive communication, various parties within the system may have diverse requirements regarding incident information and they may use the incident information according to their specific concern. Thus, the specialised requirements of incident information should be managed through distinct roles in their tasks at the organisation. Applying a role-based access control for incident information is especially important both in access and maintaining the functionality of the ISIM processes. Therefore, this study also considers using role-based access control to filter incident information as a tier within the model. As the applicability of the concepts underpinning the model, that is, situational awareness, IMC and the role-based access control mechanism to incident information was unpacked in the preceding sections, the next section is primed to present the derivation of the conceptual model.

5.5. Derivation of the Conceptual Model

As there are few descriptions of shared situational awareness for organisations, this model considered representations from other contexts (Kurapati et al., 2013a, 2013b). However, these representations were based on disruptions in supply chain management, while in a previous publication, Padayachee and Worku (2017) leveraged depictions of situational awareness from Kurapati et al. (2013b). However, the work by Padayachee and Worku (2020) was merely a proposal; therefore, this research aims to ground the model presented here considering the practical implications concerning an information system intended to address a problem in information security. In this section the individual situational awareness, shared situational awareness and role-based awareness will be considered. The subcomponents of perception, comprehension and projection are now reviewed relative to individual situational awareness.

5.5.1. Individual Situational Awareness Tier

According to the ISO/IEC 27035 (2016) standard, the first phase in ISIM is detection which involves the gathering of information related with the incident and reporting on the existences of information security events and information security vulnerabilities through a human or by automated means. Encouraging individual situational awareness is vital, as security awareness enhancement among users enables proactive incident handling skills (Bendy et al., 1999). In cyber situational awareness, individuals may not have all the access to all the information within the shared environment (Husák et al., 2020).

Perception

From an information security perspective, perception involves knowing the elements in an information system such as being perceptive to the alerts from an IDS including knowing how to report the incident (D'Amico & Kocka, 2005). Perception is the ability of a person or a vigorous process whereby individuals detect relevant signals from their environment (Bolstad et al., 2004, Dominguez, 1994). Webb et al. (2014) described the phases of collection, processing, and exploitation from risk analysis as analogues to Perception. They describe collection and process as appearing concurrently which is gathering element state data where the perception is enhanced after machine processing. The process of information security incident detection can be triggered either through manual or automatic means (Metzger, Hommel, & Reiser, 2011). An individual’s information security perception is affected by their technical or formal risk assessment (Line, Tøndel, & Jaatun, 2016) which is also associated with incident detection and reporting. Some of the parameters related to perception include (Lu & Kokar, 2015):

- Indicate the number and status of the incident: this helps users to specify and characterise the incident type, name, and different status of the incident that they perceive at the initial stage.
- Describe why a certain incident happens frequently: at perception level, users assess and analyse why a certain incident happens for a given period.

Comprehension

Comprehension is when individuals use their internal heuristics to understand, correlate, aggregate and compile what and how the cause of the incident happened from existing incident data (Lu & Kokar, 2015). From an information security perspective, comprehension involves determining which alerts are essential and which are not, and being able to discern the significance of an incident (D'Amico & Kocka, 2005). This describes the ability to inquire, filter and understand existing security concerns. Yufik (2014) argued the importance of comprehension with respect to human cognition for the purpose of inference and understanding. Within the context of situational awareness, this model proposed here incorporated the elements of correlation, and triangulation as part of understanding incident information. The elements are incorporated as they enhance the comprehension process of understanding incident information.

To attain comprehension of an incident, analysis, documentation, classification and prioritisation are key functions of the detection and assessment phase of ISIM (Tøndel, Line, & Jaatun, 2014; Cichonski et. al, 2012). Bolstad, Cuevas, Costello, and Rousey (2005) also applied situational awareness to the recovery of personnel in a military setting. Appropriating from their study, it is possible to infer and request information related to the comprehension of an incident which was revised to the context of ISIM such as (Yufik, 2014):

- What is the risk level regarding the incident (high threat, medium threat, or low threat) to the organisation?
- Determine the severity of the incident.

The incident category in terms of severity can range from a simple alarm to critical or to an emergency (ISO/IEC, 2016). Categorisation, compilation and grouping of similar incidents into clusters are important for further analysis within the ISIM processes of detection, analysis and response (Cichonski et. al, 2012). Thus, comprehension deals with the synthesis, inference and association issues of previously detected incidents (Bolstad et al., 2004; Lu & Kokar, 2015). As the comprehension process is related to the analysis and grouping of incidents (Yufik, 2014) it is further posited that the collective understanding of an incident can be improved with the processes of search, query, analyse, and triangulation. The following points discuss how the comprehension component can be supported:

- **Correlation:** This is the process of linking current incident information to previous incidents. Here the user can infer incident information by correlating the current incident with similar incidents. This implies that there must be a repository of similar incidents with their facets (damage caused, precautions etc.) available for the user to query.

- **Triangulation**: This process considers other incident categories from other sources to enhance situational awareness comprehension. Webb et al. (2014) related the concept of comprehension to drawing on multiple specialists to comprehend a state.

The analysis of an incident involves interlinking, classification and determining the status of previously detected incidents (Cichonski et. al., 2012). The process of situational awareness comprehension could be enhanced by applying those techniques to the incident assessment and decision phase of the ISIM process (Webb, Ahmad, Maynard, & Shanks, 2014).

Projection

Individual situational awareness involves projection in which users or individuals use their internal heuristics to understand and infer the causes and the patterns of incidents that occurred in their organisation (Bolstad et al., 2004; Franke & Brynielsson, 2014). Also, the process of projection, as indicated by Husák et al., (2020), is the capability to infer an upcoming forecast based on the data, information and knowledge extracted from the dynamics of the network components and comprehension of an incident situation (Yang et al., 2008). From an ISIM perspective, projection involves inferring the existing situation and predicting about a probable future incident (D'Amico & Kocka, 2005).

Bolstad et al. (2005) applied situational awareness related to the recovery of personnel in a military setting. The following questions (parameters) are related to collecting information concerning the projection of the incident which was revised to the context of ISIM:

- What could be the suspected incident from the previous incident pattern?
- How do you proactively prepare and plan for incidents before an incident occurs?

The following processes are involved during Individual Situational Awareness:

- Register incident: by user and ISIRT [during the Perception stage]
- ▪ Correlate incidents [to enhance Comprehension]
- ▪ Triangulate incidents [to enhance Comprehension]
- ▪ Project future incidents.

As organisations involve the collaboration of multiple users for information sharing, awareness cannot be done exclusively at an individual level, and the following section considers the integration of shared situational awareness into the model concept.

5.5.2. Shared Situational Awareness Tier

The process of shared situational awareness is a continuum from an individual level to a group level (Endsley, 1995). Individual stakeholders include end-users, managers, clerical staff and expert users. Consequently, in the shared situational awareness tier, all stakeholders (i.e., managers, end-users, etc.) including the ISIRT have their role in the process of mutual understanding with respect to incidents. Salmon et al. (2008) describe the difference between team situational awareness and shared situational awareness. They clarify that team situational awareness considers the interaction of the team through collaboration, communication, coordination between individual situational awareness, and shared situational awareness amid team members and the mutual situational awareness of the entire team, whereas shared situational awareness is the intersection in situational awareness elements between team members.

Endsley (1990) recommends that, during team tasks, situational awareness involves the correspondence between team members, in that individual team members are required to perceive, comprehend and project components that are specifically associated to their specific role in the team, but also to consider components that are needed by themselves and other team members. Effective team performance, thus, requires that individual team members have situational awareness of their particular elements and also shared awareness to develop a shared understanding and communication, and are able to work in teams among groups (Steinke et al., 2015).

Bolstad and Endsley (2000, p. 1) assert that shared situational awareness in collaborative decision-making tasks includes four factors:

- **Shared Situational Awareness Requirements**– “the extent to which members of the team understand which information is required by other members of the team”.
- **Shared Situational Awareness Devices** – “shared displays and environment, including communications”.

- **Shared Situational Awareness Mechanisms** – The use of shared mental models (this can be achieved through sense-making).
- **Shared Situational Awareness Processes**– “involvement of effective team processes for sharing pertinent information”.

Bolstad and Endsley (2000) indicate that shared situational awareness is achieved through various tools – shared displays, shared communication, and shared environments. The shared situational awareness requirements and shared situational awareness devices will be achieved by visualisation, sense-making and communication channels which help to understand the requirements of each team member and act as devices towards shared communication. The shared situational awareness mechanism will leverage sense-making to achieve a shared mental model. Shared situational awareness processes will be achieved by the role-based situational awareness component of the model which aims to share relevant information to the team members according to roles. The next sub-section explores the two core elements of the shared situational awareness tier, which are sense-making and visualisation.

5.5.2.1 Sense-making

There are various approaches to sense making or sense-making, hence the variations in spelling – sense-making was introduced by Dervin (1998) whereas sense making was introduced by (Weick, 1995). However, recent applications have merged the ideas together (Urquhart et al., 2016). For the sake of readability the spelling variant of “sense-making” will be used in this thesis. Weick (1995) introduced sense-making for organisational contexts, while the approach of Dervin (1998) to sense-making focuses on the individual as it makes sense of a ‘gap’ within a situation. Marshall (2016) frames sense-making as sense giving to deliberately attempt to change how people think. Weick (1995) indicated that sense-making involves understanding, interpretation and attribution where it “involves the on-going retrospective development of plausible images that rationalize what people are doing” (Weick et al., 2005, p. 409). While the approaches to sense-making appear diverse, the ideas are complementary, in that Dervin’s approach to sense-making is achieved when crossing a gap in the information landscape while Weick’s approach to sense-making is achieved retrospectively, that is to make sense of past situations (Harviainen & Melkko, 2022).

Sense-making involves making sense of unclear situations and is related to the process of situational awareness, “where individuals and organisations can understand the multifaceted associations between people, places and events to allow them to make their own judgement of future developments and act accordingly” (Jashapara, 2004, pp. 131-132). “Sense-making is an on-going accomplishment originating from the efforts to create order and make retrospective sense of what has occurred” (van Wyk et al., 2020, p. 2).

At an individual level people who have elevated levels of situational awareness can process new data using their mental model which is an organised and dynamic knowledge structure gleaned by experience (Jashapara, 2004). Sense-making involves selecting a structure from multiple frames that best fits the context – a frame is a mental model that identifies limitations and makes forecasts (Howard et al., 2015). The outcome of sense-making is situational awareness which involves “a cyclic process between mental models and dynamic data to find the best match between the two” (Jashapara, 2004, p. 132). Figure 5-5 shows the relationship between these three concepts at an individual level.

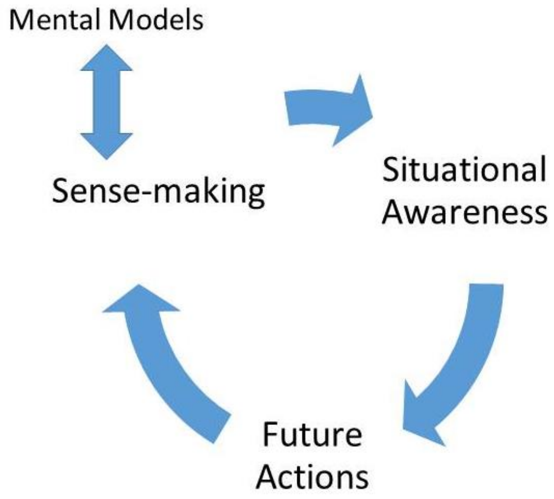


Figure 5-5: The Relationship between Mental Models, Sense-making and Situational Awareness (adapted from Jashapara (2004))

Within a shared situational awareness context, shared mental models will characterise "the intersection or conjunction among team members' mental depictions regarding various elements of their team and activity" (Maynard & Gilson, 2014, p. 8). Salas et al. (1994) pointed out that shared mental models assist in understanding the association between team processes and situational awareness and that mental models can be used as descriptive mechanisms for coordination in teams. Maynard and Gilson (2014) argue that shared mental models in research largely consider interaction, communication, and training in a face-to-face context, and there is a paucity of research on the use of information communication technology (ICT) with respect to shared mental models. Maynard and Gilson (2014) argue that ICT affects the development of shared mental models from a team and task perspective and view the attributes of technology that affect the shared mental model by applying a sense-making lens.

Appropriating from Zamani et al., (2021), this study considers the strategies proposed by Weick (1995), as this study involves the organisational context with multiple stakeholders and the aim is to make sense of the fragmented processes within ISIM. Dennis and Valacich (1999) proposed a theory of media synchronicity that posited that all tasks for group work are composed of two fundamental communication processes, *conveyance* and *convergence,* which can be used to minimise multiple and conflicting interpretations of a situation. They considered the following sense-making strategies, which were derived from Keick (1985) and Weick (2009), and which are intended to enhance sense-making in group support systems: action, triangulation, deliberation, contextualisation and affiliation.

Conveyance is a process of disseminating a diversity of information from varied sources to enable the receiver of the information to gain a mental model of the situation (Dennis et al., 2008) and it involves the following structures:

- **Contextualisation**: It refers to the "connection of the new events to past events" (Dennis & Valacich, 1999, p. 4).
- **Action**: This is the process where, "members ask questions of or propose actions, information or opinions to other group members, and await the response" (Dennis & Valacich, 1999, p. 4).
- **Triangulation**: This is the process of attaining information in a variety of formats from a variety of sources in order to obtain a complete picture (Dennis & Valacich, 1999).

Convergence is the process of reaching a common understanding of the current situation based on an individual's interpretation of the information (Dennis & Valacich, 1999) and involves the following structures:

- **Deliberation** is the process of integrating the information gained through action, triangulation, and contextualisation in order to understand the current situation (Dennis & Valacich, 1999).
- **Affiliation** considers how other individuals infer or understand information, and reach a mutually agreed upon meaning (Dennis & Valacich, 1999).

ISIM deals with various processes such as planning, detection, assessment, response and lesson learning. The above processes of sense-making can play a role in the enhancement of these ISIM processes. Conveyance can assist in transmitting information during an information security incident by combining a variety of sources using the strategies of 'contextualisation', 'action' and 'triangulation'. Convergence can assist in forming a shared mental model of incident information which supports all the processes of ISIM using the strategies of 'deliberation' and 'affiliation'. Convergence requires less deliberation when encountering new information in situations where individuals have a shared mental model, consequently encoding and decoding of existing information could be expediated (Dennis et al., 2008).

Table 5-1 considers how the strategies for sense-making could be theoretically applied to ISIM to promote shared situational awareness.

Table 5-1: The Interaction of Sense-making and ISIM

Sense-making Strategy	**Sense-making within ISIM processes**
Triangulation	Searching the incident pool of previously detected incidents.
Contextualisation	Characterisation of the incident from previous cases.
Action	Communicate incident information to stakeholders
Deliberation	ISIRT deliberates on information from the process of triangulation, contextualisation and action
Affiliation	Submitting incident information to stakeholders for feedback to ensure mutual understanding.

Visualisation has been used to enhance the usability of different interactive systems to support improved acceptance through sense-making (van Wyk et al., 2020). This is the subject of the next complementary strategy used to achieve shared situational awareness.

5.5.2.2 Visualisation

Tamassia et al. (2009) surveyed techniques of visualisation of information security using the graph drawing approach. They highlight the advantages of visualisation over textual information which is often difficult to analyse. D'Amico and Kocka (2005) indicate that visualisation is a common tool used to enhance situational awareness. A situation-awareness visualisation in information systems helps to offer “perceptually based presentations that permit decision-makers to rapidly infer the readiness of all available cyber resources” (Erbacher, 2012, p. 17). Existing models have considered visualisation from mostly an analyst’s or a decision-maker’s perspective (Erbacher, 2012).

Visualisation also enhances the users’ knowledge transfer through easy understanding between different entities (van Wyk et al., 2020). D'Amico and Kocka (2005) proposed several visualisation techniques for each level of situational awareness for information assurance. These notions are now revised within the ISIM context:

- **Perception**: Visualisation to the source IP address and its relation to other IP addresses amongst millions of transactions per day to show that the stakeholders visually see the relationship of this source address to other destination IP addresses and transactions.
- **Comprehension**: A visualisation of the links “between various entities” and an animation showing the path of the incident. For example, a path is taken by either an external or insider attacker to “gain insight into the attacker’s activities”.
- **Projection**: A visualisation that replays the visual representation and aims to determine the next entity that could be attacked if the attacker is not circumvented. For example, an attacker who gains access to the employee entity can therefore use this information to gain access to the client entity.

Although visualisation of Big Data was studied from different perspectives such as situational awareness (Jonker, Langevin, Schretlen, & Canfield, 2012) and from a human cognitive analysis perspective (D’Amico & Kocka, 2005), few studies were conducted from an ISIM perspective. While Erbacher (2012) addressed incorporating visualisation in situational awareness to predict security incidents for decision-makers, the author did not incorporate an integrated communication strategy as described in the research problem and conceptual design of this research.

More importantly, in this research study, from the perspective of ISIM, the process of visualisation is to deal with mapping and querying the existing information to show summary and graphical presentations on the incident which had taken place, and the frequency and distinctive characteristics of incident information. Such information will be visualised in the prototype (Chapter 6). Mapping and inference of data are associated with the visualisation, as data inside the system can be visualised in graphical form. It involves reading from the data, synthesising, inferring and putting together similar and different incident clusters in diverse ways. Bolstad and Endsley (2000) found that while shared displays (i.e., visualisation) were useful in building shared mental models, they decreased performance due to the mental overload and proposed that perhaps abstract shared displays which only provide the "critical information" of the display to reduce the mental strain might be more useful. They found that abstracted shared displays helped in the coordination of teams in excessive workload situations when direct communication is strained.

5.5.3. Role-Based Situational Awareness Tier

The concept of differentiated roles (individual, institutional and external) in organisations is important to enhance information security awareness in organisations (Ahlan & Lubis, 2015). It has also been proved that access control, role administration and classification and the regulation of access are key factors of information security awareness for decision-makers (Diesch et al., 2020). Hence the model presented here supports a role-based communication strategy. Such custom-made information access and communication enables users to access and use incident information that is relevant to their context. Also, it enables the management and decision makers to access, retrieve and disseminate incident information according to their access level.

5.5.4. Interaction between Individual and Shared Situational Awareness

When a new incident is encountered in organisations, it is registered by either users or the ISIRT into the incident management system. The process of detection and registration of incidents can support the identification, sorting and registration of incidents that occurred in the organisation. Then it will be shared with other groups or stakeholders in a shared awareness scheme. Although all users are required to have a basic knowledge and understanding of the incident, it is mainly the role of ISIRT to detect, prioritise and analyse incidents that are encountered in their organisation (Cichonski et al., 2012). Table 5-2 depicts the interaction between individual situational awareness and shared situational awareness within the context of ISIM.

Table 5-2: Understanding the Interaction between Individual Situational Awareness and Shared Situational Awareness

Situational Awareness in ISIM	**Individual Situational Awareness**	**Shared Situational Awareness**
Awareness of an existing situation (situation **perception)** involves situation recognition (knowing that an attack is occurring) and detection of the type of attack, source of attack, intention of attack, damage resulting from the attack, and the impact of the attack.	The user individually detects, describes, and reports an incident.	The identified incident is verified, conveyed, and shared by ISIRT for mutual awareness
Impact assessment and vulnerability analysis	User receives incident analysis report to assist in the **comprehension** of incident information.	ISIRT **comprehend**, assess, and determine incident severity level and determine the incident level.
Situation tracking	User follows the status of each incident.	ISIRT tracks the situation of each incident.
Awareness of the adversary behaviour, trends and intent analysis. Why and how the event occurred Causality analysis (via backtracking) and forensics.	User receives a report of incident behaviour, learns from incident intent. User receives a report of the incident assessment and learns from retroactive incident data.	ISIRT determines and updates incident intent behaviours. ISIRT conducts incident assessment retroactively for possible causal analysis.
Awareness of the reliability of the gathered situational awareness information and decisions. Metrics include reliability, completeness, and cleanness.	User receives verified reports of initial incident data.	ISIRT verifies the incident data input by users for its completeness and truthfulness.
Project successive actions from the adversary and constrain similar cases in the future. The constraining involves understanding motive, prospect, and ability.	User conducts projection of incident at individual level for their consumption.	ISIRT projects subsequent incidents from the previous incident.

5.6. Synopsis of the Conceptual Model – (CCA^{ISIM})

The CCA^{ISIM} model was developed by constituting the core elements of individual, shared and role-based situational awareness. The model was designated as a **C**oordinated **C**ommunication and **A**wareness approach towards enhancing **I**nformation **S**ecurity **I**ncident **M**anagement (CCA^{ISIM}). Figure 5-6 shows the first order view of the CCA^{ISIM}.

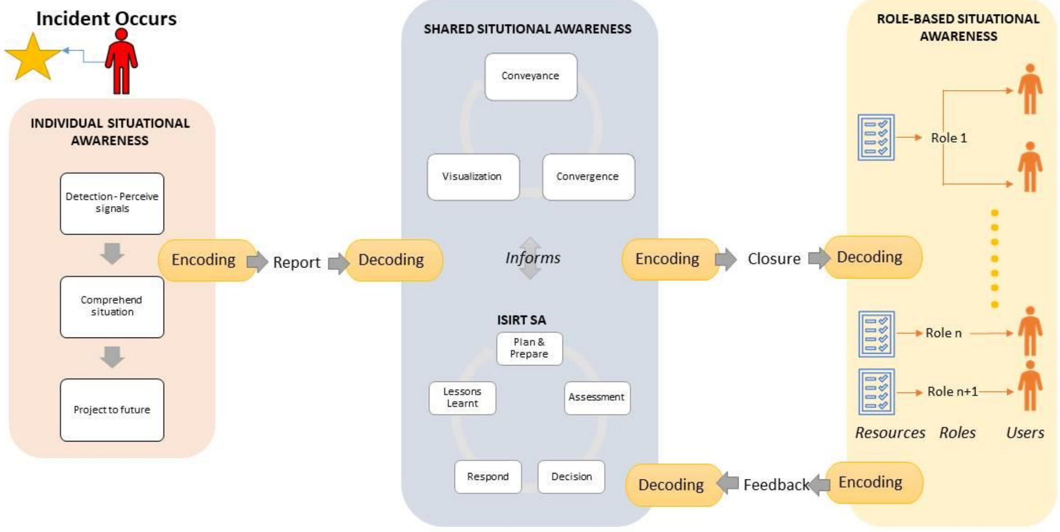


Figure 5-6: First order view of the CCA^{ISIM} Model

In Figure 5-6, the user reports an incident based on the perception derived from various elements of the incident such as the type, source and target of the incident attack. Thus, based on the characteristics of the incident and comprehension of the existing situation, the user creates a projection of the successive incident. These tasks at the individual level are encoded and communicated to the group or shared among relevant stakeholders via a report. The decoding involves including other types of contextual factors to form a richer picture of the incident. The ISIRT team will analyse, interpret, report, and conduct further planning and preparation to manage the incidents and to learn from incidents. Although it is shared among all users, it is the ISIRT SA (situational awareness) that takes ownership of the planning, assessment, decision, response, and lessons learnt and communication. However, it is executed within the framework of shared principles of situational awareness (conveyance, visualisation, and convergence). Usually, the ISIRTs are involved in the process of analysis, filtering, combining and deciding which incident information to share and report. Based on the communication within the organisation internally between ISIRT and team members, the ISIRT compiles a closure report.

While encoding deals with the creation of messages which a person requires to communicate with another person, decoding refers to the listener or audience of the encoded message to construct or understand the connotation of the message (Lunenburg, 2010). In communication, fields of experience refers to attitudes, life experiences, values and beliefs that each communicator conveys to the interactive process and that determines how messages are communicated (sent and received) (Foulger, 2004). Schramm (1954) also incorporated the ‘field of experience’ element to his communication model to denote the effect that experience and context have on the explanation of information transmitted in a communications field.

The ISIRT team encodes a closure report which is then disseminated to the wider stakeholders. The decoding of the closure report involves separating it according to roles as it will enhance the communication of incident information. The role-based access control model will be used as a basis to accommodate various stakeholders according to their field of experience, role, and their decision-making role for a given incident.

To ensure that information is communicated correctly, each individual stakeholder sends a feedback report, therefore they encode the information that they received, and send the feedback report to the ISIRT. The system decodes the report for the ISIRT by including contextual information including individual factors of the user (such as their field of experience).

5.7. Limitations of the Conceptual Model

The model is neither an automatic IDS that instantly detects incidents into its system nor primarily detects incidents from its source. Rather the model intends to implement a communication and awareness platform on already existing data in a coordinated fashion. There could be hindrances to communication such as physical, process, time, meaning and psychosocial barriers (Lunenburg, 2010). These facets were not considered in the model.

The model assumes that information is readily available in order to enhance situational awareness and communication efforts. Addressing an incident must be done timeously, however, there are instances where not all incident data is readily available in order to be able to act accordingly. This is one of the limitations of the model. Working with incomplete data could be a subject of further research.

It is often the case that information security incidents faced by an organisation is part of a larger or extended incident affecting multiple organisations, in the same sector, or in different sectors. For example, ransomware attacks could affect multiple organisations and these organisations may need to collaborate to manage these incidents. The ISIM process often requires collaboration with external organisations, including public authorities, law enforcement, etc. These external entities may be included as another role with specific privileges within the model concept. However, collaboration with external stakeholders was not the target within the model concept. Hence the prototype, discussions and applications within this research are limited to the intra-organisational perspective.

5.8. Contribution of the Model

The ISO/IEC 27035 standard was considered as a basis for the model as it presents basic theories and stages of ISIM and incorporates these concepts with principles in a systematic approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt (ISO/ IEC, 2016). Though the importance of situational awareness has been raised and studied by extant authors such as Endsley (1995) and Webb et al., (2014), few studies were devoted to pragmatic information exchange and reporting for cyber-situational awareness (Franke & Brynielsson, 2014). Although awareness and training are significant elements in the ISO/IEC 27035 standard, poor collaboration and communication are known problems within ISIM (Tøndel et al., 2014). The exploratory study (Chapter 4) revealed that there is a need for an integrated process for reporting and awareness formation within ISIM functions. As a result, the CCA^{ISIM} model was proposed as it enables collaborative and shared awareness with ISIM. Additionally researchers within the field stressed the need to study ISIM from a collaborative and user-centred approach (Ahmad, Hadgkiss, & Ruighaver, 2012), thus addressing the human-centric facets of ISIM.

The unique characteristics of applying the situational awareness model in this study are the following:

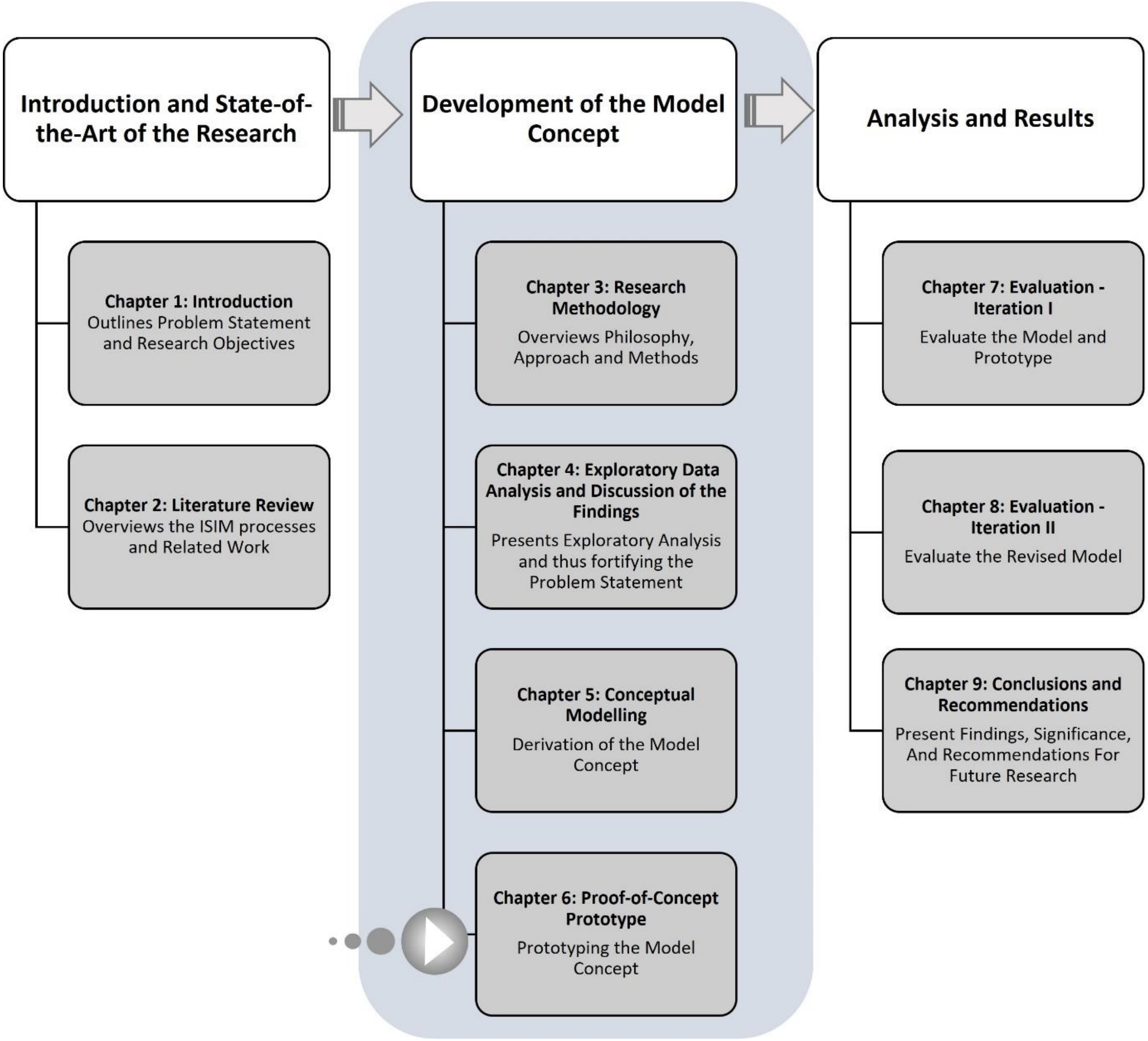
- Provides a coordinated effort towards awareness and communication integrating the concepts of ISIM, situational awareness and IMC.
- Provides a role-based access control mechanism where relevant incident information is disseminated according to the role of the user.
- Applies a user-centred approach for information access and retrieval. The model enables users to be engaged in the process of ISIM. Users have the ability to access, interact, retrieve, and use the incident information according to their roles.

5.9. Chapter Summary

This chapter provided a synopsis of the model concept. This model is unique in many aspects. Firstly, the model coordinates awareness and communication efforts within ISIM to manage information security incidents in organisations. Secondly, the model processes incident information in a progressive manner from individual to shared situational awareness. Thirdly, it proffers a role-based mechanism that attempts to manage incident information (clustering users by their role and privileges). Fourthly, the model includes a communication protocol to assist in encoding and decoding incident information according to the user’s field of experience and contextual information. The model exemplified in this study has addressed some of the most pertinent issues raised by the respondents to the exploratory study (Chapter 4). Chapter 6 will demonstrate the applicability of the model via prototyping.

CHAPTER SIX

RESEARCH ROADMAP


Introduction and State-of-the-Art of the Research
Development of the Model Concept
Analysis and Results
Chapter 1: Introduction
Outlines Problem Statement and Research Objectives
Chapter 2: Literature Review
Overviews the ISIM processes and Related Work
Chapter 3: Research Methodology
Overviews Philosophy, Approach and Methods
Chapter 4: Exploratory Data Analysis and Discussion of the Findings
Presents Exploratory Analysis and thus fortifying the Problem Statement
Chapter 5: Conceptual Modelling
Derivation of the Model Concept
Chapter 6: Proof-of-Concept Prototype
Prototyping the Model Concept
Chapter 7: Evaluation - Iteration I
Evaluate the Model and Prototype
Chapter 8: Evaluation - Iteration II
Evaluate the Revised Model
Chapter 9: Conclusions and Recommendations
Present Findings, Significance, And Recommendations For Future Research

CHAPTER 6: PROOF-OF-CONCEPT PROTOTYPE

6.1. Introduction

This chapter demonstrates the proof-of-concept of the conceptual model – A **C**oordinated **C**ommunication and **A**wareness approach towards enhancing **I**nformation **S**ecurity **I**ncident **M**anagement (CCA^{ISIM}) that was proffered in Chapter 5. The structural components and design specifications of the model (Section 6.2), the development environment (Section 6.3), the architectural components (Section 6.4), the user interaction diagram (Section 6.5) and the use case diagram (Section 6.6) are presented prior to the demonstration of the interface prototype (Section 6.7). The closing sections consider the limitations of the prototype (Section 6.8) and the concluding remarks (Section 6.9).

6.2. Structural Components and Design Specifications of the Model

The prototype was an interface prototype which simulates a subset of the functionality of the model. The encoding and decoding elements of the communication protocols were not prototyped as these functionalities are internal to the system and would theoretically use contextual information to encode and decode the incident information contained in the reports. The prototype was only evaluated on sample data. The prototype was not evaluated within a real-world context. The structural components of the prototype are derived from the core components of the model. The following sub-sections discuss the structural components of the model.

6.2.1. Individual Situational Awareness – Specific Descriptions

The individual situational awareness incorporates perception, comprehension, and projection components of the model (Section 5.5.1).

Perception

The system is predicated on the user detecting an information security incident. This process involves the perception of the source of an incident which is the basic preliminary incident data before any form of processing. It includes data related to the incident name, incident type, incident category, and incident frequency. It may also locate the basic source of the incident using its Internet Protocol (IP) address in collaboration with the Information Security Incident

Response Team (ISIRT) members. This process allows registered users to capture an occurrence of an incident on the system.

Comprehension

This process deals with further analysis of the basic incident information detected at the perception step. The comprehension component analyses possible existing relationships between available incidents for their correlation or interaction. The comprehension component enables the user to trace the frequency of an incident from a triangulation of a variety of sources. Users can visually view the source IP address and its relation to other IP addresses amongst numerous transactions. The visualisation links incident information between various entities to animate the path of the incident. Thus, such relational linkage enables the reporter of the incident to enhance their comprehensibility at an individual level so that users can relate and link their existing knowledge with the organisational incident database. As all the incident information is stored and communicated to all users depending on their role and access, the cumulative summary and aggregate analysed incident data by all users support both individual and shared understanding. This helps to have a common and shared picture of how information security incidents are manifesting in the organisation. This component leverages the strategies of Triangulation (i.e., multiple sources of data) and Correlation with known incidents from Sense-making and includes visualisation to improve the understanding of an incident.

Projection

This step considers the projection of the next incident based on the current incident encountered. The projection component attempts to visualise the frequency and patterns of incidents using graphs and charts. This step aims to determine the next entity that could be attacked if the attacker is not circumvented or the type of attack that will prevail in a specific context. For example, an attacker who gains access to an employee entity can therefore use this information to gain access into the client entity. It incorporates information on the type of incident and on the group that could be vulnerable to the attack. These projections assist users of organisations to infer and predict the probability of a reoccurrence of an incident from existing collected incident information.

The information collection for incident projection includes:

- Incident type
- Attack intention
- Incident source (origin)
- IP Address
- Incident frequency
- Incident damage

6.2.2. Shared Situational Awareness – Specific Descriptions

In the shared situational awareness component (Section 5.5.2), conveyance, convergence and visualisation are core mechanisms. This component will support the processes of conveyance and convergence with respect to strategies such as contextualisation (i.e. team members use their past experiences to develop a shared understanding), action (i.e. team members use this strategy when confronted by new incidents and they interact with one another by asking and responding to questions and seeking and providing information), triangulation (i.e. using a variety of sources to obtain a rich picture from a diversity of users), deliberation (i.e. integrate the contextualisation, triangulation and action information to form an individual mental model) and affiliation (i.e. creates a shared mental model through comparing with individual mental models). However, in a socio-technical solution, some aspects occur between human actors, and it was not practically possible to show these interactions within the interface prototype.

This component also supports the functional processes of ISIM (i.e., planning, detection, assessment, response, and lessons learnt). Some of the actions that are depicted in the prototype include detection, assessment, response, and lessons learnt. Note these depictions are largely limited in that only a minor subset of the functionality is considered. In the shared situational awareness component, the processes of comprehension and projection are also involved in promulgating a shared understanding of the incidents. The comprehension and projection at the individual level are also mirrored at the shared level for users ensuring enhanced understanding. Much of the shared situational awareness component revolves around the processes of ISIM and the engagement of the ISIRT.

Thus, the ISIRT is involved in the following objectives:

- Comprehends, assesses, and determines incident severity level.
- Assesses and updates incident metadata such as its source, intention, and type.
- Conducts incident assessment retrospectively for possible causal analysis and response.
- Verifies incident data input by users for its completeness and truthfulness.
- Projects the next incident from the previous incident.

Note these objectives of the ISIRT are also limited in the interface prototype, however, these interactions need to be considered for a full-scale implementation of the model.

6.2.3. Role-based Situational Awareness – Specific Descriptions

The various roles in the organisation are simulated in the prototype (Section 5.5.3). The differentiated role supports users to obtain incident information pertaining to their access and privileges in the organisation. In this instance, the role is categorised into three types: end-user, ISIRT and management. In this regard, the model provides a mechanism for each role to receive customised incident information.

6.2.4. Summary Requirements for Implementing the CCA^{ISIM} Model

Table 6-1 provides a list of specifications for implementing the CCA^{ISIM} model. These specifications establish the basic functionality of the model.

Table 6-1: Summary Requirements for the CCA^{ISIM} Model

Prototype Design Features	**Description**
Individual Situational Awareness	This feature enables individual users to engage in the system as part of the processes of individual situational awareness. Users are engaged in incident reporting/registrations (i.e., **perception**), incident **comprehension** and **incident projection**.
Shared Situational Awareness	The shared situational awareness feature enables users to access incident information from various users for a shared understanding. This feature works through approval and review of the incident information by the ISIRT. The sense-making strategies of conveyance and convergence also support the transformation of incident information from one group of users to another for shared understanding. It is also supported with the visualisation of incident information.
Convey Incident	This feature enables users to transfer incident information upon registration to other users in a shared environment. ISIRTs take **action** for reported incidents by collaborating with stakeholders. Users also take **action** as part of the response process in the form of complying with precautions or recommended actions. Moreover,

Prototype Design Features	**Description**
	users can **triangulate** and **contextualise** incident information to support their decision-making and action taking.
Converge Incident	**Deliberation** involves integrating the incident information gained through action, triangulation, and contextualisation in order to understand the current situation. The registered incident information will be converged in a repository central system for shared understanding. **Affiliation** or a shared model of understanding about the incident is achieved through incident sharing among individual users. The centralised data repository is supported by centralised management by the ISIRT and sharing of converged incident information supports affiliation (shared mental model) among users for mutual understanding.
Contextualisation	Contextual information (e.g., incident type, incident source, incident category) about the incident is collated from the individuals then by the ISIRT to support the shared understanding, comprehension, and projection of an incident.
Action	Team members use this strategy when confronted by a new incident and they interact with one another. This can be through providing incident information, linking incident information, and interacting with other individual users to understand the nature of the incident.
Triangulation	Using a variety of sources to obtain a richer picture from a diversity of users. The triangulation of incident information or crosschecking from the system can be performed by end-users, ISIRT and management using various criteria such as incident source, damage, intention, and severity. The triangulation feature helps users to obtain a nuanced understanding of the general patterns and trends of incidents for appropriate action.
Deliberation	This feature involves integrating the incident information from the processes of action, triangulation, and contextualisation.
Affiliation	This feature generates a shared mental model by comparing individual mental models. The association of an incident from one individual to another which supports the relation of incident information from the individual to the shared level is supported by a central repository.
Role-based Situational Awareness	The role-based feature enables users to access incident information pertaining to their role and privilege. This feature clusters users into different groups such as end-user, ISIRT member and management. This may involve a classification of incident information according to organisational information security policies (it is beyond the scope of the thesis to consider how the roles and privileges will be defined).

6.3. The Development Environment

This section explains the development environment for the prototype that is built based on a subset of the requirements. A local workstation running the Windows 10 operating system was utilised for developing the prototype. Regarding the application program, Java was used for programming and MySQL was used for the database management. Specifically, Oracle Java (JDK) 7 was used as the programming language. Apache Tomcat 7 was used as a server for the interface prototype development platform. See Appendices D, E and F for more on the development.

6.4. Architectural Diagram

According to the architectural diagram (Figure 6-1), users are involved in various functions of the processes of ISIM from individual situational awareness to shared situational awareness in a continuum. Individual users have the responsibility to detect, comprehend and report incidents as part of the processes of ISIM and to assess incidents. The users interact with the mechanisms of the model from various perspectives – from the individual to the shared situational awareness space as filtered by role-based situational awareness. For instance, the projection at the individual level is linked and progresses to shared projection. The comprehension at the individual level progresses to shared comprehension through a shared mental model. The shared situational awareness projection is also linked to the processes of ISIM planning and preparation for future incidents among the ISIRT and managers. The projected incident information is dispatched to managers or decision-makers for the purpose of planning and preparation. The management can also retrieve incident information in a summarised report after the shared situational awareness projection.

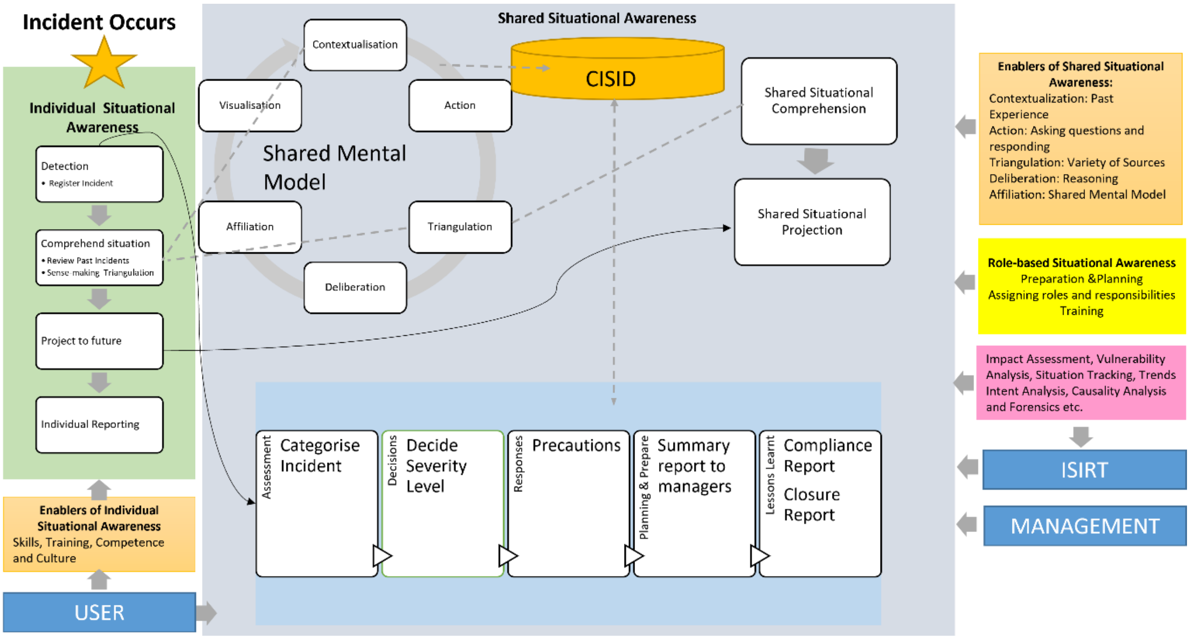

Incident Occurs
Individual Situational Awareness
Detection
• Register Incident
Comprehend situation
• Review Past Incidents
• Sense-making Triangulation
Project to future
Individual Reporting
Enablers of Individual Situational Awareness
Skills, Training, Competence and Culture
USER
Shared Situational Awareness
Contextualisation
Visualisation
Action
Shared Mental Model
Affiliation
Triangulation
Deliberation
CISID
Shared Situational Comprehension
Shared Situational Projection
Assessment
Categorise Incident
Decisions
Decide Severity Level
Responses
Precautions
Planning & Prepare
Summary report to managers
Lessons Learnt
Compliance Report
Closure Report
Enablers of Shared Situational Awareness:
Contextualization: Past Experience
Action: Asking questions and responding
Triangulation: Variety of Sources
Deliberation: Reasoning
Affiliation: Shared Mental Model
Role-based Situational Awareness
Preparation &Planning
Assigning roles and responsibilities
Training
Impact Assessment, Vulnerability Analysis, Situation Tracking, Trends Intent Analysis, Causality Analysis and Forensics etc.
ISIRT
MANAGEMENT

Figure 6-1: Architecture Diagram

The ISIM processes of assessment, decision, response, and lessons learnt are considered in the prototype, however, the preparation and planning processes for the next information security incident was not considered. For each of the ISIM processes assessment, decision, response, and lessons learnt a limited functionality was considered, that is ‘categorise incident’ (i.e., assessment), ‘decide severity level’ (i.e., decision) ‘precaution’ (i.e., response) and ‘compliance report’ (i.e., lessons learnt) were prototyped respectively. The management body can assess an ‘incident comprehension summary report’ that supports the process of planning and preparation of ISIM for the next incident. As part of the lessons learnt process, the incident closure report, is intended to dispatch an exhaustive report for every incident transaction that occurred in the organisation by the ISIRT, including its severity and current status, to all users and managers. The incident closure report which denotes the execution of the lessons learnt process is important to provide users with an overall status of the incident in the organisation which provides a comprehensive information about the characteristics of the incident.

The functions of detection, comprehension and projection at the individual situational awareness level proceed to the shared mental model which is enabled by: contextualisation, action, triangulation, deliberation, affiliation and visualisation. These components are involved in supporting shared situational awareness comprehension and shared situational awareness projection. All the incident information from the individual to the shared level is stored in the Central Information Security Incident Database (CISID). Generally, the system is supported and enabled through skill, training, context, and a role-based approach in which users learn from past experiences, take action and engage in the routine incident management system according to their functional role. The ISIRT is engaged in more higher levels of incident assessment such as impact assessment, vulnerability analysis, situation tracking, trends intent analysis, causality analysis and forensics etc. Note these higher-level functionalities were not explored in the prototype. Thus, only a limited subset of design features is implemented in the prototype.

6.5. User interaction Design

The user interaction design is based on the architectural diagram to show the detailed interaction of users. Based on a subset of the requirements for the model in Section 6.2.4, the interface prototype was designed according to the program flow depicted in Figure 6-2.

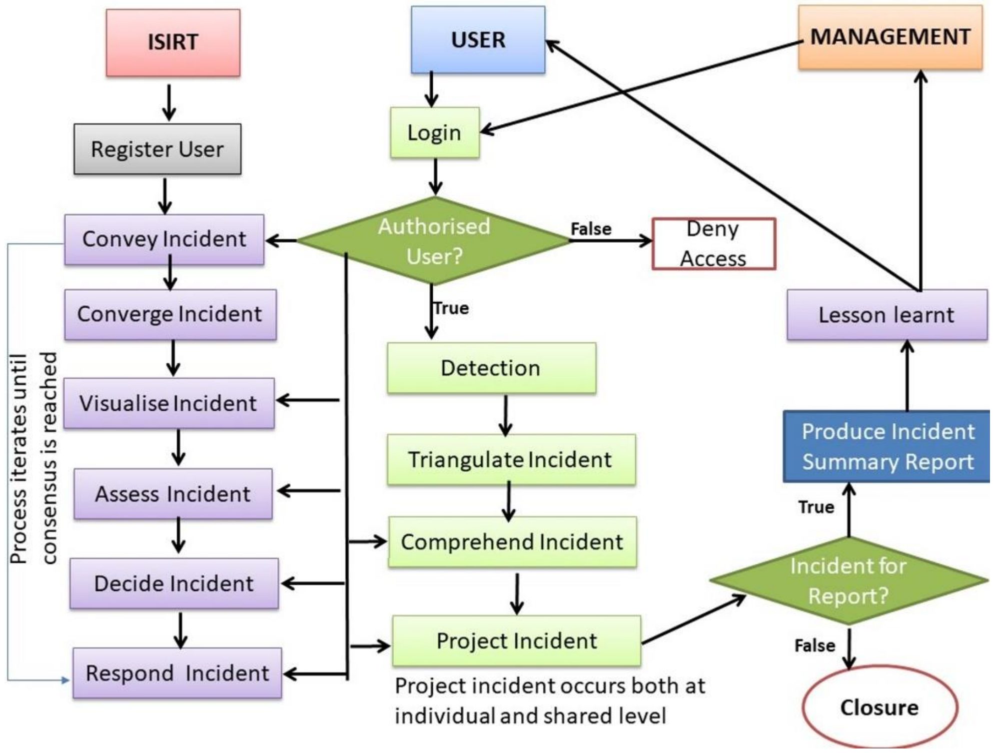


Figure 6-2: Program Flow Diagram Showing User Interaction

Figure 6-2 shows a detailed explanation followed by listing the steps for interacting with the system:

- The user logs into the system using their credentials.
- The system will only allow the user to log and access the functions if the user is known or authorised. Otherwise, it will deny the user from accessing the functions.
- The user then registers an incident (i.e., detection) that was encountered by them.
- The user triangulates incident information that is already registered in the database. This process extends to correlation with past incidents.
- The user ‘comprehends’ the incident information guided by the system.
- The user accesses incident information (from ISIRT) to enhance the comprehension step.
- The user can project incident information according to past incident information.
- The projected information by users and ISIRT will be shared with all users for a shared understanding.
- The users (usually the ISIRT involved) convey, converge, visualise, assess, and ‘decide’ on, incident information.
- The users (usually the ISIRT involved) respond to incident information. This step and the previous steps occur iteratively until consensus is reached or a shared understanding is reached.
- The users learn lessons from the incident information.
- The user can access the incident summary report (usually the ISIRT and management involved).

6.6. Use Case Diagram

The use case diagram (Figure 6-3) shows the sequence of actions in a given system boundary in which users interact with the components of a system in the standardised Unified Modelling Language (UML). In line with the conceptual modelling discussed in Chapter 5, which leverages a role-based access control structure in this system, three types of users (i.e., end-user, ISIRT member, and manager) are represented to show how they interact with the use cases. In addition, concerning role-based functions, roles are integrated into the use case diagram.

The processes of incident management related to awareness are included in the use case diagram. Some of the processes such as planning and preparation are not directly incorporated in the use case diagram but indirectly support the other functions through various processes such as assessment, decision, response, and reporting.

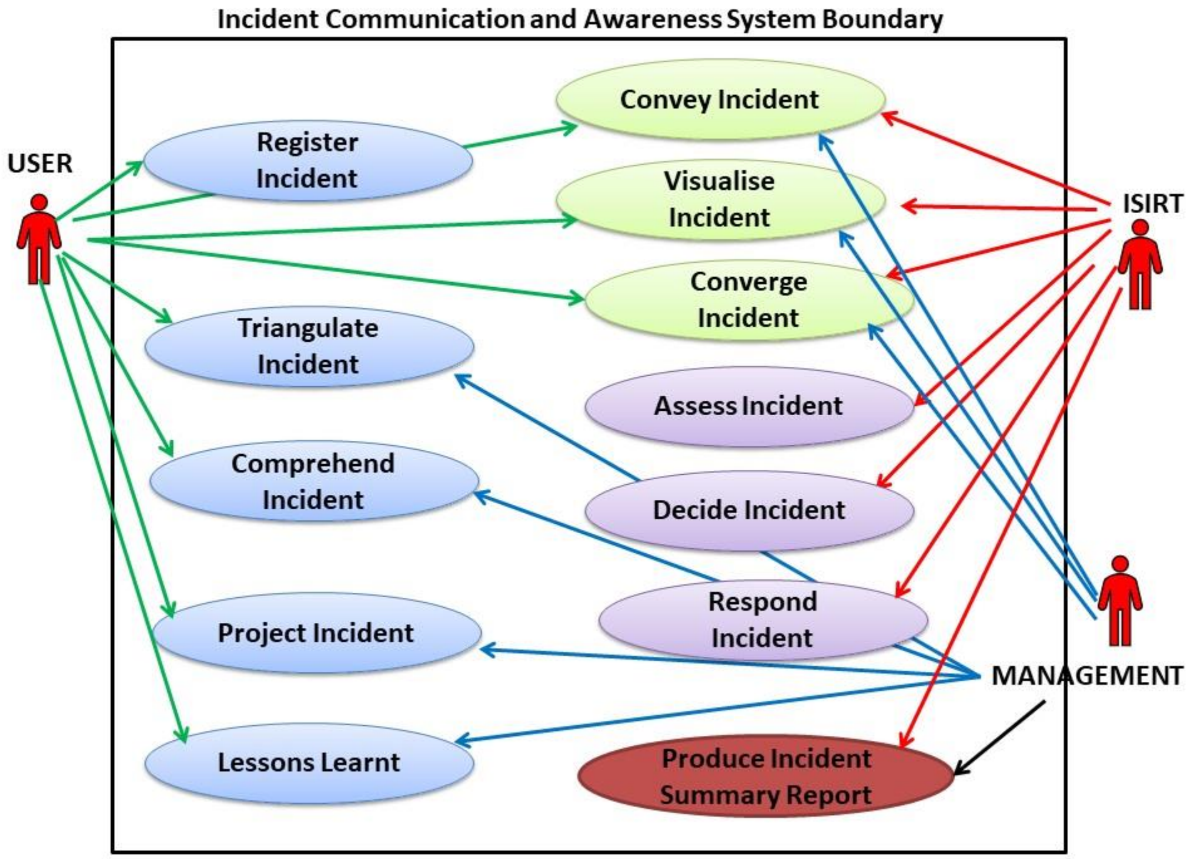


Figure 6-3: Use Case Diagram

Figure 6-3 depicts the different roles of users in organisational settings with their specific functional roles towards information security awareness. The details of the functions are described below.

Detect-Register Incident

This process deals with information security incident reporting or registration by all users. All users, using their credentials may supply the database with incident data when they encounter an information security incident within the domain. Accordingly, users input incident data when they encounter a suspicious incident (e.g., a warning alert from an antivirus system). Such incident registration serves as the detection and identification phase of ISIM. All users can register an incident with the following attributes: incident type, attack intention, incident source, IP address, incident frequency, and incident damage.

Triangulate Incidents

This process involves crosschecking incidents according to the various criteria related to an incident. All users can access this process. The triangulation criteria may differ from organisation to organisation based on their policy, experience, and the organisational information security priorities. A sample of information security criteria that could be implemented is depicted in Table 6-2.

Table 6-2: Information Security Incident Triangulation Criteria (adapted from (ISO/IEC, 2016 and Jouini et al., 2014))

Incident Type	Causes (Intention)	Incident Source	Damage (Caused)	Category (Method)	Severity
-Theft of data -Password loss -Compromise -Interception -Unauthorised access -Infection -Sniffer -Abuse of-privilege -Violation of security policy -Password confidentiality -Malware attack	-Deliberate -Accidental -Error -Ethical hacking -Unknown	-Internal -External -Hackers -Foreign -Unknown	-Theft/loss of assets -Financial loss -Service delivery disruption -System malfunction -Network damage -Software supply chain attacks -Advanced persistent threats (APT) -Data disclosure	-Network Worm -Trojan Horse -Bot Net -Blended Attack -Malicious code embedded on web -Denial of Service -Social Engineering -Intrusion against network -Spying -Phishing -Virus -Logic bomb	-Emergency -Critical -Warning -Information (i.e., a class of less critical incidents which simply involves informing users about the existence of the incident)

Assess Incident

The incident assessment process involves steps to critically examine the reported incident. It includes the process of incident categorisation through incident attributes. This process involves analysis of the incident in terms of its various characteristics. ISIRT members engage in the steps that require the requisite technical background regarding the assessment of the incident. The analysis involves – identifying the incident, who reported it, the nature of the incident, the contextual information regarding the incident and the type of the incident.

Decide on (i.e., Determine) the Incident Severity

Information security incidents registered in organisations can have diverse levels in terms of risk, damage, and threat for the organisation as shown in Table 6-2. The ISIRTs can determine the incident severity based on the information collected from users. Consequently, an appropriate ranking level should be assigned to the incident in order to review the extent of the damage that could be potentially caused by the incident. In relation, the ISO/IEC 27035 standard, recommends four layers of ranking depending on the incident listed. The rankings are as follows: Emergency, Critical, Warning and Information (i.e., a class of less critical incidents which simply involves informing users about the existence of the incident). This process is performed by the ISIRT, as it requires technical expertise.

The assessment of the severity rankings is calculated by considering the incident type, incident damage and contextual issues of the organisation. Although the ranking criterion for severity depends on the organisational context, the following criteria are used to determine the severity of an incident (ISO/IEC, 2016): incident type, causes, source and intention.

The categorisation criteria in this case also may differ from organisation to organisation based on their policy, past experience, and the organisational information security priorities. For instance, an organisation could determine its severity level as "**Critical**" based on the following calculation:

If *Incident type = "compromise," causes= "deliberate," origin= "External," Category = "Financial loss,"* **then** *Severity=* ***"Critical."***

This determination of incident severity only marginally addresses the full ISIM process of 'decision'. This consideration is for demonstration purposes only. The full ISIM processes of incident response and incident decision are not part of the implementation of the interface prototype.

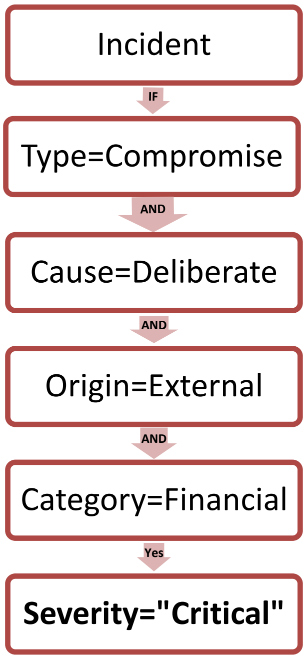


Figure 6-4: Instance of Incident Severity Ranking

Figure 6-4 shows only an instance of an incident severity ranking scenario. The severity levels were hard-coded into the prototype.

Comprehend Incident (Information)

Users obtain analysed and triangulated incident data that enables them to correlate past incident data with current incident data. The 'past incident data' is a repository of previously encountered information security incidents that were processed by ISIRT and other users. The aim is to enable users to obtain processed incident information for their consumption and awareness.

Respond (to) Incident

Responding to incidents involves a number of set actions based on the incident severity and its threat to the organisation. The ISIRT and the management participate in the response process in line with their organisational information security policy. This process could involve preventing the occurrence of an incident, reducing its severity, or recovering from the incident.

Project (Future) Incidents

Users project (i.e., forecast) incident information by characterising several incident parameters. The projection of the incident is based on incident characteristics. Users input the various characteristics of the incident such as its source, intention, IP address and cause of the incident. Thereafter, the projection step forecasts future incidents based on their input. In the prototype this was realised visually via a simulated graph. The ISIRT is also involved in projection, however, their prognosis will be informed by their higher level of expertise.

Convey and Converge Incident Information

This activity involves transferring, conveying, and converging incident information from a variety of sources to enhance a shared understanding. Here, users can transmit incident information to a centralised repository. Users can use this repository of past incidents to infer information about current incidents and to respond appropriately.

Visualise Incident Information

Visualisation of incident information enhances shared situational awareness. The visualisation helps to project the nature of the next incident and it aids the comprehensibility of current incidents.

Incident Summary Report

Any user can detect an incident and report that incident initially. The ISIRT then transforms the initial report by the user into a high-level report to enhance shared understanding. The managers receive a summarised and refined incident report that serves for decision-making and future planning.

Lessons Learnt

The lesson learning mechanism is a way of ensuring that the incident is less likely to occur in the future or if it does to minimise the damage it could cause. The mechanism could be achieved by ensuring that users comply with the organisational information security policies. For instance, individuals could be notified of their compliance or non-compliance with information security policies thus increasing their awareness of ISIM processes, which is one of the main objectives of the study.

6.7. Demonstration of the Interface Prototype

The aim of the interface prototype was to demonstrate how the interfaces would appear rather than designing a scalable system. The prototype demonstration is structured according to the following model elements:

- Individual Situational Awareness
- Shared Situational Awareness
- Role-Based Situational Awareness

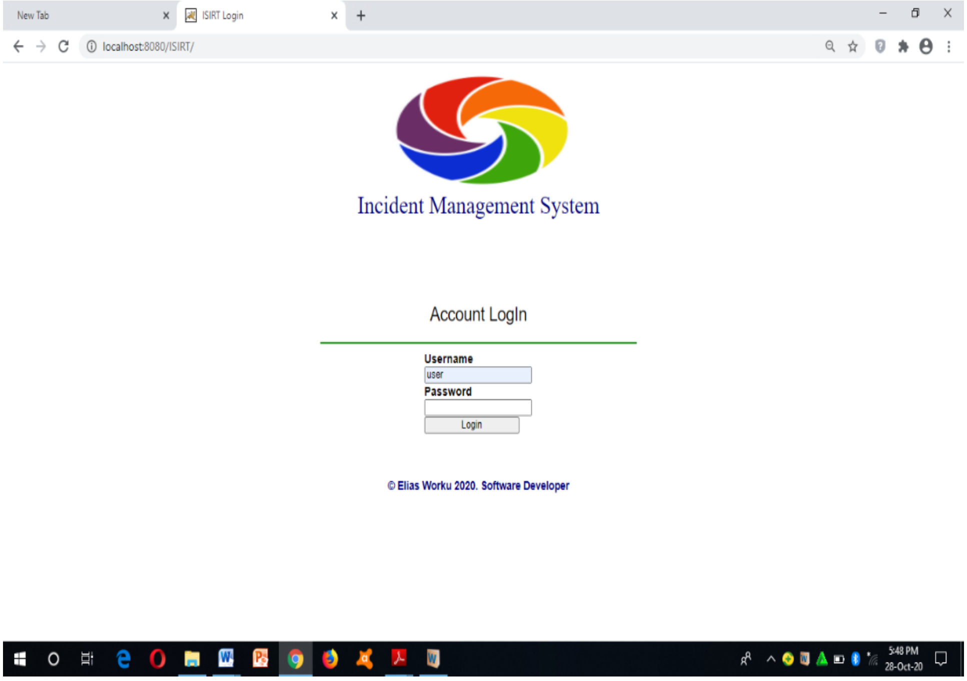
This section depicts the interaction of the system with each user role, such as end-users, ISIRT members and management (decision-makers). As discussed in Section 6.2, the interface simulation of the prototype is depicted to show the interaction at discrete levels of the model (individual, shared and role-based).

6.7.1. Individual Situational Awareness

The individual situational awareness component shows how users (such as end-users) interact with the system to conduct the processes of detection, comprehension, and projection. This component specifically includes the processes of incident registration, obtaining a comprehension report, triangulation and projecting an incident at an individual level.

Login page for all users

The system has distinctive login privileges according to the various access roles. Users sign in according to their user credentials based on their level and user profile. Figure 6-5 shows the login page interface for all users.



Incident Management System

Account LogIn

Username: user

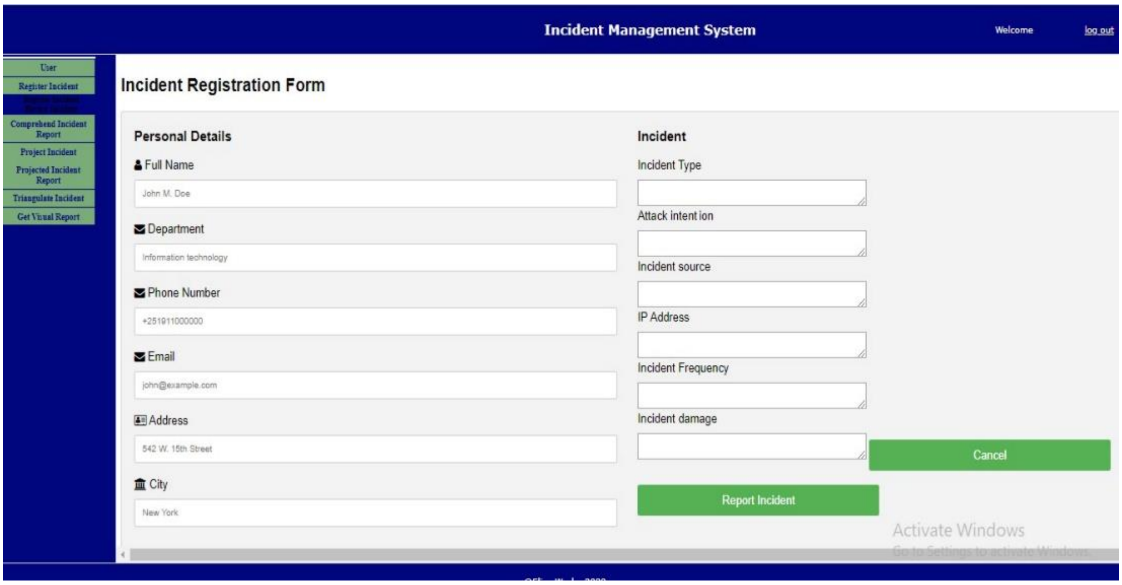
Password:

© Elias Worku 2020. Software Developer

Figure 6-5: Users' Login Form

Detection-Registration of an Incident

The **perception phase** at the individual level occurs when the user detects an information security incident, which leads to registering the incident on the system. The system administrator or the ISIRT provides the required credentials for all users. It includes their personal details such as full name, department, phone number, email address and physical address, etc.).



Incident Registration Form

Personal Details

Full Name: John M. Doe

Department: Information technology

Phone Number: +251911000000

Email: john@example.com

Address: 542 W. 15th Street

City: New York

Incident

Incident Type:

Attack intent ion:

Incident source:

IP Address:

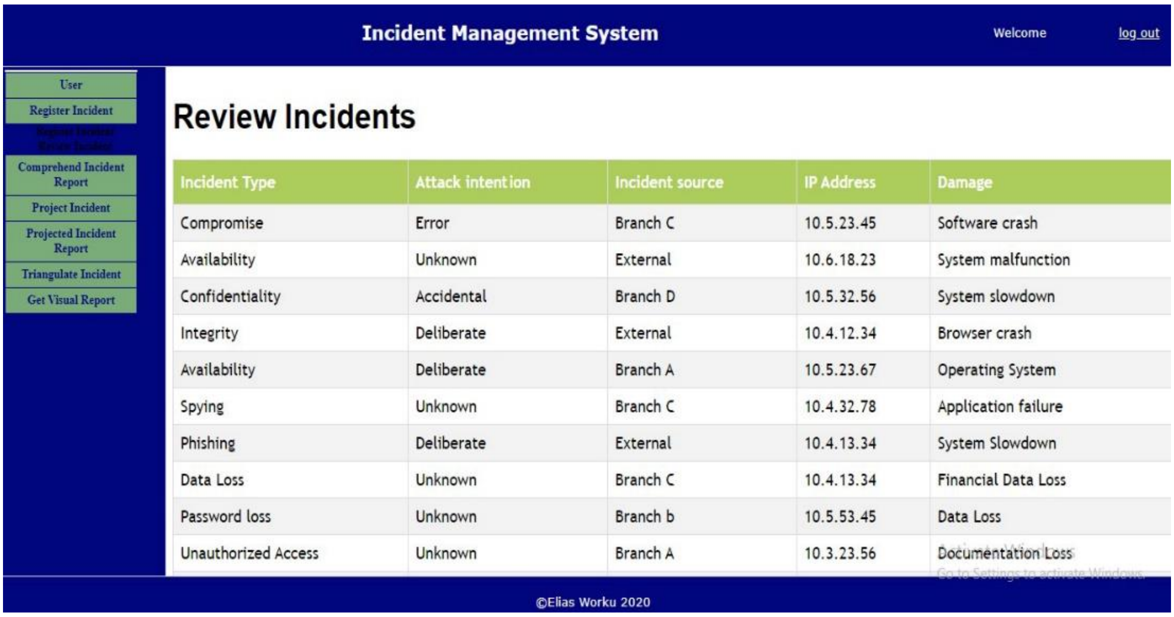
Incident Frequency:

Incident damage:

Figure 6-6: An Instance of the Information Security Incident Reporting Page

The captured personal information data is utilised to compile a profile of users in order to identify the reporter of an incident.

Figure 6-6 shows the incident registration or reporting page. The reporting page helps users in the system to identify various attributes of the incident (i.e., type, intention, source, IP address, frequency, and damage). All users register this basic incident information irrespective of their role and user group. Once the incident is registered, it will be available for review and assessment by the ISIRT members. The ISIRT members will embed additional information such as incident cause, damage, ‘precaution’, severity, etc. ‘Precaution’ is the set of actions that users must comply with as part of the ISIM response process. Moreover, all users will also be able to access incident information according to their role.



Review Incidents

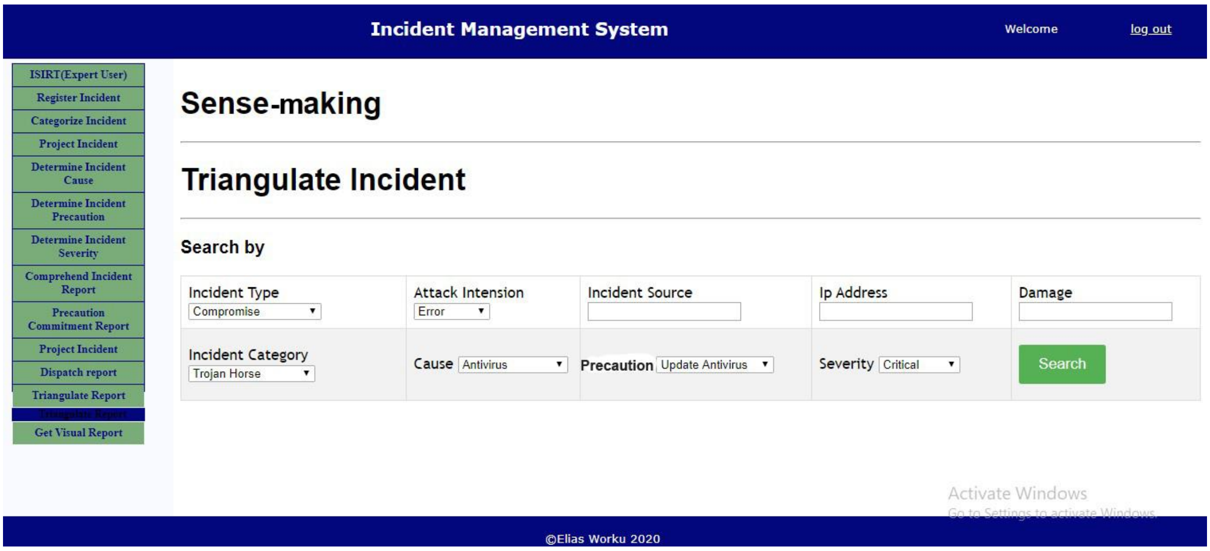
Incident Type	Attack intention	Incident source	IP Address	Damage
Compromise	Error	Branch C	10.5.23.45	Software crash
Availability	Unknown	External	10.6.18.23	System malfunction
Confidentiality	Accidental	Branch D	10.5.32.56	System slowdown
Integrity	Deliberate	External	10.4.12.34	Browser crash
Availability	Deliberate	Branch A	10.5.23.67	Operating System
Spying	Unknown	Branch C	10.4.32.78	Application failure
Phishing	Deliberate	External	10.4.13.34	System Slowdown
Data Loss	Unknown	Branch C	10.4.13.34	Financial Data Loss
Password loss	Unknown	Branch b	10.5.53.45	Data Loss
Unauthorized Access	Unknown	Branch A	10.3.23.56	Documentation Loss

Figure 6-7: An Instance of a Review Incident Report

Users can review past incident information to enhance the shared understanding of related incidents. This review report allows users to review the type of incident, intention, source (i.e., branch) and the damage caused. Figure 6-7 shows the summary report of past information security incidents. Although the ‘Review Incidents’ functionality was not demonstrated to the participants, it was available in the prototype for review.

Comprehension of the Incident

Comprehension of an incident at an individual level includes triangulation and correlation with other incidents that are related within the organisation. It is supported by a sense-making functionality of past incidents in order to enhance the understanding of the current incident. During the comprehension stage, the user can triangulate information via a system query. Figure 6-8 shows the triangulation mechanism to retrieve incident information as part of the comprehension process.



Sense-making

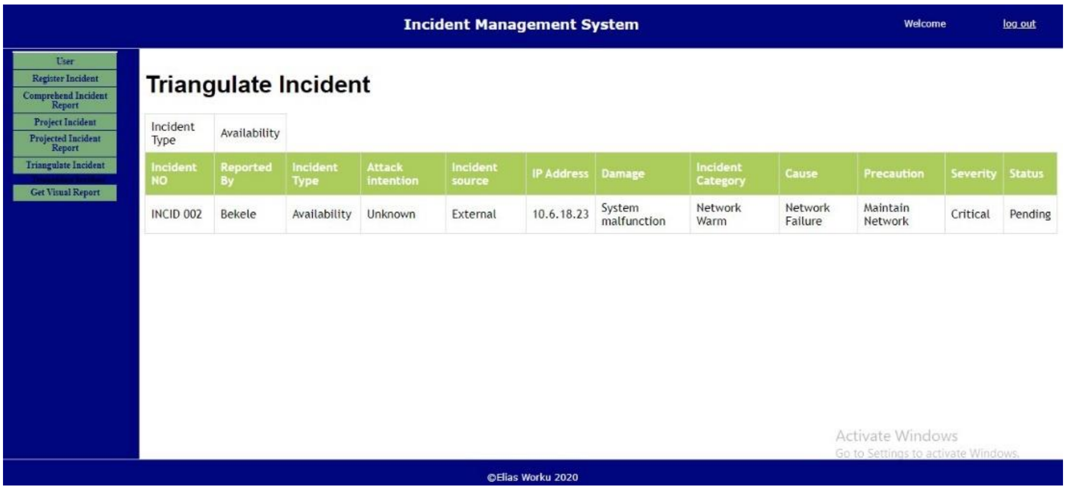
Triangulate Incident

Search by

Incident Type Compromise	Attack Intension Error	Incident Source	Ip Address	Damage
Incident Category Trojan Horse	Cause: Antivirus	Precaution: Update Antivirus	Severity: Critical	Search

Figure 6-8: Demonstration of Incident Triangulation

Figure 6-9 shows the report of the triangulated incident information from the search demonstrated in Figure 6-8. Depending on the incident data, the result shows the number of incident data associated with the parameters of the incident. The triangulated incident information shows the incident number, who reported the incident, incident type, attack intention, incident source, IP address, incident category, incident causes, the recommended precaution, the severity, and the status of the incident.



Triangulate Incident

Incident Type	Availability

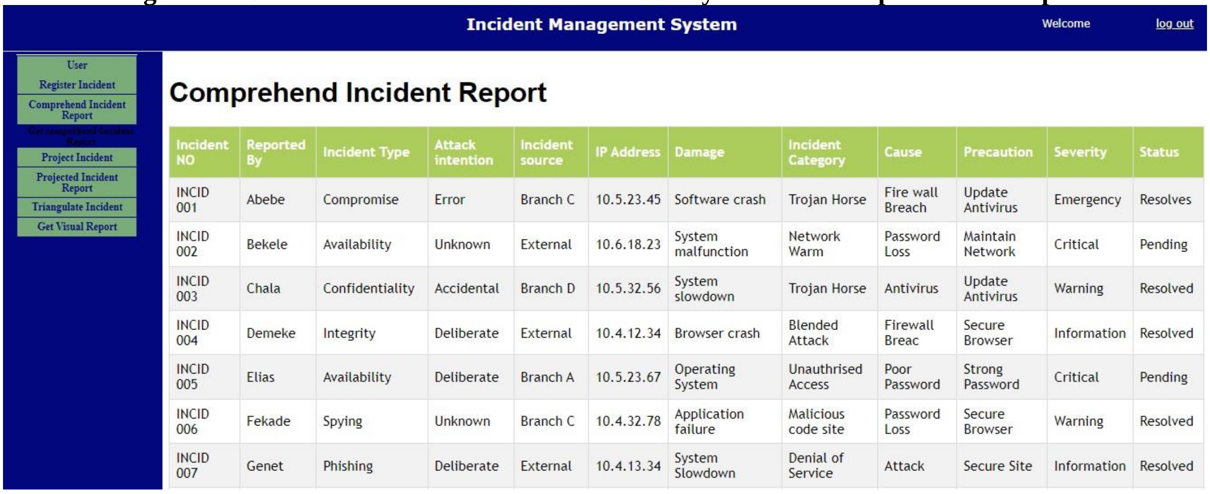
Incident NO	Reported By	Incident Type	Attack intention	Incident source	IP Address	Damage	Incident Category	Cause	Precaution	Severity	Status
INCID 002	Bekele	Availability	Unknown	External	10.6.18.23	System malfunction	Network Warm	Network Failure	Maintain Network	Critical	Pending

Figure 6-9: An Instance of an Information Security Incident Triangulation Report

The triangulation functionality was not demonstrated to the participants but was available in the prototype for inspection. The triangulation function works in the prototype by selecting the incident number, intention, source, and other parameters.

Correspondingly, users reach the comprehension phase regarding an incident from the 'Comprehend Incident Report' (see Figure 6-10). This report (comprehend incident report), which is depicted in the demonstration shows the triangulated incident with its attributes such as the incident type, incident intention, incident source, IP address, incident damage, incident category, incident cause, incident precaution, incident severity and incident status for further understanding. In this comprehension process, the ISIRT updates it according to the incident report whereas users access the comprehension report for understanding purposes.

Figure 6-10: An Instance of an Information Security Incident Comprehension Report


Incident Management System
Welcome
log out
User
Register Incident
Comprehend Incident Report
Get comprehend Incident Report
Project Incident
Projected Incident Report
Triangulate Incident
Get Visual Report

Comprehend Incident Report

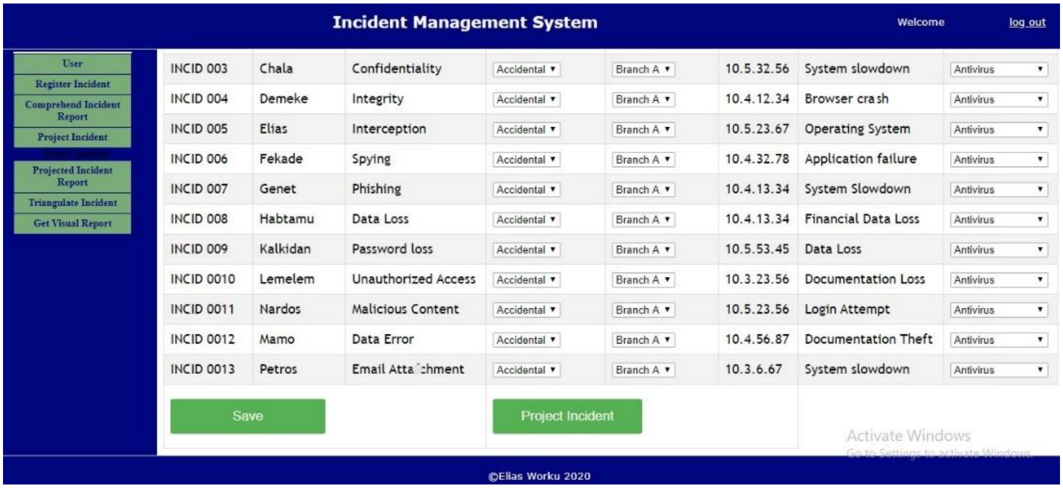
Incident NO	Reported By	Incident Type	Attack intention	Incident source	IP Address	Damage	Incident Category	Cause	Precaution	Severity	Status
INCID 001	Abebe	Compromise	Error	Branch C	10.5.23.45	Software crash	Trojan Horse	Fire wall Breach	Update Antivirus	Emergency	Resolves
INCID 002	Bekele	Availability	Unknown	External	10.6.18.23	System malfunction	Network Warm	Password Loss	Maintain Network	Critical	Pending
INCID 003	Chala	Confidentiality	Accidental	Branch D	10.5.32.56	System slowdown	Trojan Horse	Antivirus	Update Antivirus	Warning	Resolved
INCID 004	Demeke	Integrity	Deliberate	External	10.4.12.34	Browser crash	Blended Attack	Firewall Breac	Secure Browser	Information	Resolved
INCID 005	Elias	Availability	Deliberate	Branch A	10.5.23.67	Operating System	Unauthrised Access	Poor Password	Strong Password	Critical	Pending
INCID 006	Fekade	Spying	Unknown	Branch C	10.4.32.78	Application failure	Malicious code site	Password Loss	Secure Browser	Warning	Resolved
INCID 007	Genet	Phishing	Deliberate	External	10.4.13.34	System Slowdown	Denial of Service	Attack	Secure Site	Information	Resolved

This incident information will be registered in the central information security repository. The registered incident information will then be reviewed and 'comprehended' by ISIRT members for validity and dissemination. In the comprehension process and function, this 'comprehended' incident information can be accessed by all users. Thus, all users can request, access, and utilise this comprehension report for their consumption thus enhancing their awareness.

Projection of Future Incidents

Users can project incidents from previously submitted incidents. The projection of incidents at this level by an individual enables the user to independently infer the pattern of incidents in their organisation without the support of ISIRT. Such projected incident information will be available for review by the ISIRT members. The ISIRT will use this information and their technical expertise to adjust the user projection into an enhanced incident forecast. Figure 6-11 shows the projection component of an incident at the individual level. At this stage, there is a mechanism for users to project incidents at their role level through selecting and matching the various attributes of the incident such as source, cause, branch, damage, and incident category. Users select numerous parameters of the incident and activate the 'Project Incident' button to acquire the projection report.

Figure 6-11: An Instance of an Information Security Incident Projection Page



INCID 003	Chala	Confidentiality	Accidental ▾	Branch A ▾	10.5.32.56	System slowdown	Antivirus ▾
INCID 004	Demeke	Integrity	Accidental ▾	Branch A ▾	10.4.12.34	Browser cra sh	Antivirus ▾
INCID 005	Elias	Interception	Accidental ▾	Branch A ▾	10.5.23.67	Operating System	Antivirus ▾
INCID 006	Fekade	Spying	Accidental ▾	Branch A ▾	10.4.32.78	Application failure	Antivirus ▾
INCID 007	Genet	Phishing	Accidental ▾	Branch A ▾	10.4.13.34	System Slowdown	Antivirus ▾
INCID 008	Habtamu	Data Loss	Accidental ▾	Branch A ▾	10.4.13.34	Financial Data Loss	Antivirus ▾
INCID 009	Kalkidan	Password loss	Accidental ▾	Branch A ▾	10.5.53.45	Data Loss	Antivirus ▾
INCID 0010	Lemelem	Unauthorized Access	Accidental ▾	Branch A ▾	10.3.23.56	Documentation Loss	Antivirus ▾
INCID 0011	Nardos	Malicious Content	Accidental ▾	Branch A ▾	10.5.23.56	Login Attempt	Antivirus ▾
INCID 0012	Mamo	Data Error	Accidental ▾	Branch A ▾	10.4.56.87	Documentation Theft	Antivirus ▾
INCID 0013	Petros	Email Atta ̈chment	Accidental ▾	Branch A ▾	10.3.6.67	System slowdown	Antivirus ▾

©Elias Worku 2020

After the user clicks the 'project incident' button, an incident projection report will be retrieved from the system by triangulating a simulated visual projection report. The data for the projection is set by the user in order to obtain the visualised interface-based projection according to their input parameters. Users initially input various parameters for incident projection such as intention, branch, and cause of incident for projection purposes. After the users have inputted the required parameters on the projection page, the system retrieves incident data from the database to show the pattern of projection across various incident types. Note this process was simulated. The number of incidents, attack type or incident severity as a visualisation is displayed. The projection of incidents is displayed in a visualised manner so that users can easily infer the most pressing incident in the organisation. Figure 6-12 shows how the individual situational awareness incident projection simulation can be retrieved. Figure 6-12 shows the projected probability of incident occurrence (vertical) in relation to incident case type (horizontal) that occurred in the organisation.

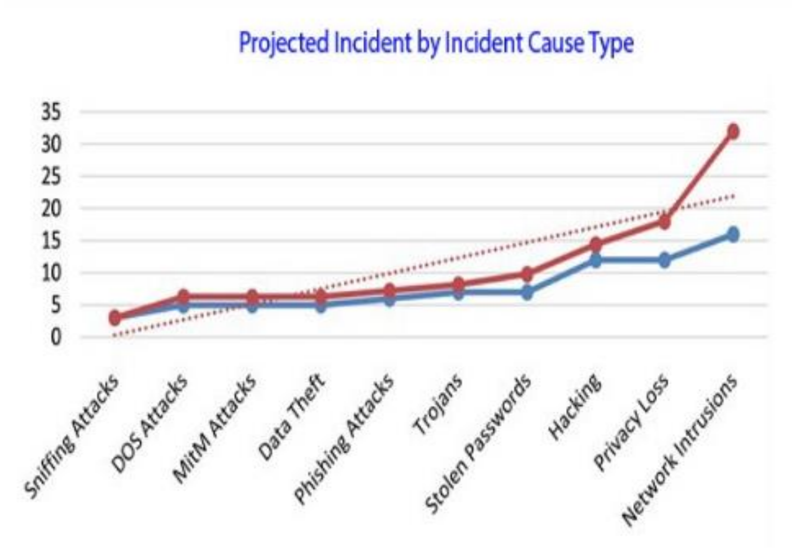


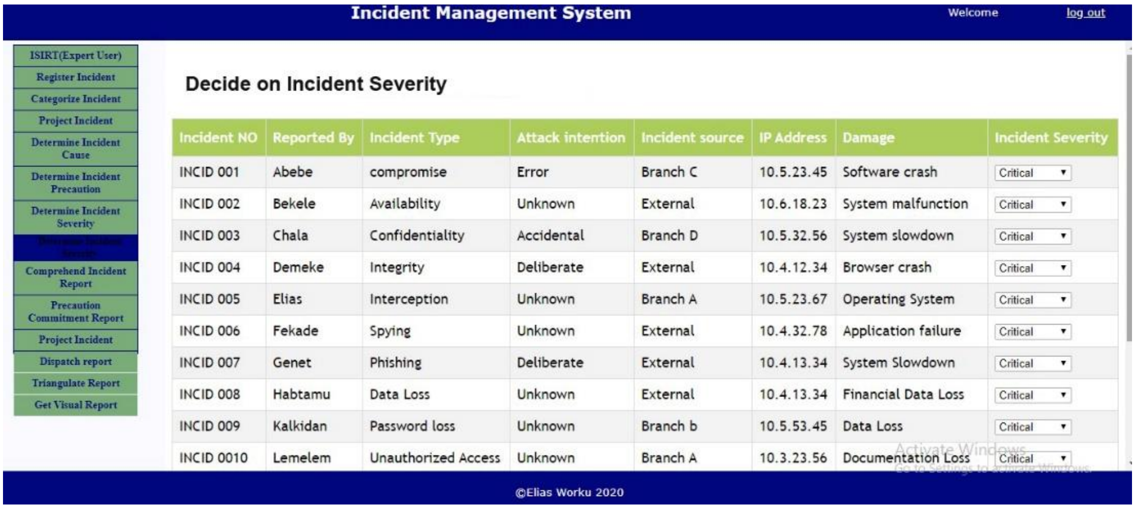
Figure 6-12: An Instance of an Individual Situational Awareness Incident Projection Report

6.7.2. Shared Situational Awareness

From a shared situational awareness perspective, ISIRT members are responsible for disseminating and augmenting incident information to all stakeholders. Figure 6-10 is an example of how the actions recommended by the ISIRT assist users to reach the comprehension phase regarding an incident from the ‘Comprehend Incident Report’ by specifying the ‘incident precaution’, ‘incident severity’ and the incident status for further understanding.

This process enhances the user’s mental model as additional information incorporated by the ISIRT improves their individual situational awareness of an information security incident. In the interaction between the individual and the shared situational awareness, the prototype simulates a process that enables users to individually detect, describe, comprehend, project, and report an incident. The incident reporting process would have been limited without this interaction.

The ISIRT reviews, comprehends, projects, analyses and incorporates supplementary incident information. The system further shows the detailed data-set components required to review and report incidents at the individual level. After any stakeholder (end-user, management, ISIRT member) has registered and input the data required by the system, the information will be available for display for end-users and management. As part of the assessment, decision and response processes of ISIM, the ISIRT then determines the parameters of the incident such as ‘incident severity’ and ‘incident precaution’.



Decide on Incident Severity

Incident NO	Reported By	Incident Type	Attack intention	Incident source	IP Address	Damage	Incident Severity
INCID 001	Abebe	compromise	Error	Branch C	10.5.23.45	Software crash	Critical ▾
INCID 002	Bekele	Availability	Unknown	External	10.6.18.23	System malfunction	Critical ▾
INCID 003	Chala	Confidentiality	Accidental	Branch D	10.5.32.56	System slowdown	Critical ▾
INCID 004	Demeke	Integrity	Deliberate	External	10.4.12.34	Browser crash	Critical ▾
INCID 005	Elias	Interception	Unknown	Branch A	10.5.23.67	Operating System	Critical ▾
INCID 006	Fekade	Spying	Unknown	External	10.4.32.78	Application failure	Critical ▾
INCID 007	Genet	Phishing	Deliberate	External	10.4.13.34	System Slowdown	Critical ▾
INCID 008	Habtamu	Data Loss	Unknown	External	10.4.13.34	Financial Data Loss	Critical ▾
INCID 009	Kalkidan	Password loss	Unknown	Branch b	10.5.53.45	Data Loss	Critical ▾
INCID 0010	Lemelem	Unauthorized Access	Unknown	Branch A	10.3.23.56	Documentation Loss	Critical ▾

Figure 6-13: An Instance of Information Security Incident Severity Decisions by ISIRT

Figure 6-13 shows how ISIRT members engage in the processes of ISIM by analysing the incident attributes such as incident reporter, incident type, incident intention, incident source, IP address, and incident damage. The ISIRT uses these attributes to determine the incident severity level. This contextual information is shared with users which enhances their comprehension of information security incidents. Moreover, ISIRT members have the access and the credentials to notify users of actions taken and actions required by other users and stakeholders. It also helps users in comprehending the type of action to undertake after the review of the decision of the severity of the incident that users have previously reported to the system. The ‘precaution’ for incidents, which is part of the response process of ISIM, is significant in the proactive management of incidents. Accordingly, users can prioritise and characterise the incidents from their prior knowledge or the organisational information security policies and procedures of the institution or the national information security policies.

Moreover, it is their responsibility to engage with the recommended precautions. The ‘precaution’ function helps users to take actions as part of the response phase of ISIM.

Shared situational awareness includes various functions related to incident processes and other related functions such as conveyance, visualisation, and convergence. The shared situational awareness component coordinates the incident information received from individuals, analyses, comprehends, decides, and disseminates further information to other users.

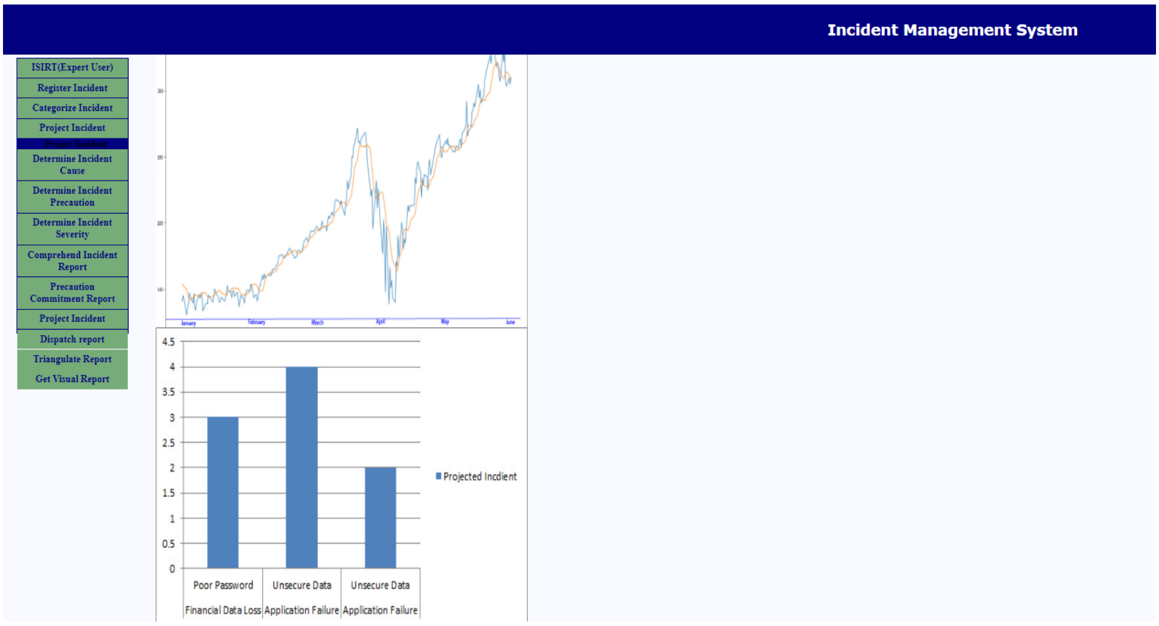
Comprehension Component – Shared Situational Awareness

Comprehension of an incident at the shared level includes triangulation, and correlation of incidents. The comprehension function and report in the shared situational awareness originates from various stakeholders. In addition, the ISIRT comprehends and analyses the incident information to be incorporated in the central system for dissemination to all users. In the shared situational awareness component, as depicted in Figure 6-10, the comprehension process enables all users to get access and understand the shared incident information made by the ISIRT such as incident category, incident precaution and incident severity.

Projection Component – Shared Situational Awareness

The simulated interface prototype summarised and projected the occurrences of an incident. This will possibly be implemented using statistical data extracted out of existing data. Thus, projection may be automated. The summarised projection can be presented in graphic illustrations based on required information such as severity, incident characteristics, and attack level. An example of showing a visualisation of the next incident predicted (i.e., projection) is shown in Figure 6-14 (for ISIRT) and Figure 6-20 (for managers). The projection information depicted in Figure 6-14 was not part of the demonstration for the participants, however, it was prototyped. The projection phase involves summary inference and reporting from the input system. These forms of reports can be retrieved for multiple users according to the incident type and severity level of the incident to be reported in an illustrated manner for shared visual understanding. These types of reports may be filtered according to the mechanisms of role-based access control however it is beyond the scope of this thesis to depict the various projections per role.

Figure 6-14: An Instance of an Information Security Incident Projection Report for ISIRT Members



The projection diagram (Figure 6-14) shows how incident parameters are related – it enables the ISIRT members to visualise and to consider the predictions of patterns of incident attacks over a period of months in their organisation (uppermost graphic). It also allows ISIRT members to visualise the projected incident pattern in the organisation through various characteristics such as the critical impact of the projected incident (lower graphic). Such projections of an incident support the decision-making processes of users, management and ISIRT for planning and preparation for the next incident.

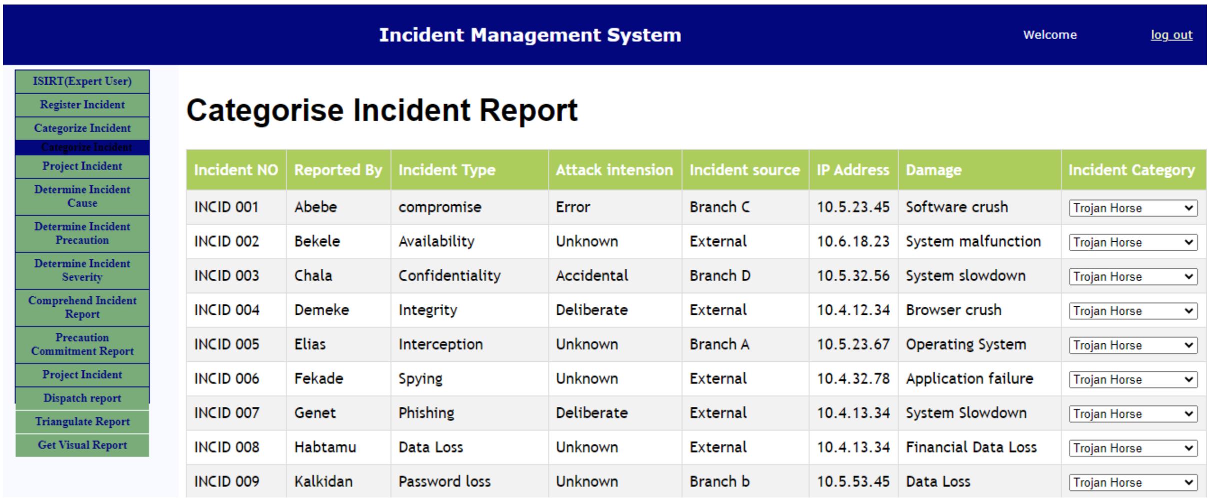
The processes of ISIM follows a cyclic process – plan and prepare; detect and report; assess and decide; respond (i.e., prevent, reduce, recover); and lessons learnt. These processes should be stored in a CISID. The following section discusses how the different processes of ISIM are incorporated into the interface prototype of the model.

Planning and Preparation

The planning and preparation processes are promoted by the ISIRT in consultation with end-users and management. This part of the process was not demonstrated in the interface prototype as it is mostly related to managerial and the decision-making process. However, after managers have reviewed the incident comprehension summary report and various visualisations (see Figures 6-19 - 6-23), they can plan and prepare for future incidents.

Assessment

The ISIRT assesses and categorises incident information that is submitted from individual users. Figure 6-15, which is demonstrated for the participants and available in the prototype, shows the assessment of different incident information. It is the responsibility of the ISIRT team to verify, assess and provide incident metadata (such as incident category, incident cause, etc.) to the incident report. This is related to the attributes such as reported by incident type, incident intention and incident source, IP Address, damage, and incident cause.



Categorise Incident Report

Incident NO	Reported By	Incident Type	Attack intension	Incident source	IP Address	Damage	Incident Category
INCID 001	Abebe	compromise	Error	Branch C	10.5.23.45	Software crush	Trojan Horse
INCID 002	Bekele	Availability	Unknown	External	10.6.18.23	System malfunction	Trojan Horse
INCID 003	Chala	Confidentiality	Accidental	Branch D	10.5.32.56	System slowdown	Trojan Horse
INCID 004	Demeke	Integrity	Deliberate	External	10.4.12.34	Browser crush	Trojan Horse
INCID 005	Elias	Interception	Unknown	Branch A	10.5.23.67	Operating System	Trojan Horse
INCID 006	Fekade	Spying	Unknown	External	10.4.32.78	Application failure	Trojan Horse
INCID 007	Genet	Phishing	Deliberate	External	10.4.13.34	System Slowdown	Trojan Horse
INCID 008	Habtamu	Data Loss	Unknown	External	10.4.13.34	Financial Data Loss	Trojan Horse
INCID 009	Kalkidan	Password loss	Unknown	Branch b	10.5.53.45	Data Loss	Trojan Horse

Figure 6-15: Instance of an Incident Categorisation Report

Decision (Determine Severity)

ISIRT members are involved in the process of decision-making for various parameters of incident information (see Figure 6-13). ISIRT members determine the incident ‘precaution’ (i.e., the response) and severity. Note this is merely a subset of the activities that the ISIRT must engage in during an incident scenario. Here, contextualisation of past experiences supports the decision-making processes of ISIM. The ISIRT determines incident severity as reported by individual users. For instance, 'INCID 001' was reported by 'Abebe' from 'Branch C'. The damage is reported as a 'software crash'. The ISIRT reviews the incident and may determine its severity to be 'critical'. Perhaps the severity level for the incident by the user had been reported as 'Information' initially. (Note, a severity level of "Information" denotes a less critical incident and requires that users be merely informed about them). In this scenario, the revised severity level of the incident from the ISIRT will be disseminated to the users that have the required role-based privileges. This will assist in the relevant users having a shared situational awareness of the current state thus improving the stakeholder's comprehensibility of incident information.

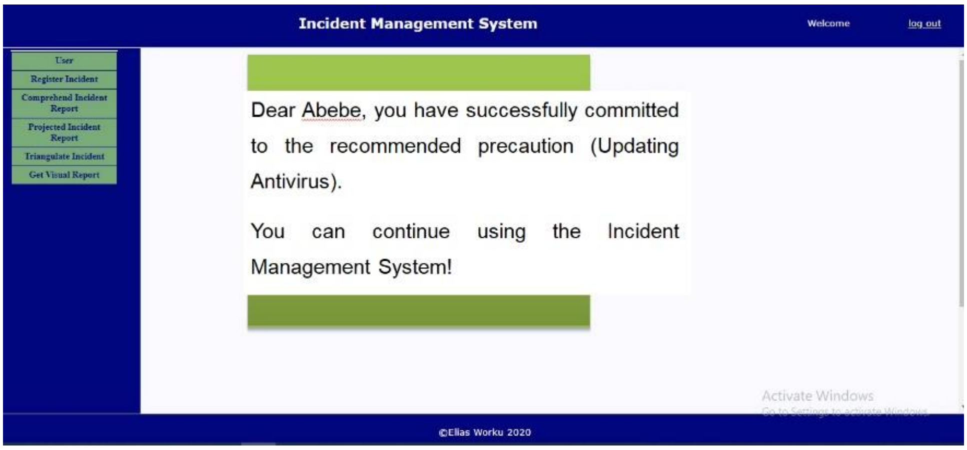
While it is suggested that these types of reports may be filtered according to the mechanisms of role-based access control, it is beyond the scope of this work to specify how the information per role will be disseminated as it will depend on the organisational context. Perhaps end-users may not have access to the user's details who reported the incident in order to maintain privacy or perhaps managers will only have access to information related to their branch that they manage.

Response

Users can review the 'response' to an incident which is formulated by the ISIRT. For instance, users have awareness of what actions or 'precautions' to undertake for a certain incident. The response for a particular incident (such as changing passwords for a compromised system) may be reproduced from similar incidents within similar contexts. Figure 6-10 demonstrates the different types of precautions that users should be aware of for each incident. The CISID will store this type of information.

Lessons Learnt

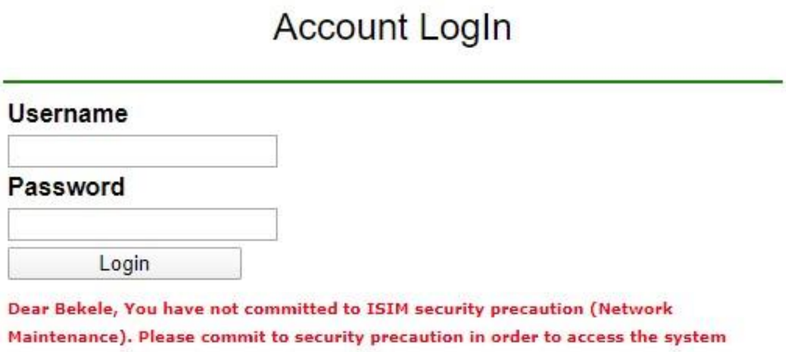
To promote the 'lessons learnt', users are provisioned with a summarised data of incidents (i.e., closure report) The prototype demonstrated a possible approach to ensure compliance with the 'precautions' instituted by the ISIRT. The approach involves the receipt of personalised messages to ensure compliance. The compliance or non-compliance with information security incident precautions will enable users to either gain access or to have their access rights suspended respectively. For instance, Figure 6-16 and Figure 6-17, which are demonstrated in the demo and available in the prototype show distinct compliance reports for two different users. Figure 6-16 shows a positive compliance report and Figure 6-17 shows a negative compliance report to suspend the user.


Incident Management System
Welcome
log out
User
Register Incident
Comprehend Incident Report
Projected Incident Report
Triangulate Incident
Get Visual Report
©Elias Worku 2020
Activate Windows
Go to Settings to activate Windows.

Dear Abebe, you have successfully committed to the recommended precaution (Updating Antivirus).

You can continue using the Incident Management System!

Figure 6-16: An Instance of a Positive Compliance Report

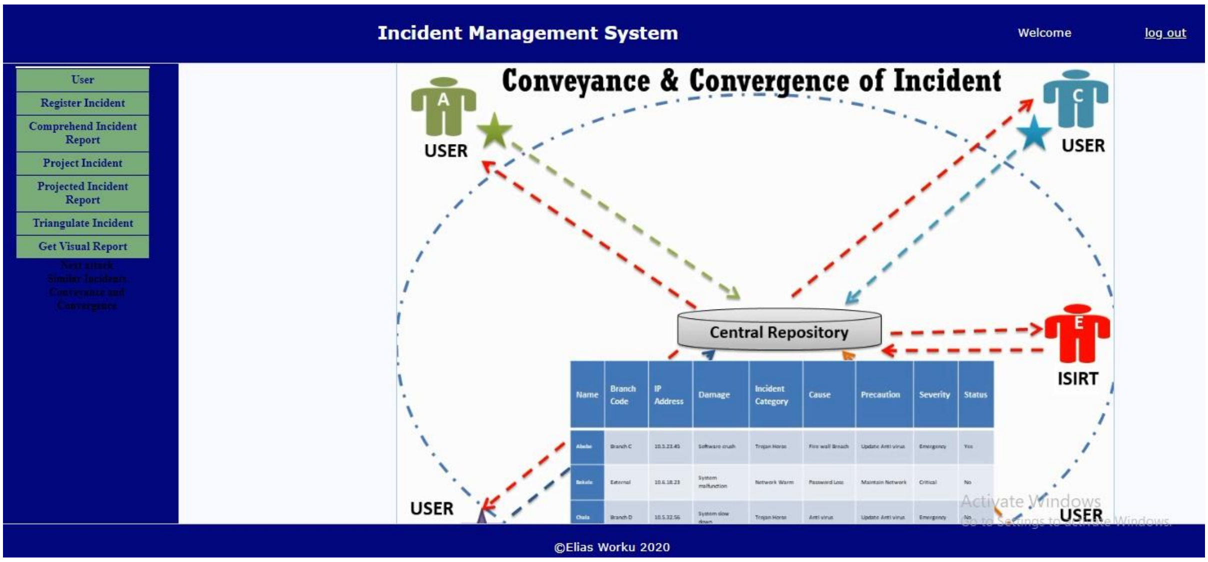


Dear Bekele, You have not committed to ISIM security precaution (Network Maintenance). Please commit to security precaution in order to access the system

Figure 6-17: An Instance of a Negative Compliance Report

Conveyance and Convergence

The notion of conveyance and convergence is a key function within shared situational awareness. Figure 6-18, which is demonstrated to participants in the demo and available in the prototype shows the prototype interface of the conveyance and convergence mechanisms. Figure 6-18 simulates the incident reporting mechanism in a converged approach so that it is retained in the central repository from multiple individuals for shared access. It is implied in the conceptual model that each user will convey (i.e., conveyance) raw information about an incident. It is possible that multiple users can convey information on the same incident type so that it will be combined by the ISIRT. Similarly, multiple users could convey information on similar (but not the same) incident, also contributing to a common understanding thus reaching convergence. The implementation of these processes is beyond the scope of this project.



Name	Branch Code	IP Address	Damage	Incident Category	Cause	Precaution	Severity	Status
Abebe	Branch C	10.5.23.45	Software crash	Trojan Horse	Fire wall Breach	Update Anti virus	Emergency	Yes
Bekele	External	10.6.18.23	System malfunction	Network Worm	Password Loss	Maintain Network	Critical	No
Chala	Branch D	10.5.32.56	System slow down	Trojan Horse	Anti virus	Update Anti virus	Emergency	No

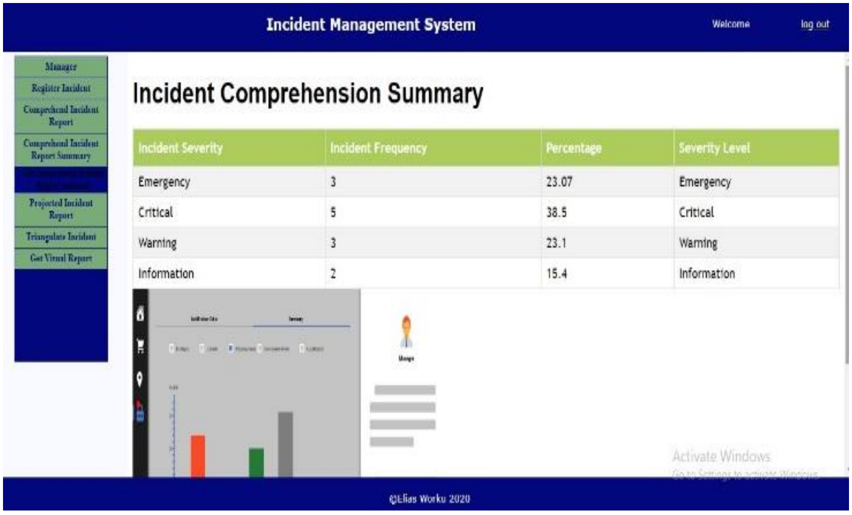
Figure 6-18: Conveyance and Convergence of Incident Information

6.7.3. Role-Based Situational Awareness

The basis for the dissemination of security incident information using role-based access control is primarily dependent on the general policies, procedures, and plans of the particular organisation. The aim of providing role-based access and differentiation is to provide information according to their level of access in the organisation. It is assumed that managers have access to more classified and summarised information on the system, whereas end-users have less access to such information. Moreover, technical users such as ISIRT members have their own administrative and controlling role in accessing the system.

Figures 6-19 to Figure 6-23 depicts instances of information security incident reports for users with ‘manager’ privileges as an illustration of role-based access control configuration. The figures show examples of summarised incident data, targets, and actions for users with a management role. Figure 9-19, Figure 6-20, and Figure 2-21 were demonstrated to the participants and were made available in the prototype for review. However, Figure 6-22 and Figure 6-23 were neither demonstrated nor available in the prototype, but they serve as examples as possible reporting mechanisms. These visualisations were proposed during the prototype development but were not included in the deployed prototype in order to simplify the interfaces for the participants. Figure 6-19 shows the instance of an incident report page for managers depicting a basic visualised ‘comprehension’ summary report.

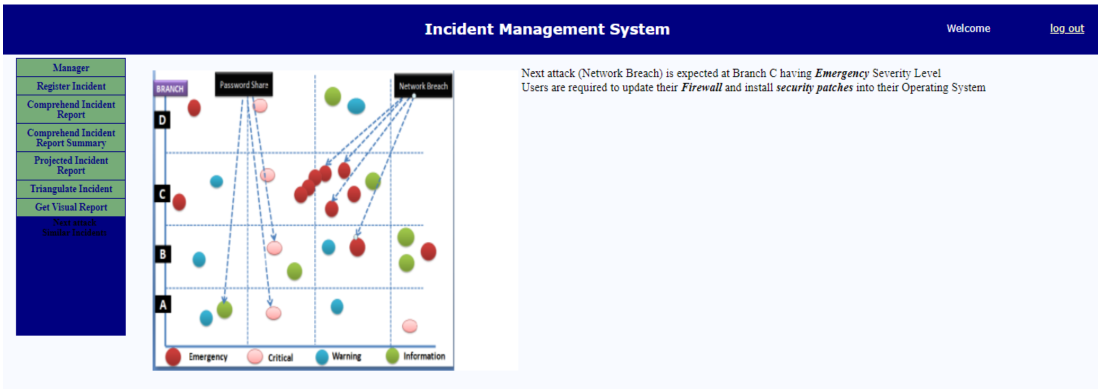
Figure 6-19: An Incident ‘Comprehension’ Summary Report for Managers


Incident Management System
Welcome
log out
Manager
Register Incident
Comprehend Incident Report
Comprehend Incident Report Summary
Projected Incident Report
Triangulate Incident
Get Visual Report
Activate Windows
©Elias Worku 2020

Incident Comprehension Summary

Incident Severity	Incident Frequency	Percentage	Severity Level
Emergency	3	23.07	Emergency
Critical	5	38.5	Critical
Warning	3	23.1	Warning
Information	2	15.4	Information

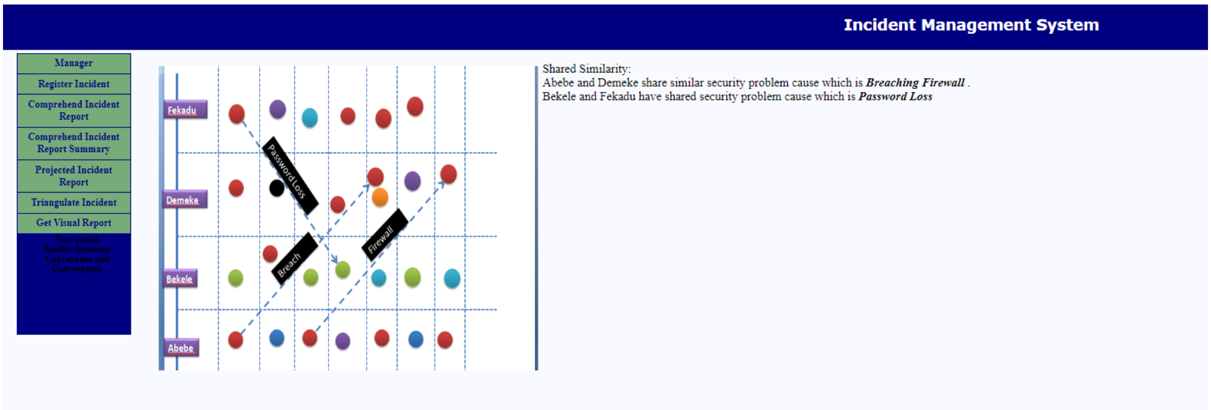
Figure 6-20 shows a visualised instance of a projected incident report page for managers with severity levels and ‘precautions’ to be undertaken. Note this visualised report was also available for other users as well for demonstration purposes within the prototype.



Next attack (Network Breach) is expected at Branch C having ***Emergency*** Severity Level
Users are required to update their ***Firewall*** and install ***security patches*** into their Operating System

Figure 6-20: A Projected Incident Report for Managers with Severity Levels and 'Precautions'

Figure 6-21 shows a visualisation of the most repeated security breaches, the most common security causes, and the most common incident occurrences. Such projections of an incident support the decision-making process of users, management and the ISIRT for planning and preparation for the next incident. Note this visualised report was also available for access by end-users and the ISIRT as well for demonstration purposes within the prototype.



Shared Similarity:
Abebe and Demeke share similar security problem cause which is ***Breaching Firewall*** .
Bekele and Fekadu have shared security problem cause which is ***Password Loss***

Figure 6-21: An Instance of an Information Security Incident Similarity Mapping Report

Figure 6-22 shows an instance of an information security incident summary report under the category of 'Business Impact' for managers.

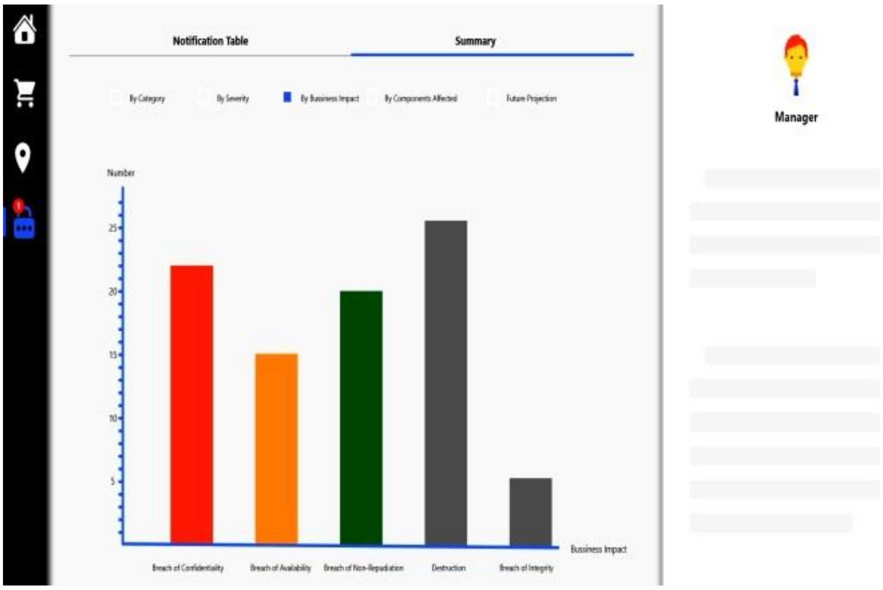
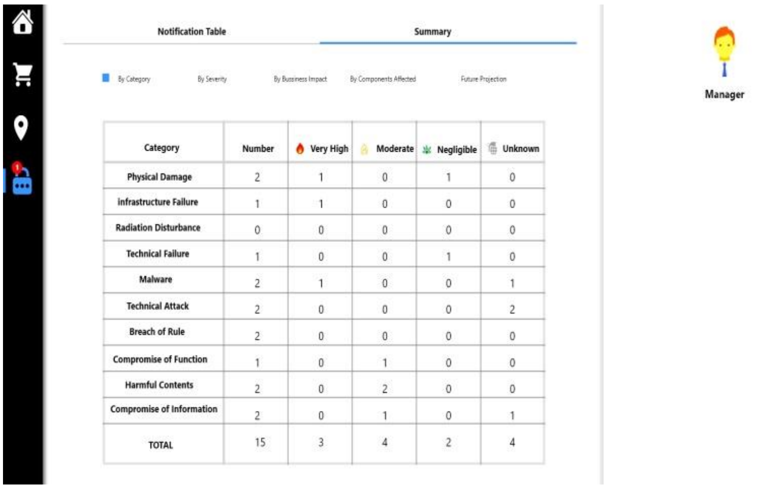


Figure 6-22: An Information Security Incident Summary Report

Figure 6-23 shows an instance of an information security incident report depicted by a matrix of incident categories and severity type.



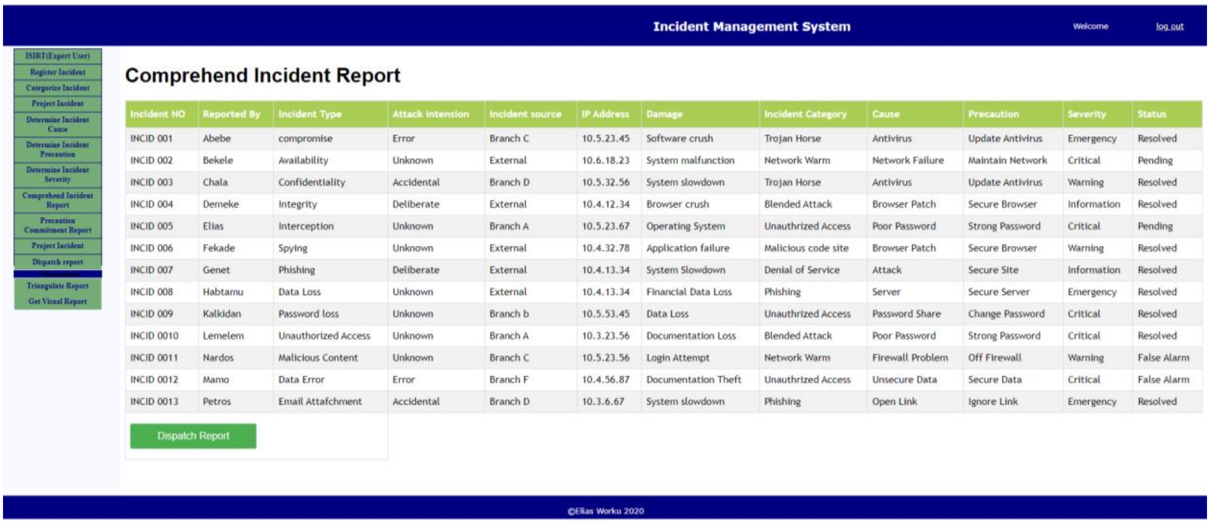
Category	Number	Very High	Moderate	Negligible	Unknown
Physical Damage	2	1	0	1	0
Infrastructure Failure	1	1	0	0	0
Radiation Disturbance	0	0	0	0	0
Technical Failure	1	0	0	1	0
Malware	2	1	0	0	1
Technical Attack	2	0	0	0	2
Breach of Rule	2	0	0	0	0
Compromise of Function	1	0	1	0	0
Harmful Contents	2	0	2	0	0
Compromise of Information	2	0	1	0	1
TOTAL	15	3	4	2	4

Figure 6-23: An Information Security Incident Matrix Report

Figure 6-22 and Figure 6-23 are instances of the report which were neither demonstrated to the participants during the evaluation nor included in the prototype.

Closure Report

The last process of the conceptual model is the closure report which is depicted as the 'comprehend incident report' on every incident transaction that occurred in the organisation. Figure 6-24 shows an instance of the summary report of incident closures to be dispatched to all users.



Comprehend Incident Report

Incident NO	Reported By	Incident Type	Attack intension	Incident source	IP Address	Damage	Incident Category	Cause	Precaution	Severity	Status
INCID 001	Abebe	compromise	Error	Branch C	10.5.23.45	Software crush	Trojan Horse	Antivirus	Update Antivirus	Emergency	Resolved
INCID 002	Bekele	Availability	Unknown	External	10.6.18.23	System malfunction	Network Warm	Network Failure	Maintain Network	Critical	Pending
INCID 003	Chala	Confidentiality	Accidental	Branch D	10.5.32.56	System slowdown	Trojan Horse	Antivirus	Update Antivirus	Warning	Resolved
INCID 004	Demeke	Integrity	Deliberate	External	10.4.12.34	Browser crush	Blended Attack	Browser Patch	Secure Browser	Information	Resolved
INCID 005	Elias	Interception	Unknown	Branch A	10.5.23.67	Operating System	Unauthrized Access	Poor Password	Strong Password	Critical	Pending
INCID 006	Fekade	Spying	Unknown	External	10.4.32.78	Application failure	Malicious code site	Browser Patch	Secure Browser	Warning	Resolved
INCID 007	Genet	Phishing	Deliberate	External	10.4.13.34	System Slowdown	Denial of Service	Attack	Secure Site	Information	Resolved
INCID 008	Habtamu	Data Loss	Unknown	External	10.4.13.34	Financial Data Loss	Phishing	Server	Secure Server	Emergency	Resolved
INCID 009	Kalkidan	Password loss	Unknown	Branch b	10.5.53.45	Data Loss	Unauthrized Access	Password Share	Change Password	Critical	Resolved
INCID 0010	Lemelem	Unauthorized Access	Unknown	Branch A	10.3.23.56	Documentation Loss	Blended Attack	Poor Password	Strong Password	Critical	Resolved
INCID 0011	Nardos	Malicious Content	Unknown	Branch C	10.5.23.56	Login Attempt	Network Warm	Firewall Problem	Off Firewall	Warning	False Alarm
INCID 0012	Mamo	Data Error	Error	Branch F	10.4.56.87	Documentation Theft	Unauthrized Access	Unsecure Data	Secure Data	Critical	False Alarm
INCID 0013	Petros	Email Attafchment	Accidental	Branch D	10.3.6.67	System slowdown	Phishing	Open Link	Ignore Link	Emergency	Resolved

Figure 6-24: An Instance of the Closure Process

This closure process was not demonstrated to the participants but was available on the prototype for the participants to review. Also, the prototype did not demonstrate the dispatching function which is intended to enhance the lessons learnt process.

6.8. Limitations of the Prototype

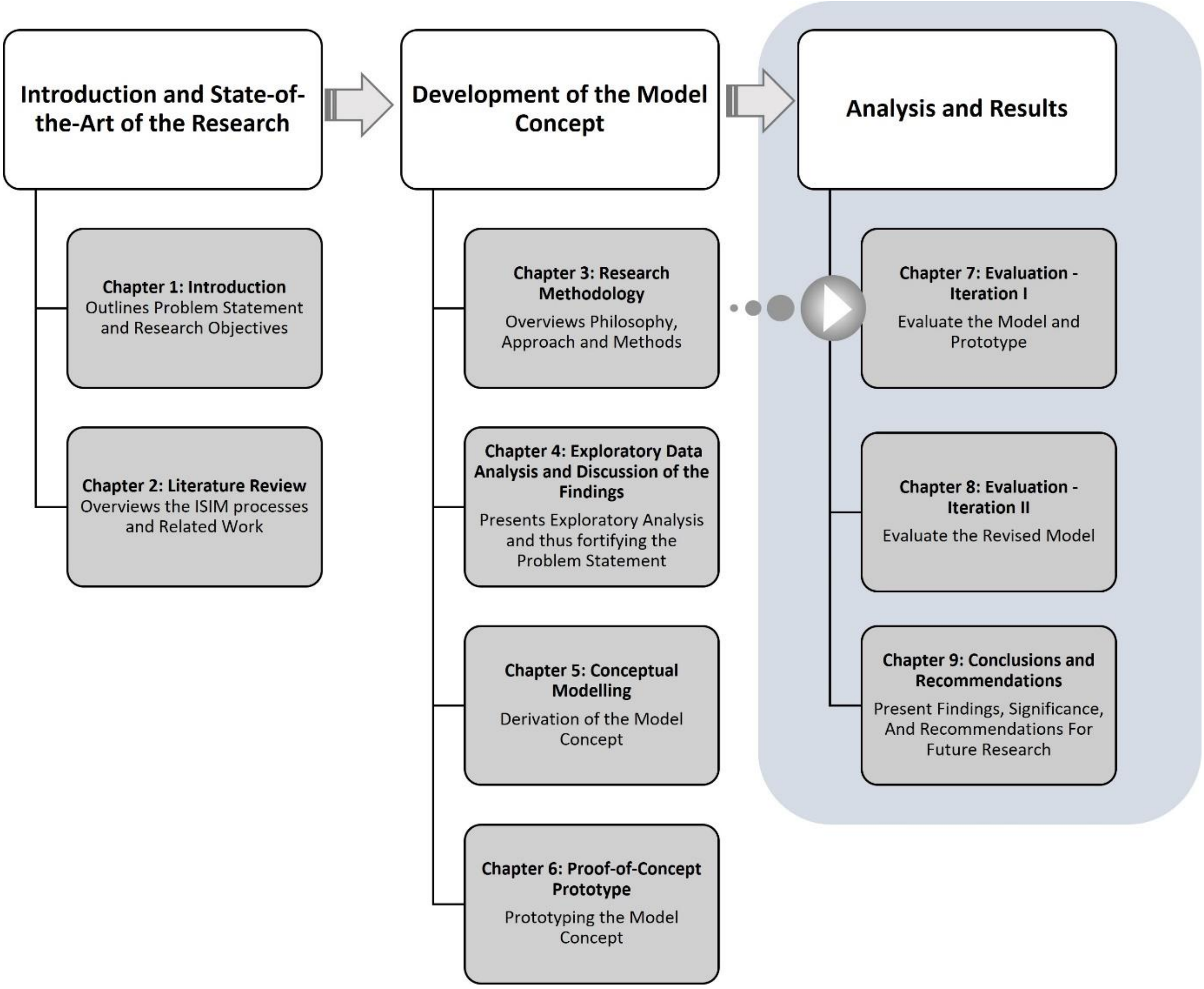
The interface prototype did not demonstrate all the functionality of the model. The prototype incorporated the main elements from the model and those aspects that are related to the core aims of the research. The encoding and decoding of the communication protocols were not fully explicated as some processes are internal to the user and there would be several interactions between all information provided and the user's final report. The prototype simply demonstrated the initial capturing, but the user is expected to incorporate the information from the comprehension screen for the final report. However, end-users may perform a projection after capturing the initial report. The interface prototype did not use real data for its implementation. Most of the data was hard coded. The prototype was tested using sample data and not actual organisational data. Only a limited subset of ISIM processes were considered.

6.9. Chapter Summary

This chapter demonstrated and illustrated an interface prototype with limited functionality as a proof-of-concept of the conceptual model derived in Chapter 5. The prototype demonstrated how awareness efforts can be coordinated to improve communication. The simulated prototype demonstrated how the components of individual, shared and role-based situational awareness may possibly work in collaboration for supporting the processes of ISIM. Chapter 7 discusses the evaluation of the model and prototype.

CHAPTER SEVEN

RESEARCH ROAD MAP


Introduction and State-of-the-Art of the Research
Chapter 1: Introduction
Outlines Problem Statement and Research Objectives
Chapter 2: Literature Review
Overviews the ISIM processes and Related Work
Development of the Model Concept
Chapter 3: Research Methodology
Overviews Philosophy, Approach and Methods
Chapter 4: Exploratory Data Analysis and Discussion of the Findings
Presents Exploratory Analysis and thus fortifying the Problem Statement
Chapter 5: Conceptual Modelling
Derivation of the Model Concept
Chapter 6: Proof-of-Concept Prototype
Prototyping the Model Concept
Analysis and Results
Chapter 7: Evaluation - Iteration I
Evaluate the Model and Prototype
Chapter 8: Evaluation - Iteration II
Evaluate the Revised Model
Chapter 9: Conclusions and Recommendations
Present Findings, Significance, And Recommendations For Future Research

CHAPTER 7: EVALUATION – ITERATION I

7.1. Introduction

This chapter considers the evaluation step of the Design Science Research (DSR) methodology. The aim of this chapter is to evaluate the model concept (Chapter 5) and the proof-of-concept prototype (Chapter 6). The evaluation of the model is conducted over two iterations. Iteration I was conducted among end-users and information security experts (some of them working in expertise managerial positions) while Iteration II involves information security experts only. This chapter will present the results of the first iteration, which involved surveying end-users and security experts who were purposively sampled. An overview of the instrument used for the evaluation which was discussed in detail in Chapter 4 is presented in Section 7.2.

The sampling frame for the evaluation and the analysis of the data is presented in Section 7.3 and Section 7.4 respectively. Both descriptive and inferential statistics were presented while the qualitative data was analysed thematically using Atlas ti.

Section 7.5 presents the correlation between the variables for further inspection of the constructs. Section 7.6 considers the recommended revisions by the participants while Section 7.7 discusses the results. The validity and reliability measures, ethical procedures, and the concluding remarks are presented in Section 7.8, Section 7.9, and Section 7.10 respectively.

7.2. Instrumentation

The instrument used for the evaluation (Appendix B) comprised three sections.

- Section I – captured biographical data (such as age, experience, job category and gender).
- Section II – captured model acceptance based on the Technology Acceptance Model (TAM) using a Likert scale (from 1-5 (Strongly Disagree to Strongly Agree)).
- Section III – captured data related to the model validity and reliability.

Sections I and II were completed by all users (both end-users and expert users). Section III (model validity and reliability) was specifically completed by expert users only as it is directly related to evaluating system applicability and benefit which requires an advanced level of understanding technical requirements – applicability and usability.

7.3. Sample

A purposive sampling strategy was used to select five Ethiopian organisations (n = 5). The organisations were selected based on various criteria: (i) probable vulnerability to information security incidents, (ii) managing large data sets, (iii) engagement with ISIM and (iv) proximity to the research context (i.e., Ethiopian organisations). The invitation for evaluation of the model was sent to forty purposively selected potential respondents. A sample of thirty-seven respondents participated in the evaluation. Thus, the response rate was 92.5%. The actual sample involved in the evaluation consisted of twenty-eight end-users (n=28) and nine information security experts (n=9).

7.3.1. Background of Participating Organisations

The participating organisations were representative of several domains – Banking, Information Technology (IT), Telecom and Regulatory Bodies. The following section concisely describes the nature of the organisations involved in the evaluation survey. (Note the superscript **2** denotes the organisations who participated in Phase II).

Organisation A^2

Organisation A^2 is a government-based institution which has been provisioning banking and financial services for the public and governmental institutions for more than 60 years. The organisation is reliant on a customised information security system to manage and control its data and informational assets.

Organisation B^2

Organisation B^2 is a private company with more than 100 employees in the ICT sector. The organisation is involved in the delivery of hardware and software applications to its clientele. In addition, the organisation has introduced various information security tools and products for its establishment and for the market. As a software company, the organisation can potentially be involved in information security aspects directly or indirectly.

Organisation C^2

Organisation C^2 is a telecom corporate owned by government and has been involved in the provision of telephone and internet services throughout Ethiopia for many years. The company has a large customer base including organisational subscribers and typically deals with large volumes of information security data or metadata.

Organisation D^2

Organisation D^2 is a private commercial organisation which is involved in the banking sector. The company has been providing financial and insurance services for several years. The company has also introduced contemporary Information Communication Technology (ICT) facilities to achieve its goals. The organisation recruits specialised human resources related to ICT and communication to manage its business. As a private financial organisation and with a large customer base, the organisation is vulnerable to information security incidents.

Organisation E^2

Organisation E^2 is a state-based security agency that has been working in controlling and safeguarding the national information security issues within Ethiopia. The organisation is mandated to formulate policies and to guide organisations (both government and private) in their application of information security controls and policies.

Table 7-1 summarises the profile of the organisations involved in the evaluation survey.

Table 7-1: Profile of Participating Organisations

Organisation	Sector	Sample (Security Expert)	Sample (End-User)	Total Participants
Organisation A^2	Government	2	6	8
Organisation B^2	Private	2	5	7
Organisation C^2	Corporate by Government	2	6	8
Organisation D^2	Private	1	5	6
Organisation E^2	Security Agency	2	6	8
	Total	**9**	**28**	**37**

7.3.2. Profile of the Participants

Table 7-2 summarises the profile of the respondents that participated in the evaluation survey.

Table 7-2: Profile of Participants

No	Item	Category	Frequency	Percentage (%)
1	Gender	Male	22	59.5
		Female	15	40.5
2	Job Category	End-User	28	75.7
		IT Security Manager	6	16.2
		IT Security Administrator	2	5.4
		IT Security Auditor	1	2.7
3	Age	18-25	3	8.1
		26-30	27	72.9
		=>31	7	18.9
4	Experience (Years)	1-3	8	21.6
		4-7	22	59.4
		>=8	7	18.9
5	Country	Ethiopia	37	100%

Table 7-2 depicts the demographic characteristics of the participants involved in the study. In the study, 59.5% of the participants were male, and 40.5% of the participants were female. The job categories are from diverse professions that are described in detail below. The ages in years ranged as follows: 18-25 years (8.1 %), 26-30 (72.9 %) and 31 and older (18.9 %). Thus, the majority of participants are between the ages of 26 and 30. Regarding their job experience, 21.6% have 1 to 3 years of experience, 59.4% of them have from 4 to 7 years of experience and 18.9% have more than 8 years of experience. The majority of the participants' job experience is between 4 and 7 years. Finally, all the participants involved in the study were from Ethiopian organisations.

By design, the majority of participants were end-users (75.7%). The expert users who were involved in the evaluation survey encompassed information security managers (16.2%), information security administrators (5.4%) and information security auditors (2.7%). One of the respondents selected the "other" choice, however, this individual's job title was 'ICT Manager' which involves the role of 'Information Security Manager'. Therefore, this participant was categorised as an 'Information Security Manager' for the purposes of this analysis. Figure 7-1 shows the job categories of respondents who participated in the evaluation of the model and the prototype.

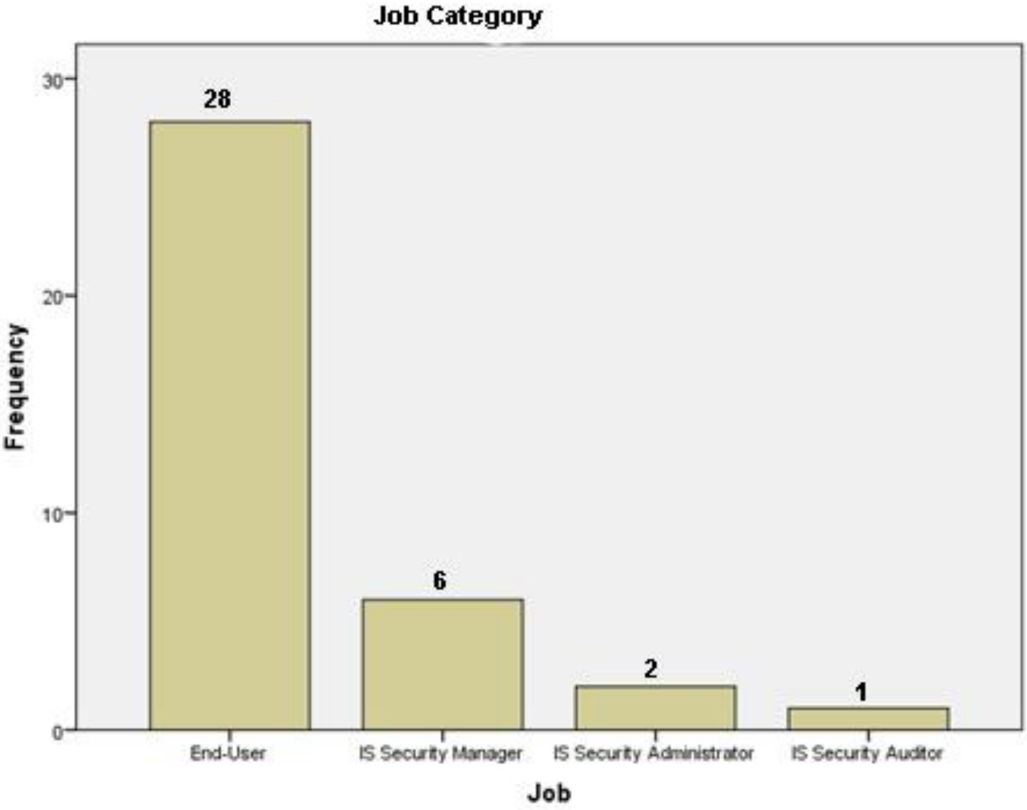


Figure 7-1: Job Categories of Participants

7.4. Data Analysis

The quantitative data was analysed using descriptive and inferential statistics. All the quantitative data analysis was analysed using SPSS (Statistical Package for Social Sciences)-Version 22 tool. The quantitative data was analysed according to the thematic construct of the study. The theme is categorised into two parts: model acceptance and model validity and reliability. Section 7.4.1 describes the analysis of model acceptance and Section 7.4.2 discusses the model validity and reliability. (A link to the redacted raw data is referenced in Appendix G.)

7.4.1. Model Acceptance

There are four constructs that were espoused to analyse the model and prototype: ‘Intent to use’, ‘Perceived usefulness’, ‘Ease of use’ and ‘Compatibility and Scalability’. Descriptive statistics were applied to analyse and provide statistical explanations for the questions for each construct. The questionnaire for this part was distributed to both information security experts and end-users. Table 7-3 summarises the descriptive statistics (i.e., mean, standard deviation, minimum and maximum) of the results for all respondents (n=37).

Table 7-3: Descriptive Statistics of the Constructs

Question number	Item	N	Minimum	Maximum	Mean	Std. Deviation
Question # 1	Intent to Use Q1	37	2	5	4.00	.850
Question # 2	Intent to Use Q2	37	2	5	3.89	.875
Question # 3	Intent to Use Q3	37	2	5	3.89	.906
Question # 4	Perceived Usefulness Q1	37	2	5	4.00	.913
Question # 5	Perceived Usefulness Q2	37	2	5	4.03	.866
Question # 6	Perceived Usefulness Q3	37	2	5	4.00	.943
Question # 7	Ease of Use Q1	37	2	5	4.00	.943
Question # 8	Ease of Use Q2	37	2	5	3.95	.911
Question # 9	Ease of Use Q3	37	1	5	3.86	1.032
Question # 10	Compatibility and Scalability Q1	37	1	5	3.97	.986
Question # 11	Compatibility and Scalability Q2	37	1	5	3.92	.983
	Valid N (listwise)	37				

According to the statistics, the table shows that the mean values for all the questions are above 3.8, which indicates that there is a positive acceptability response for the model and prototype. The details of the questions and acceptability responses are shown in this section. The data was also analysed for correlations between the control variables such as age, experience, job category and gender across the constructs of intent to use, perceived usefulness, ease of use and compatibility and scalability. The Spearman's test was conducted to test correlation of variables. The statistical results do not show significant value with a p-value for all the tests which was not significant (p-value much higher than 0.05). For instance, Table 7-4, Table 7-5 and Table 7-6 show the correlation statistics of intention to use of the system with job category, age and experience respectively. Thus, there exists no statistically significant correlation between intent to use of the system and other factors such as age, experience, and job category of the respondents.

Table 7-4: Analytical Statistics between Intention to Use of a System and Job Categories

Correlations				
			Job	Intenttotal
Spearman's rho	Job	Correlation Coefficient	1.000	-.085
		Sig. (2-tailed)	.	.618
		N	37	37
	Intenttotal	Correlation Coefficient	-.085	1.000
		Sig. (2-tailed)	.618	.
		N	37	37

Abbreviation: Intention to Use (Intenttotal)

Table 7-5 shows the insignificant correlations between intent to use and age of the respondents.

Table 7-5: Analytical Statistics between Intent to Use of a system and Age

Correlations				
			Age	Intenttotal
Spearman's rho	Age	Correlation Coefficient	1.000	-.007
		Sig. (2-tailed)	.	.967
		N	37	37
	Intenttotal	Correlation Coefficient	-.007	1.000
		Sig. (2-tailed)	.967	.
		N	37	37

Abbreviation: Intention to Use (Intenttotal)

Table 7-6 shows the insignificant correlations between the intent to use and the experience of the respondents.

Table 7-6: Analytical Statistics between Intent to Use of a System and User Experience

Correlations				
			Experience	Intenttotal
Spearman's rho	Experience	Correlation Coefficient	1.000	.022
		Sig. (2-tailed)	.	.899
		N	37	37
	Intenttotal	Correlation Coefficient	.022	1.000
		Sig. (2-tailed)	.899	.
		N	37	37

Abbreviation: Intention to Use (Intenttotal)

A similar insignificant statistical figure is also identified for perceived usefulness, and ease of use of the system across different variables such as age, gender, job category and experience. Table 7-7 shows the descriptive statistics of ‘model acceptance’ by expert users. Since the minimum value is 2 and the maximum value is 5, the mean value for expert users is also above 3.7, that indicates higher levels of acceptability.

Table 7-7: Model Acceptance by Expert Users

	N	Minimum	Maximum	Mean	Std. Deviation
Age	9	28	40	32.56	3.609
Experience	9	6	12	9.56	2.007
Intent1	9	2	5	3.78	.972
Intent2	9	2	5	3.78	.972
Intent3	9	2	5	3.78	.972
Perceive1	9	2	5	3.89	1.054
Perceive2	9	2	5	3.78	.972
Perceive3	9	2	5	3.89	1.054
Ease1	9	2	5	3.89	1.054
Ease2	9	2	5	3.78	.972
Ease3	9	2	5	3.78	.972
Compscale1	9	2	5	3.78	.972
Compscale2	9	2	5	3.78	.972
Valid N (listwise)	9				

Abbreviation: Intent to Use (Intent1, Intent2, Intent3), Perceived Usefulness (Perceive1, Perceive2, Perceive3), Ease of Use (Ease1, Ease2, Ease3), Compatibility and Scalability (Compscale1, Compscale2)

Intent to Use

There were three questions raised with respect to the Intent to Use construct:

- Intent to use Question 1 (IUQ1): "*Assuming I had access to a system similar to the prototype, I intend to use it in an incident response scenario to assist in the coordination of communication and awareness efforts with respect to responding and resolving information security incidents".*

- Intent to use Question 2 (IUQ2): *"Assuming I had access to a system similar to the prototype, I intend to use it to enhance my awareness about organisational information security incidents".*

- Intent to use Question 3 (IUQ3): "*Given that I had access to the system, I predict that I would use the system of communication and awareness towards achieving collaborative and proactive information security incident reporting".*

The analysis of the Intent to Use construct is summarised in Table 7-8.

Table 7-8: Statistical Analysis of Intent to Use

Question Code	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
IUQ1	0	2 (5.4%)	7 (18.9%)	17 (45.9%)	11 (29.7%)	37 (100%)
IUQ2	0	3 (8.1%)	7 (18.9%)	18 (48.6%)	9 (24.3%)	37 (100%)
IUQ3	0	3 (8.1%)	8 (21.6%)	16 (43.2%)	10 (27%)	37 (100%)

Abbreviation: Intent to Use Question 1 (IUQ1), Intent to Use Question 2 (IUQ2), Intent to Use Question 3 (IUQ3)

In response to Question #1 (IUQ1), most of the participants (75.6%; n=28) (i.e., an aggregation of strongly agree and agree responses), indicated a positive intention to use the system in an incident response scenario to assist in the coordination of communication and awareness efforts with respect to responding and resolving information security incidents.

Cases in point:

> *"I will use definitely the system (prototype) to help me in communication of incidents"*
>
> [Participant C#9, End-User]
>
> "*The post incident report patterns indicate better predication [sic]"*
>
> [Participant C#23, End-user]
>
> *"The communication or reporting of incident information in our company enables us for response and user help from various customers"*
>
> [Participant C#13, End-user]

A validation for using a system similar to the prototype was raised by a few respondents. This included improved incident data regarding previous incidents and future incidents. Cases in point:

> *"One of the serious problems in incident management is lack of documentation about previous incidents and the prototype is very useful in that aspect"*
>
> [Participant C#29, Expert user]

> *"Our customers are various so the digital archive and predication [sic] would help use in estimating emerging threats"*

[Participant C#13, End-user]

Some aversion to the intention to use the system similar to the prototype was also raised such as sharing sensitive information which may be classified, the high complexity of the system, requirement for more contextual data such as categories and the need for system integration. Cases in point:

> *"Some of the classified sensitive incident information, as [the] security agency requires [the data to be] undisclosed to all users"*

[Participant C#36, Expert user]

> *"The conceptual model is complex for me, but the prototype likely enables incident reporting"*

[Participant C#11, End-user]

> *"As telecom security helpdesk, such systems would help us in coordinating incoming security incident data but its management requires more categories"*

[Participant C#8, End-user]

> *"Yes, I intend to use it. But if it has to be integrated with the system of the organisation"*

[Participant C#33, Expert user]

> *"It will be good if such systems will be integrated to our organisation using our system login so that we can update ourselves about information security incident cases of our organisation"*

[Participant C#3, End-user]

Intent to Use Q2

In response to Question #2 (IUQ2), most of the participants (72.9%; n=27) (i.e., an aggregation of strongly agree and agree responses) indicated that they intend to use the prototype to enhance their awareness about organisational information security incidents.

Some respondents remarked positively about their intention to use the simulated system. Cases in point:

> *"The system seems help in raising awareness about information security incidents"*
>
> [Participant C#1, End-user]

> *"The system is good towards raising awareness of information security incident rather than resolving"*
>
> [Participant C#4, End-user]

> *"The use of such systems besides the manual means of awareness could enable engagement"*
>
> [Participant C#14, End-user]

Some participants had the following caveats to the use of the prototype such as the requirement for customisation or contextualisation, integration, policy, and security compliance. Cases in point:

> *"Our data systems and internet security is [sic] faced with information security threats. However, i believe that it will be good also if it can be customized to unique organisational security settings"*
>
> [Participant C#8, End-user]

> *"This systems seems separate from organisational systems. I may use the system in case if it is integrated to our organisational system"*
>
> [Participant C#7, End-user]

> *"I will use it but it depends on my organisational policy and compliance to security features"*

[Participant C#12, End-user]

> *"The security incident management system is applicable given the contextual information of organisations,*

[Participant C #10, End-user]

Intent to Use Q3

In response to Question #3 (IUQ3), most of the participants (70.2%; n=26) (i.e., an aggregation of strongly agree and agree responses) indicated positively that they predict that they would use the system of communication and awareness towards achieving collaborative and proactive information security incident reporting.

Cases in point:

"Our customers are various so the digital archive and predication would help use in estimating emerging threats"

[Participant C#13, End-user]

"The division of levels such as individual, shared and expert can enhance professional collaboration"

[Participant C#14, End-user]

Some suggestions raised by the information security experts consist of the inclusion of alerting mechanisms and clustering incident information according to security policies. Case in point:

> *"Proactive incident requires also alerting mechanism in critical conditions"*

[Participant C#37, Expert user]

Besides the proactive nature of incidents, one user also indicated that the categorisation of information security incidents should be based on organisational security polices and directives.

> *“Categorization of incident into different cluster should be inline with* organisational *security policies”*

[Participant C#36, Expert user]

One limitation raised against the value of the proposed system is the lack of prediction of unanticipated incidents. Cases in point:

> *“The system may not necessarily be proactive in that some of the information security threats may not be anticipated earlier”*

[Participant C#32, Expert user].

> *“For the available incident information, it is possible to know its prediction. But for unknown incident proactive reporting could not be achieved”*

[Participant C#17, End-user]

Some respondents raised concerns regarding the value of the proposed system under specific circumstances. First the issue of unreported incidents (Participant C#18) will be problematic for management. Second the usefulness of a proposed system without a supporting helpdesk (Participant C#22) as the proposed system will require adequate support, Third, a collaborative system across several branches may be challenging (Participant. C#27) to manage.

Cases in point:

> *“How the management know if there are unreported incidents”*

[Participant C#18, End-user]

> *“A dedicated service desk is required to organize such task”*

[Participant C#22, End-user]

> *"Collaboration in organisations having many branches such as regions may be difficult using intranet"*
>
> [Participant C#27, End-user]

Perceived Usefulness

Three questions were raised with respect to the Perceived Usefulness construct:

- Perceived Usefulness Question 1 (PUQ1): *"Using a system based on the model concept will increase my effectiveness in reporting an information security incident"*.
- Perceived Usefulness Question 2 (PUQ1): *"I would find a system based on the model concept useful towards achieving a shared, interactive and participatory platform for the coordination and management of information security incidents"*.
- Perceived Usefulness Question 3 (PUQ3): *"I would find a system based on the model concept valuable towards enhancing my effectiveness in an incident response scenario by maximising the coordination of communication and awareness efforts with respect to information security incidents"*.

The analysis of the Perceived Usefulness construct is summarised in Table 7-9.

Table 7-9: Statistical Analysis of Perceived Usefulness

Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
PUQ1	0	3 (8.1%)	6 (16.2%)	16 (43.2%)	12 (32.4%)	37 (100%)
PUQ2	0	2 (5.4%)	7 (18.9%)	16 (43.2%)	12 (32.4%)	37 (100%)
PUQ3	0	3 (8.1%)	7 (18.9%)	14 (37.8%)	13 (35.1%)	37 (100%)

Abbreviation: Perceived Usefulness Question 1 (PUQ1), Perceived Usefulness Question 2 (PUQ2), Perceived Usefulness Question 3 (PUQ3)

Perceived Usefulness Q1

In response to Question #4 (PUQ1), most of the participants (75.6%; n=28) (i.e., an aggregation of strongly agree and agree responses), indicated positively that using a system based on the model concept will increase their effectiveness in reporting an information security incident. Cases in point:

"This model system can be utilized to achieve best reporting for incident management"

[Participant C#31, Expert user]

"Information security severity rating or graph helps to use for better understanding"

[Participant C#22, End-user]

Some concerns that were raised with respect to the perceived usefulness include the threat of internal users, the need for the integration of additional technical mechanisms, the sensitivity of national threats, and the need to have awareness of past incident information. Cases in point:

> *"Effectiveness of reporting not necessarily achieved though this system. Other electronic reporting schemes could be integrated"*

[Participant C#37, Expert user]

> *"Internal and external staff/employee should be identified as some insiders could compromise the system"*

[Participant C#36, Expert user]

> *"The reporting function alone cannot achieve effectiveness unless integrated to technical means"*

[Participant C#28, End-user]

> *"Some of the national security threats are sometimes problematic to report in this platform"*

[Participant C#11, End-user]

> *"The effectiveness of information security incident depends on my previous awareness and lesson I got from my staff and colleagues"*

[Participant C#3, End-user]

One end-user raised an important caveat to the usefulness of the proposed system that it is dependent on adaption and use:

> *"The effectiveness of the system depends on organisational adaption and use"*
>
> [Participant C#26, End-user]

Perceived Usefulness Q2

In response to Question #5 (PUQ2), most of the participants (75.6%; n=28) (i.e., an aggregation of strongly agree and agree responses), indicated that they found a system based on the model concept useful towards achieving an interactive and participatory platform for the coordination and management of information security incidents.

Cases in point:

> *"The shared and participatory approach [sic] of users is important in organisational setup for achieving common understanding about information security threats"*
>
> [Participant C#4, End-user]

> *"Multiple communication channels could also enhance the awareness besides the digital means of communication"*
>
> [Participant C#36, Expert user]

Issues such as staff turnover may hinder shared understanding and prejudice the shared approach. A case in point:

> *"As most staff shift organisations so frequently, shared approach in incident management takes time but can serve as start-up [sic]"*
>
> [Participant C#37, Expert user]

Other respondents (end-users) also raised important complementary strategies to enhance the usefulness of the system concept such as the need for staff training, and policy and compliance integration. Cases in point:

> *"The system would be more crucial for users to be provided training before they start [sic] job"*

[Participant C#4, End-user]

> *"I believe that it should be approved and streamlined into the policy of the organisation"*

[Participant C#9, End-user]

> *"The compliance section of our organisation can use this as its mandatory for its effective use"*

[Participant C #25, End-user].

Perceived Usefulness Q3

In response to Question #6 (PUQ3), most of the participants (73%; n=27) (i.e., an aggregation of strongly agree and agree responses), indicated that they would find a system based on the model concept valuable towards enhancing their effectiveness in an incident response scenario by maximising the coordination of communication and awareness efforts with respect to information security incidents. A case in point:

> *"The application of the system could help in organisational information security compliance"*

[Participant C#13, End-user]

There are some relevant concerns that were raised by the respondents which included the problem of negligent insiders and the lack of time to effectively use a system of this calibre. Cases in point:

> *"Some employees are negligent towards dedicated use of such systems. It requires collaboration with compliance, law and cyber response teams"*

[Participant C#36, Expert user]

> *"Considering many business hours of organisations , they may not have time to use such systems by quitting business tasks"*

[Participant C#37, Expert user]

One end-user emphasised that these types of systems must be aligned with information security policies to be effective. Case in point:

> *"Integration of such system with operational security policies will support for effective reporting"*

[Participant C#20, End-user]

A caveat to the use of the proposed system reiterated the issue of managing highly sensitive incident information which could compromise an organisation. Case in point:

> *"I believe that not all organisational security incidents should be reported"*

[Participant C#11, End-user]

Ease of Use

Regarding the Ease of Use construct, there were three questions raised:

- Ease of Use Question 1 (EOUQ1): *"I would find a system based on the model concept easy to use in an incident response scenario."*

- Ease of Use Question 2 (EOUQ2): *"Interacting with the system will not require huge mental effort."*

- Ease of Use Question 3 (EOUQ3): *"My interaction with a system based on the model concept will enable a shared mental model of an information security incident thereby easing the incident management process."*

The analysis of the Ease of Use construct is summarised in Table 7-10.

Table 7-10: Statistical Analysis of Ease of Use

Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
EOUQ1	0	3 (8.1%)	7 (18.9%)	14 (37.8%)	13 (35.1%)	37 (100%)
EOUQ2	0	3 (8.1%)	7 (18.9%)	16 (43.2%)	11 (29.7%)	37 (100%)
EOUQ3	1	3 (8.1%)	7 (18.9%)	15 (40.5%)	11 (29.7%)	37 (100%)

Abbreviation: Ease of Use Question 1 (EOUQ1), Ease of Use Question 2 (EOUQ2), Ease of Use Question 3 (EOUQ3)

Ease of Use Q1

In response to Question #7 (EOUQ1), most of the participants (73%; n=27) (i.e., an aggregation of strongly agree and agree responses), indicated that they would find a system based on the model concept easy to use in an incident response scenario. There were some concerns raised around the technical complexity of the proposed concept. However, some suggestions to increase the understandability of the technical facets included training and a consideration of local languages in the implementation. Cases in point:

> *"Some of the technical security features may not be understood by normal or end-users. It requires integration with technical issues and follow up training for end-users"*
>
> [Participant C#36, Expert user]

> *"It would be more easy [sic] if it can be available in local language"*
>
> [Participant C#18, End-user]

> *"Follow up training of updates requires for easy use"*
>
> [Participant C#24, End-user]

> *"The system is user-friendly but some of the technical event words and categories requires some explanation or contextual meaning"*
>
> [Participant C#37, Expert user]

> *“Some of the incident parameters look like difficult [sic] for ordinary users to recognize”*

[Participant C#8, End-user]

Ease of Use Q2

In response to Question #8 (EOUQ2), most of the participants (72.9 %; n=27) (i.e., an aggregation of strongly agree and agree responses) indicated that interacting with the system will not require a huge mental effort. Case in point:

> *“Engaging with the system is not that much difficult”*

[Participant C#7, End-user]

However, the respondents raised their concerns on the potential usage of the system in terms of technical complexity. Training was offered as a suggestion to improve the understandability of the technical facets. Cases in point:

> *“Interacting with the system is easy but users may not know their IP address or may change with time”*

[Participant C#34, Expert user]

> *“Some users in organisations may not recognize the technical terms such as ip address of incident unless they got pre training”*

[Participant C#10, End-user]

> *“New staff could be recruited without adequate experience. So it may be difficult to introduce to some of the jargons . so requires training”*

[Participant C#37, Expert user]

There were some caveats to the use of the proposed system. There must be enforcing mechanisms and knowledge of incidents to encourage use of the system.

Cases in point:

> *"User may not use the system unless some form of enforcing mechanism is in place"*

[Participant C#13, End-user]

> *"The system requires to some extent familiarity for emerging incidents and its change of system"*

[Participant C#25, End-user]

Ease of Use Q3

In response to Question #9 (EOUQ3), most of the participants (70.2%; n=26) (i.e., an aggregation of strongly agree and agree responses) indicated that their interaction with a system based on the model concept will enable a shared mental model of an information security incident thereby easing the incident management process. A case in point:

> *"Risk determining indicators could be useful for some unforeseen incidents"*

[Participant C#36, Expert user].

Some of the issues raised included disclosure of sensitive information which may compromise the privacy and increase susceptibility of the organisation to threats. Further sharing information could become a burden to the organisation. Cases in point:

> *"Conceptually the system attempts to [a] share mental model but communicating such information with customers is extra burden or task"*

[Participant C#37, Expert user]

> *"Disclosure of classified incident information to other users may [be a] risk for unintended purposes"*

[Participant C#15, End-user].

> *"Easy cohesion of incident information in [a] shared environment may be susceptible for unintended use"*

[Participant C#17, End-user]

Compatibility and Scalability

With respect to the Compatibility and Scalability construct, there were two questions raised:

- Compatibility and Scalability Question 1 (CSQ1): *"Using the system would be compatible with my own existing organisational system design".*
- Compatibility and Scalability Question 2 (CSQ1): *"If the system is scalable, it will potentially be used by many users on a wider scale in an incident response scenario".*

The analysis of the Compatibility and Scalability construct is summarised in Table 7-11.

Table 7-11: Statistical Analysis of Compatibility and Scalability

Question	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**Total**
CSQ1	1 (2.7%)	2 (5.4%)	6 (16.2%)	16 (43.2%)	12 (32.4%)	37 (100%)
CSQ2	1 (2.7%)	2 (5.4%)	7 (18.9)	16 (43.2%)	11 (29.7%)	37 (100%)

Abbreviation: Compatibility and Scalability Question 1 (CSQ1), Compatibility and Scalability Question 2 (CSQ2)

Compatibility and Scalability Q1

In response to Question #10 (CSQ1), most of the participants (75.6%; n=28) (i.e., an aggregation of strongly agree and agree responses) indicated that using the system would be compatible with their own existing organisational system design. Cases in point:

> *"Most of our systems has been online, so I think it could be compatible"*

[Participant C#7, End-user]

> *"I think such systems can work together with other similar platforms"*

[Participant C#20, End-user]

Concerns of compatibility issues were also raised in relation to existing systems. There could be issues with internal system customisation. A case in point:

> *"We have our own internal security reporting system (CERT). So it may not be compatible with that"*
>
> [Participant C#37, Expert-user]

Two respondents referred to the fact that the system needs to be secure. Perhaps the system may be hosted on an intranet server behind a firewall to provide security and privacy. Cases in point:

> *"Such incident system requires strong protection. It could be part of organizational existing strong system"*
>
> [Participant C#36, Expert user]

> *"My organization currently does not have such systems but it will be useful if the bank has introduced intranet systems for such purpose"*
>
> [Participant C#1, End-user]

Compatibility and Scalability Q2

In response to Question #11 (CSQ2), most of the participants (73%; n=27) (i.e., an aggregation of strongly agree and agree responses) of the participants indicated that if the system is scalable, it will potentially be used by many users on a wider scale in an incident response scenario. Cases in point:

> *"It will be useful more if the system can be available in all branches in networked manner such as core-banking system [sic]"*
>
> [Participant C#4, End-user]

> *"I think the model can be scalable to be used in different branches of our organisation"*
>
> [Participant C#32, Expert user]

> *"It can be scalable also to incorporate long time data as an archive in larger organisations as incident data increases"*

[Participant C#36, Expert user]

Issues of variation in requirement needs was raised as a concern. Cases in point:

> *"Many users these days are interested to be aware [sic] about cyber incident in their organisation. However, it will be good if it can be customized specific to organisational context"*

[Participant C#1, End-user].

> *"Different organisations have their own preference of security incident management. So it requires their strategic decision and contextual security police line up"*.

[Participant C#37, Expert user]

Two end-users proffered good suggestions to improve the effectiveness of the model concept. First progressive scalability and integration. Second integration with national systems which could further enhance incident awareness. Cases in point:

> *"The scalability of such system would be effective if it will be in progressive manner"*

[Participant C#15, End-user]

> *"It will be also good if there will be any room to integrate and work with the national security management for better incident awareness"*

[Participant C#5, End-user]

7.4.2. Model Validity and Reliability

Section III of the questionnaire was completed by respondents from the expert groups (n=9) in organisations. The constructs in this section of evaluation include:

- Abstraction: "*Do you think that the model concept (the application of situational awareness and the Interactive Communication Model) can conceptually resolve the problems associated with the poor coordination of awareness and communication of security incidents?"*

- Originality: *"Is the model concept unique in its aim of integrating situational awareness and communication models for easing the coordination of incident related security problems?"*

- Justification*: "Is the model concept justified in a comprehensible manner in the approach for the coordination of communication and awareness efforts in information security management?"*

- Benefit: *"Will the model concept benefit organisations in the coordination of communication and awareness efforts in information security management?"* and *"Does the implementation of such a model concept outweigh the cost of its deployment compared to the risks of contemporary information security threats?"*

Abstraction

In response to Question #12 (77.8%, n = 7), most of the experts indicated that the model concept can conceptually resolve the problems associated with the poor coordination of awareness and communication of security incidents. Only two respondents indicated that the applications of the model would not resolve the problem of coordination and awareness of security incidents. Figure 7-2 (pie chart) demonstrates the responses.

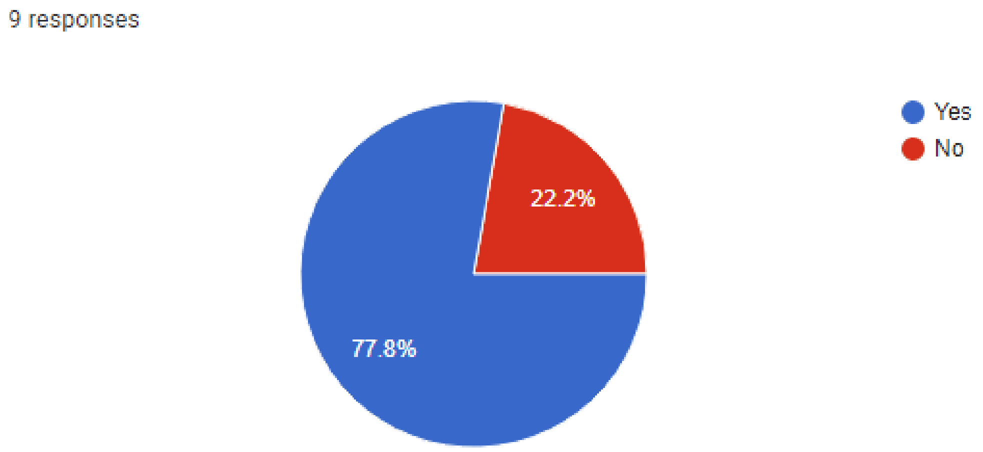


Figure 7-2: Responses for the Abstraction Item (Iteration I)

Respondents highlighted the contribution of the model in terms of the framing (i.e., the situational awareness model and Interactive Model of Communication (IMC)), remarking on the importance of documentation, lesson learning, analysis, training, archiving, trend analysis, forecasting and reporting. Cases in point:

> *"The model and system, besides awareness raising, helps to document information systems security incidents that happened in the organisation. This will also is very important for lesson, doing analysis and providing training for new staff and serve as archive data for trend analysis and forecasting"*
>
> [Participant C#35, Expert user]

> *"Both concepts (situational awareness and interactive communication model) are important for solving the awareness and reporting of information security incident in organisations"*
>
> [Participant C#34, Expert user]

One expert user remarked positively in terms of the system concept addressing the human-centric challenges that beleaguer organisations. Case in point:

> *"Although some of information security challenges are associated with technical matters, this model and system, mostly resolve the human aspect of the challenges such as communication and awareness"*
>
> [Participant C#31, Expert user]

Some experts had reservations regarding the proposed system concept, on issues such as the sensitivity of incident information and the human-centeredness of the concept. Cases in point:

> *"Some of the incident information related to national threat may require some time to quarantine and analyse before communicating"*
>
> [Participant C#36, Expert user]

> *"The system may not totally solve the poor communication of incidents alone as some of the challenges are related to technical features"*
>
> [Participant C#32, Expert user]

Originality

In response to Question #13, the majority of the participants (66.7%; n=6), indicated that the model concept is unique in its aim of integrating situational awareness and communication models for easing the coordination of incident related security problems. Figure 7-3 (pie chart) demonstrates the responses.

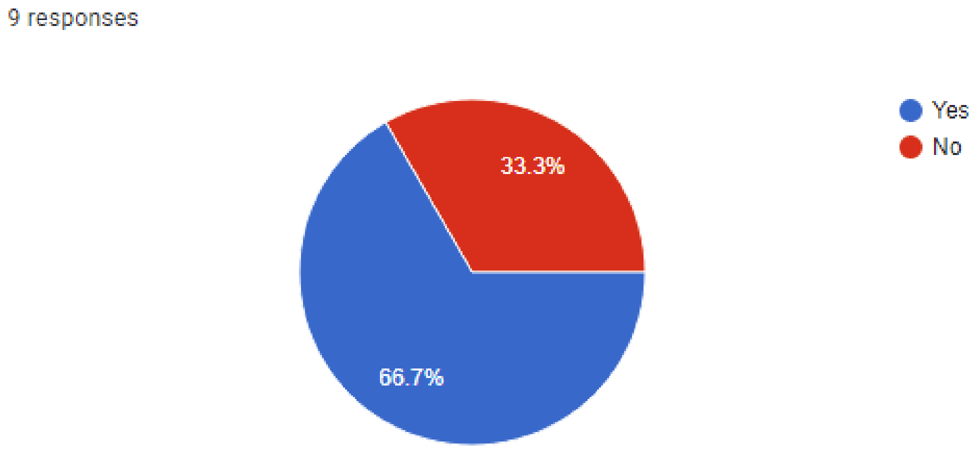


Figure 7-3: Responses for the Originality Item (Iteration I)

Cases in point:

> *"The model has come up with unique approach to show how to solve information security communication challenges"*

[Participant C#30, Expert]

> *"Although there exist some model related to this, this technically and practically have depicted how to report and raise awareness using the model"*

[Participant C#36, Expert user]

> *"The awareness aspects of security management are not new. But this system has attempted to uniquely show the practical application of communication and situational awareness in organisational context"*

[Participant C#37, Expert user]

> *"As an information security auditor, I have never seen such systems introduced in the organisations that I had worked"*

[Participant C#31, Expert user]

One respondent was doubtful about the system regarding its applicability:

> *"The model and systems seems [sic] unique but it specifically depends on organisational information security problems"*

[Participant C#35, Expert user]

Two respondents indicated that they were uncertain about the originality. Cases in point:

> *"Since I do not explore on the area, I am not sure about it"*

[Participant C#33, Expert user]

> *"Although there exist [sic] some model related to this, this technically and practically have depicted how to report and raise awareness using the model"*

[Participant C #36, Expert user]

Justification

In response to question #14 (77.8%; n =7), the majority of the participants indicated that the model concept is justified in a comprehensible manner in the approach for the coordination of communication and awareness efforts in information security management. Figure 7-4 depicts the responses.

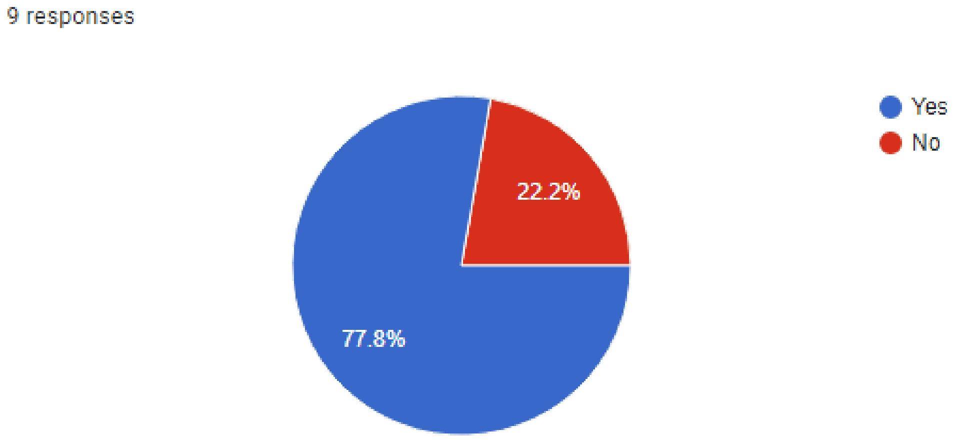


Figure 7-4: Responses for the Justification Item (Iteration I)

The participants raised some issues of concern such as the context and the need for proper training protocols. Cases in point:

> *"The model would have been more explained from contextual or existing organisational incident scenario"*
>
> [Participant C#36, Expert user]

> *"It is justifiable, but encoding or remembering IP address for normal users may be difficult unless they get some training"*
>
> [Participant C#33, Expert user]

> *"It is justifiable. But it will be also very good if it will be presented in local languages for more user to understand it and use it very easily"*
>
> [Participant C#32, Expert user]

Benefit

In response to question #15 (66.7%; n = 6), the majority of the respondents indicated that the model concept would benefit organisations in the coordination of communication and awareness efforts in information security management. Figure 7-5 demonstrates the responses.

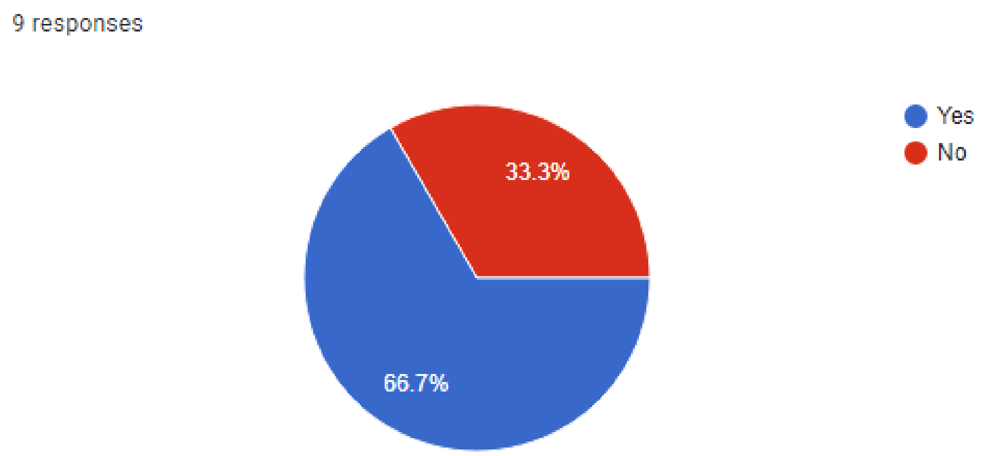


Figure 7-5: Responses for the General Benefit Item (Iteration I)

Expert users have stressed the benefit of the system in different circumstances such as in raising awareness and reporting of information security incidents. Cases in point:

> *"Organisations are very much challenged in raising awareness of users about security incidents. We usually use manual means of communication. So this system will help us to easily aware our staff [sic]"*
>
> [Participant C#31, Expert user]

> *"The model and prototype could support organisations in solving their reporting of incident information. The coordination of communication and awareness of incidents rather requires comprehensive and collaborative approach besides systems"*
>
> [Participant C#35, Expert user]

Some expert users raised concerns regarding the vulnerability of exposing incident information and the feasibility of the system concept. Cases in point:

> *"Our organisation is working to protect national security of citizens. Such systems may expose all the incident information without further analysis or impact analysis or without input from decision makers"*

[Participant C#36, Expert user]

> *"Cost-benefit analysis is required before determining the feasibility of such systems"*

[Participant C#37, Expert user]

In response to question #16 (88.9%; n = 9), the majority of the respondents indicated that the implementation of such a model concept outweighs the cost of its deployment compared to the risks of contemporary information security threats. Only one expert user selected a negative response. Figure 7-6 demonstrates the responses.

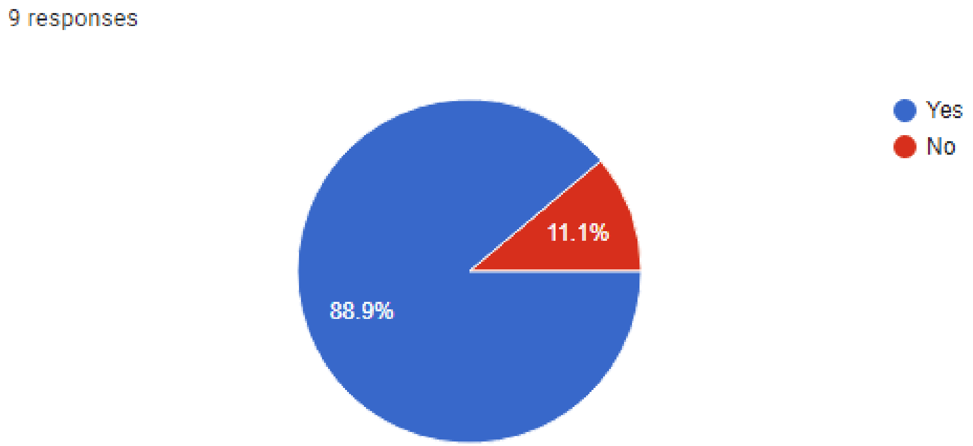


Figure 7-6: Responses for the Cost-Benefit Item (Iteration I)

Some respondents had a few caveats to the use such as concerns for the requirement of a budget for its implementation. Case in point:

> *"Compared to its benefit, the cost of the implementation is cheaper. Organisations can adequately budget for such systems"*,

[Participant C#31, Expert user]

While others also indicated uncertainty about the control of incidents, nevertheless, they stressed that the implementation of the system would improve the proactive incident management and raised the concern of cost of risk associated by publishing classified information. Cases in point:

> *"Although the control of cyber-security threats are always uncertain, the implementation of such systems could improve users awareness in proactive way which has implication in mitigating risks before its happening"*
>
> [Participant C#35, Expert user]

> *"It could be implemented but the cost could be related to the risks associated with publishing classified information"*
>
> [Participant C#36, Expert user]

One expert user also remarked about doing pre-planning, determining costs and risks associated with its implementation:

> *"Feasibility of such systems requires pre-planning, determining costs associated with risk and use",*
>
> [Participant C#37, Expert user]

7.4.3. Summative Analysis

The analytical network generated from ATLAS-ti v22. is shown in Figure 7-7. The network shows how the different thematic codes of the analysis are interrelated to each other. Different codes are generated from the qualitative data. Thus, the themes in the study are further explained in the codes which are generated from the qualitative data from the respondents.

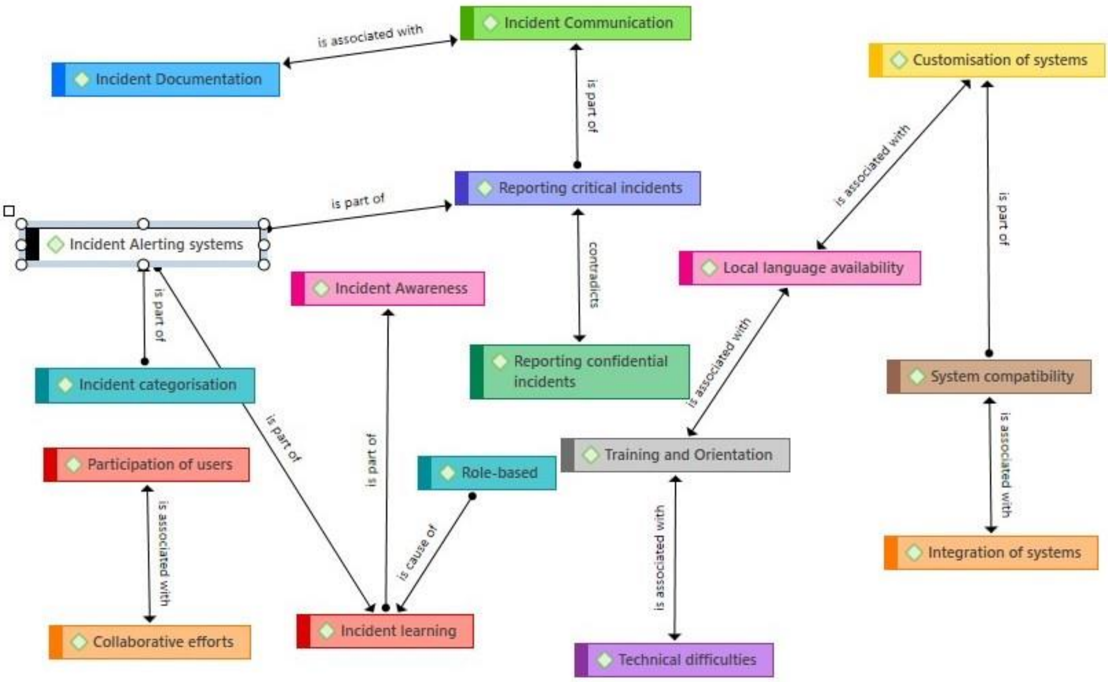


Figure 7-7: Analytical network Generated for Qualitative Data

The map demonstrates how incident communication, incident awareness, incident categorisation and incident alerting systems are related. For instance, incident alerting systems are part of the reporting of critical incidents which is addressed in this study within the scope. Although not all the recommendations in the codes are addressed in the improvements, the generated codes are depicted in the network analysis such as customisation, language aspects, training, integration, collaboration, participation of users and incident learning.

7.5. Correlations between Constructs

A Spearman's correlation test was conducted to determine if there is a relationship between the constructs. Accordingly, a strong, positive correlation exists between the different constructs, which is statistically significant. The nonparametric correlation test for association of the different constructs is shown in Table 7-12. In order to do so, the values for each question (such as Intent to Use 1, Intent to Use 2, Intent to Use 3) was transformed into new variables such as 'Intent to Use Total' to determine the overall mean. These calculations were performed for all the constructs (Perceived Usefulness, Ease of Use and Compatibility and Scalability). Then, a nonparametric correlation test was applied for its association between the constructs.

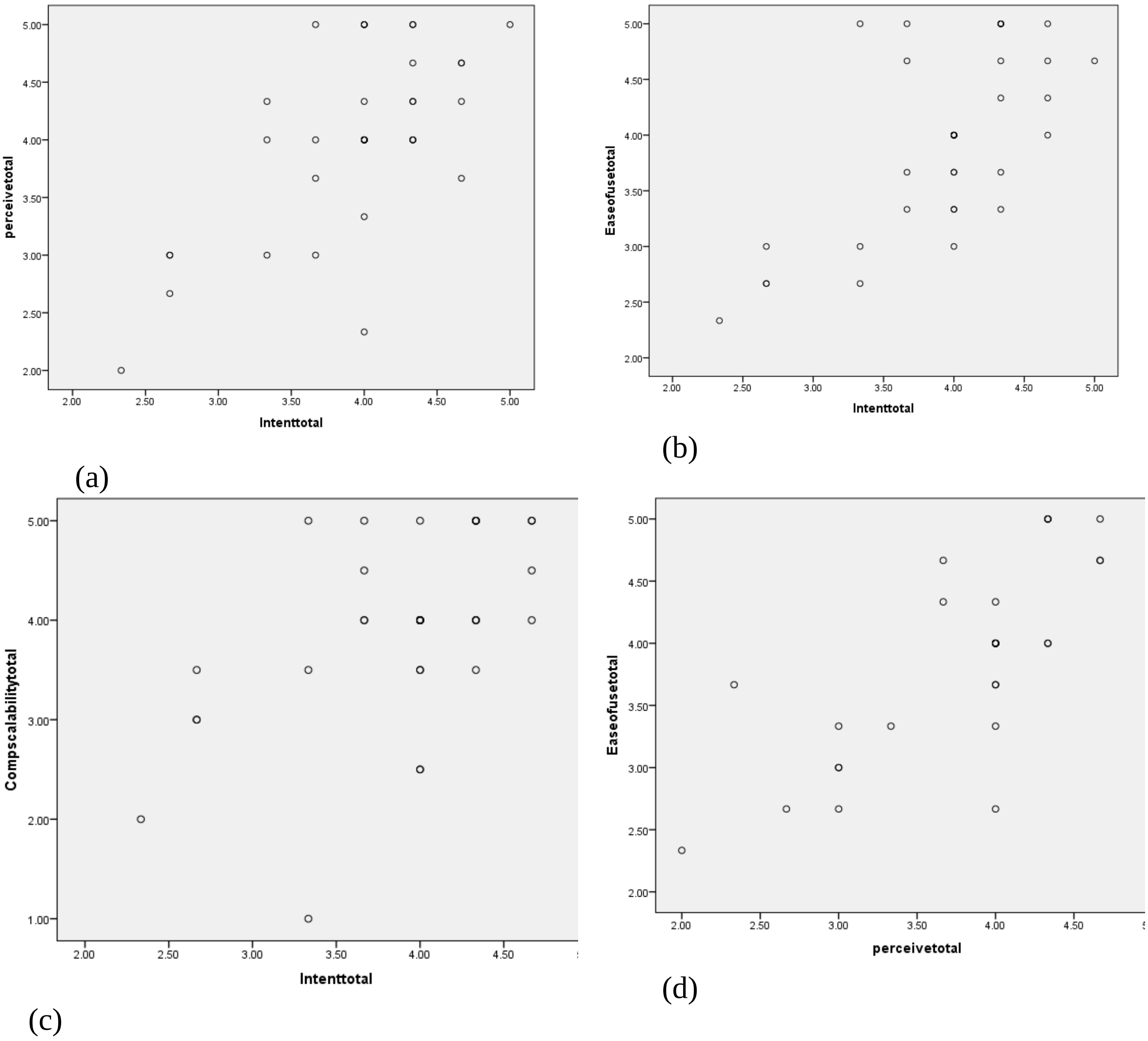
Table 7-12: Nonparametric Correlations between Constructs

			Intenttotal	perceivetotal	Easeofusetotal	Compscalabilitytotal
Spearman's rho	Intenttotal	Correlation Coefficient	1.000	.546**	.598**	.516**
		Sig. (2-tailed)	.	.000	.000	.001
		N	37	37	37	37
	Perceivetotal	Correlation Coefficient	.546**	1.000	.589**	.659**
		Sig. (2-tailed)	.000	.	.000	.000
		N	37	37	37	37
	Easeofusetotal	Correlation Coefficient	.598**	.589**	1.000	.830**
		Sig. (2-tailed)	.000	.000	.	.000
		N	37	37	37	37
	Compscalabilitytotal	Correlation Coefficient	.516**	.659**	.830**	1.000
		Sig. (2-tailed)	.001	.000	.000	.
		N	37	37	37	37
**. Correlation is significant at the 0.01 level (2-tailed).						

Abbreviations: Intention to use (Intenttotal), Ease of use (Easeofusetotal, Perceived Usefulness (perceivetotal), Compatibility and Scalability (Compscalabilitytotal)

According to the statistics, a strong and positive correlation exists between the Intent to Use and Perceived Usefulness, which is statistically significant (with correlation coefficient (cc) = .546, p = .000). There is a strong, positive correlation between the Intent to Use and Ease of Use, which is statistically significant (cc = .598, p = .000). Also, a strong and positive correlation exists between the Intent to Use and Compatibility and Scalability, which is statistically significant (cc = .516, p = .001). Thus, there is a statistically significant association between the constructs of Intent to Use, Perceived Usefulness, Ease of Use and Compatibility and Scalability.

A correlation matrix was run to demonstrate the correlation between the constructs. A scatter plot was generated to show this correlation. Figure 7-8 shows the scatter plot of the correlation coefficient of the variables. The correlation coefficient figure in the scatter plot depicts a positive correlation between the variables. Intent to Use the system has a direct and positive relationship with Perceived Usefulness (Figure 7-8 (a)). Intent to use the system has a direct and positive relationship with Ease of Use (Figure 7-8 (b)). Intent to Use the system has a direct and positive relationship with Compatibility and Scalability (Figure 7-8 (c)). There is also a positive correlation between the Perceived Usefulness of the system and the Ease of Use of the system (Figure 7-8 (d)).



(a)

(b)

(c)

(d)

Figure 7-8: Scatter Plot Showing the Correlation Coefficient of the Variables

According to the comments from the experts and end-users, the model could be improved from various perspectives. Some of the recommendations may be considered at the conceptual model level while other recommendations may be considered at the interface design level. There are also some comments that are beyond the scope of this research project. These include the customisation, translation to local language issues and employee training.

7.6. Recommended Revisions

Although many comments were provided which were constructive to the model, the study has systematically identified those comments which will contribute to the enhancement of the model concept. The comprehensive list of improvements suggested by the respondents is enumerated below.

The following themes demonstrate the improvements recommended by the participants involved in Iteration I.

- The model concept must be customisable to specific contexts.
- An application of the model concept requires training and orientation.
- An alerting mechanism must be incorporated to improve the response times to critical incidents.
- An application of the model concept must be integrated with existing systems.
- An application of the model concept must be available in local languages for increased usability.
- A look-up feature for IP addresses to ease incident management processes must be incorporated.

Customisation

Some respondents recommended that the system must be customised to an organisational context. The model concept is an elementary model which is intended to be customisable to various contexts. However, due to time limitations, it is not possible to demonstrate the model concept within various contexts within this research project. Nevertheless, this recommendation will be considered under future research directions.

Cases in point where respondents recommended customisation:

> *"I believe that companies to introduce such systems by designing their own one from their contextual situation"*
>
> [Participant C#14, End-user]
>
> *"Many users these days are interested to be aware about cyber incident in their organisation. However, it will be good if it can be customized specific to organisational context"*
>
> [Participant C#1, End-user]
>
> *"The system is user-friendly but some of the technical event words and categories requires some explanation or contextual meaning"*
>
> [Participant C#37, Expert user]
>
> *"Different organisations have their own preference of security incident management. So it requires their strategic decision and contextual security police [policy] line up"*
>
> [Participant C#37, Expert user]
>
> *"The model and systems seems unique but it specifically depends on organisational information security problems"*
>
> [Participant C#35, Expert user]

Another issue related to customisation was the consideration of incident categories according to the definition of specific organisational contexts. Various organisations have their own incident definitions. Thus, such organisations could incorporate more categories contextually. Additional information security causes and precautions could be incorporated for improved and comprehensive understanding.

Cases in point where respondents recommended further customisable features:

> *"As telecom security helpdesk, such systems would help us in coordinating incoming security incident data but its management requires more categories"*
>
> [Participant C#8, End-user]

> *"Categorization of incident into different cluster should be inline with organisational security policies"*
>
> [Participant C#36, Expert user]

> *"The system is user-friendly but some of the technical event words and categories requires some explanation or contextual meaning"*
>
> [Participant C#37, Expert user]

Training and Orientation

Training or orientation of end-users is also an essential element in increasing the usability of the model concept. This improvement is out of the scope of the study, nonetheless it is an important caveat to using the model concept. Cases in point where respondents recommended training and/or orientation include:

> *"The system would be more crucial for users to be provided training before they start job"*
>
> [Participant C#4, End-user]

> *"The system may require prior orientation or training before applying in organisational context"*
>
> [Participant C#1, End-user]

> *"Security incidents change with time, so follow-up training is required"*
>
> [Participant C#21, End-user]

“Follow up training of updates requires for easy use”

[Participant C#24, End-user]

“Some of the technical security features may not be understood by normal or end-users. It requires integration with technical issues and follow up training for end-users”

[Participant C#36, Expert user]

“I agree but user training should be a prerequisite to use the system”

[Participant C#29, Expert user]

“New staff could be recruited without adequate experience. So it may be difficult to introduce to some of the jargons .[sic] so requires training”

[Participant C#37, Expert user]

“It is justifiable, but encoding or remembering IP address for normal users may be difficult unless they get some training”.

[Participant C#33, Expert user]

An Alerting Mechanism

The importance of an alerting mechanism in response to a critical incident was recommended. The alerting mechanism is intended to provide support during critical incidents. The incorporation of an alerting mechanism is to improve response times to critical incidents unlike other types of incidents. This will also support the response and decision-making process of ISIM which makes it more efficient. This enhancement is demonstrated in Section 8.2.

Cases in point where respondents recommended an alerting mechanism include:

“Proactive incident requires also alerting mechanism in critical conditions”

[Participant C#37, Expert user]

> *"Alerting in case of critical incident for the group enhances its effectiveness".*

[Participant C#21, End-user]

Integration with Existing Systems

Integration with existing systems was also recommended by the respondents. The rationale behind this recommendation is for easy access, convenience, and adaptive usage according to their organisational context. Some respondents suggested the possibility of the system being integrated into the existing organisational systems. It is justified that the integration of the system enables users to access and update in the operational use of routine business. Cases in point where respondents recommended integration include:

> *"It will be good if such systems will be integrate to our organisation using our system login so that we can update ourselves about information security incident cases of our organisation"*

[Participant C#3, End-user]

> *"This systems seems separate from organisational systems. I may use the system in case if it is integrated to our organisational system".*

[Participant C#7, End-user]

> *"At this time, it is difficult to predict its application as it requires integration to organisational settings"*

[Participant C# 26, End-user]

> *"Integration of such system with operational security policies will support for effective reporting"*

[Participant C#20, End-user]

> *"It will be also good if there will be any room to integrate and work with the national security management for better incident awareness"*

[Participant C#5, End-user]

> *"Yes, I intend to use it. But if [sic] it has to be integrated with the system of of[sic] the organization"*

[Participant C#33, Expert user]

> *"Effectiveness of reporting not necessarily achieved though this system. Other electronic reporting schemes could be integrated".*

[Participant C#37, Expert user]

System Availability in Local Languages

The integration of local languages was also emphasised by many participants to improve the usability of the system. It is beyond the scope of the project to include this recommendation, nevertheless it is an important caveat to implementing a system based on the model concept.

Cases in point where respondents recommended the integration of local languages include:

> *"Some of the security issues will be more understandable if presented in local language"*

[Participant C#18, End-user]

> *"It would be more easy if it can be available in local language".*

[Participant C#18, End-user]

> *"Such systems, if available in local languages would help more"*

[Participant C#21, End-user]

> *“Local language availability of such systems may help better use”*

[Participant C#24, End-user]

> *“It is justifiable. But it will be also very good if it will be presented in local languages for more user to understand it and use it very easily”*

[Participant C#32, Expert user]

Lookup feature for IP Addresses

Some respondents have raised the concern that IP (Internet Protocol) addresses may not be recognisable by all users. Perhaps the name of the user involved in the incident can serve as an identifying mechanism for enhancing the comprehensibility of an incident. However, this may compromise the privacy of the user. Therefore, a look-up feature is introduced as an enhancement to the interface prototype without compromising the privacy of the users. The look-up feature will also not explicitly unveil all the details of the individual.

Cases in point where respondents recommended an approach to identify IP Addresses include:

> *“Some users in organisations may not recognize the technical terms such as ip address of incident unless they got pre training”*

[Participant C#10, End-user]

> *“Interacting with the system is easy but users may not know their IP address or may change with time”*

[Participant C#34, Expert user]

> *“It is justifiable, but encoding or remembering IP address for normal users may be difficult unless they get some training”.*

[Participant C#33, Expert user]

7.7. Discussion of Findings – Iteration I

In this study, most of the comments were gathered from end-users which shows a high intention of usability. The acceptability of the model concept and prototype was well-received. Some of the issues expressed that may influence the intention to use a system based on the model concept encompassed the themes of contextualisation, system integration and customisation. Some respondents were also uncertain regarding the significance of the model concept. Moreover, some concerns of language localisation of the system were also raised.

The TAM is a valid and robust model to be applied in many studies due to its simplicity and understandability (King & He, 2006). The study considered the constructs of the TAM (Intent to Use, Perceived Usefulness, and Ease of Use) to measure the acceptability of the model concept in organisations. As the TAM is extensible, Compatibility and Scalability were also considered as these elements affect the acceptability of new systems. While the TAM can be extended based on the nature of the research, its application in DSR is also widely acceptable (Abu-Dalbouh et al., 2017). The model is highly suitable to the technological domain. For instance, the TAM was used to assess employee adoption of information systems security measures (Jones et al., 2010).

According to Mlekus et al. (2020) the technology-inherent characteristics such as output quality, eloquence, dependability, and novelty were significant predictors of technology acceptance in newly designed systems. Moreover, the TAM serves as a valuable general framework and is consistent with a number of studies into the factors that influence users' intention to use modern technology (Charness & Boot, 2016).

The evaluation of the model by various users and experts using the TAM has significant implications for theory and practice. First, it has substantiated and provided empirical data to the theoretical framework of the TAM elements (Intent to Use, Perceived Usefulness, and Ease of Use) for evaluating the model. Second, the TAM enables organisations in the study to explore whether the model concept would be acceptable or usable before scaling up or applying the system within the scope of the organisation.

7.8. Validity and Reliability Measures

The validity and reliability of the data collected is described in Section 7.8.1 and Section 7.8.2. The quantitative and qualitative data was analysed in a triangulated manner in order to achieve validity.

7.8.1. Validity and Reliability – Quantitative Data

Cronbach's alpha α is one of the most widely used measures of reliability in the social and organisational sciences to measure internal consistency (Bonett & Wright, 2015). Table 7-13 shows the results of the Cronbach alpha test results run.

Table 7-13: Cronbach's Alpha Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.754	.870	12

The Cronbach alpha coefficient of the overall instrument was found to be 0.754. A Cronbach alpha test score above 0.7 is acceptable in terms of internal consistency of the survey.

7.8.2. Validity and Reliability – Qualitative Data

The qualitative data was assessed for trustworthiness by means of credibility, conformability, transferability, dependability and authenticity. Table 7-14 shows the validity and reliability measures, definitions, and evidence of compliance in the process of the evaluation.

Credibility was ensured via triangulation, peer analysis and verification by the respondents.

Dependability was ensured by confirming the results and applying appropriate statistical measures for the quantitative data.

Conformability was achieved by conducting rigorous data analysis and verification by respondents and by checking the summary of responses by the respondents.

Transferability was ensured by a systematic methodological application of the research instruments for data collection and analysis.

To achieve *Authenticity*, respondents were provided the opportunity to review a summary of the responses.

Table 7-14: Evidence of Validity and Reliability Measures

Measures	Techniques applied	Evidence of compliance
Credibility	-Two iterations of data gathering were conducted (including Iteration II). -Data Triangulation via multi-methods was applied. -Provision of 'thick descriptions' (i.e., providing as much detail as possible) in the analysis. -Participants were guided with the results of the study where the experts assisted in improving the artefacts. -Quotations from participants were integrated into the analysis. -The statistician conducted peer analysis. -Any descriptions that were inconsistent with the expectations of the researcher were considered in the analysis.	-Chapters 7 and 8 demonstrate the two iterations. -Data was analysed by triangulating quantitative and qualitative data through statistical description and analytical inferences (See section 7.4). -The context of the organisations involved was detailed in Section 7.3. -Participants were presented with the recommendations from Iteration. I. -The statistician ensured that the data was analysed independently. -All quotations including negative comments were considered – the negative comments were considered in Iteration II as recommendations for improvement.
Dependability	-An experienced statistician conducted an inquiry audit (external audit) on the integrity of the result outputs to maintain dependability.	-An audit was maintained by the statistician. -All data was captured online.
Conformability	-An audit trail was applied to ensure conformability. -The researcher comprehensively detailed the process of data collection, data analysis, and interpretation of the data. -Confirmation bias and subjectivity were overcome by using thematic analysis – data was coded in a justifiable manner so that it will provide meaningful analysis after categorisation using Atlas ti. -The supervisor assisted in reviewing the data analysis. -Conformability was additionally ensured by associating the existing literature that reported similar results to the study at hand.	-The data was reviewed by a statistician and the supervisor. -All the statistical designs and data results were confirmed for their consistency and reliability.
Transferability	-Transferability was achieved by affording clear descriptions of the methodology to ensure repeatability. -Provision of contextual information	-Although the application of the data is not universally transferable to external organisations, the sample data demonstrates the application of the

Measures	Techniques applied	Evidence of compliance
	about how the data was collected, the organisational setting of the selected entities and the respondent's setting. -The researcher provided existing situational analysis about the data collected such as organisational issues, information security culture of the organisation and the context of Ethiopia and the respondent's level.	data within the context of the organisations. -Chapter 3 clearly expressed the DSR methodology used.
Authenticity	-The experts were allowed to review the aggregated responses for confirmation. -The ethical procedures are ensured through confidentiality and anonymity which allow participants to express themselves truthfully.	-Qualitative data was collected to confirm the authentic experiences of the respondents. -The quotes and data from respondents were used verbatim. See Section 7.4.

7.9. Ethical Procedures

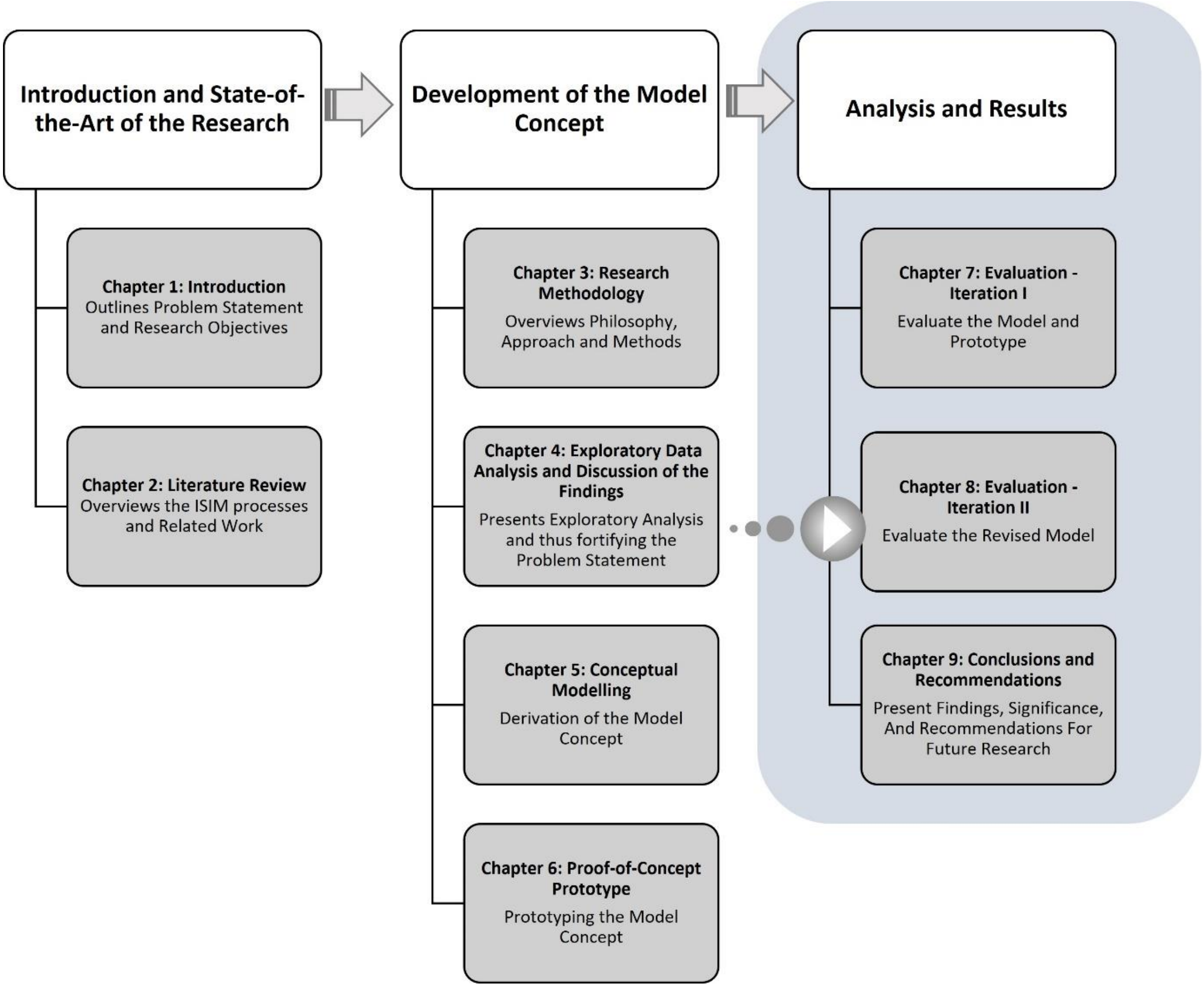
Appropriate ethical procedures were followed in order to collect data from the respondents. All participants were adequately informed regarding the nature of the study. Each participant had to provide their consent before engaging with data collection. Moreover, respondents were given the right to withdraw at any time without penalty. The right to confidentiality and anonymity was also upheld and no sensitive or personally identifying information was gathered. The responses were not directly associated with the participant's identity. Phase II was conducted during the Covid pandemic, thus appropriate Covid-19 protocols were maintained. Data was collected through online mechanisms to guarantee the health and safety of respondents so that they were not exposed to any vulnerabilities owing to the pandemic.

7.10. Chapter Summary

This chapter involved evaluating the fit for purpose of the model and interface prototype that was demonstrated in Chapters 5 and 6 respectively. This chapter provided quantitative and qualitative analysis of the responses from the participants. The analysis demonstrated that the respondents have a positive intention of acceptability of the model concept. The evaluation leveraged the TAM using a DSR approach to evaluate the model concept. Although the model received positive feedback, there is room for improvement. The model concept could be improved through usability and adaptability by a consideration of the organisational context. Chapter 8 discusses Iteration II of the study which leverages the expertise of the information security professionals in order to enrich and enhance the feedback about the usability of the model concept.

CHAPTER EIGHT

RESEARCH ROADMAP



Introduction and State-of-the-Art of the Research

Chapter 1: Introduction
Outlines Problem Statement and Research Objectives

Chapter 2: Literature Review
Overviews the ISIM processes and Related Work

Development of the Model Concept

Chapter 3: Research Methodology
Overviews Philosophy, Approach and Methods

Chapter 4: Exploratory Data Analysis and Discussion of the Findings
Presents Exploratory Analysis and thus fortifying the Problem Statement

Chapter 5: Conceptual Modelling
Derivation of the Model Concept

Chapter 6: Proof-of-Concept Prototype
Prototyping the Model Concept

Analysis and Results

Chapter 7: Evaluation - Iteration I
Evaluate the Model and Prototype

Chapter 8: Evaluation - Iteration II
Evaluate the Revised Model

Chapter 9: Conclusions and Recommendations
Present Findings, Significance, And Recommendations For Future Research

CHAPTER 8: EVALUATION – ITERATION II

8.1. Introduction

This chapter re-evaluates the revised model concept based on the recommendations from Iteration I (Chapter 7). Accordingly, the **C**oordinated **C**ommunication and **A**wareness approach towards enhancing **I**nformation **S**ecurity **I**ncident **M**anagement (CCA$^{\text{ISIM}}$) model was improved with reference to the suggestions that the respondents provisioned during the evaluation process in Iteration I (Section 8.2). The revised model is evaluated by the experts only in this iteration (Section 8.3). This iteration relied on expert advisors to confirm the validity of the amendments owing to the technical nature of the enhancements. The measures for abstraction, originality, justification, and benefit are reconsidered by the experts (Section 8.3). The responses are then summarised, and the findings are discussed in Section 8.4 and Section 8.5 respectively. The concluding remarks are presented in Section 8.6.

8.2. The Refined Model

Although all comments provided were useful, it was reasoned that it would be essential to focus on those aspects that would enhance the model concept within the scope of the study. Additionally, there are capacity limitations that have to be considered in terms of the ability of the researcher to attend to all proposed improvements. The three recommendations under consideration are: an alerting mechanism, a lookup feature for IP (Internal Protocol) addresses and the inclusion of additional incident categories. These features are considered in the system as they enhance the process of critical incident identification which supports the response and decision-making processes of Information Security Incident Management (ISIM). These modifications will also contribute to the awareness and communication facets of the model.

8.2.1. Enhancement 1: An Alerting Mechanism

Respondents indicated that there should be a mechanism to alert users should a critical incident occur. Alerts that focus on the distribution of information assists in determining critical conditions of information security incidents such as a malicious attack, virus, spoofing, spam, etc. (Villegas-Ch et al., 2021). This feedback can be addressed in the study at both the model and prototype levels (interface design).

The refined model will now encompass an alerting mechanism (Figure 8-1). Although all incident information is communicated and shared among users, the alerting mechanism in this context is incorporated for critical incident management. Appropriating from Ahlan et al. (2015), critical incident alerts need to be considered as one of the processes of ISIM. The availability of these types of mechanisms enhances the decision-making process of ISIM, in that users will be aware of critical incidents which enable them to act instantly. The alerting mechanism has timely and significant importance for users to enhance the management of incident handling. Thus, the idea for the improvement of the model is appropriated from Ahlan et al. (2015) in that users considered an alerting mechanism as a process of the comprehensive approach of ISIM.

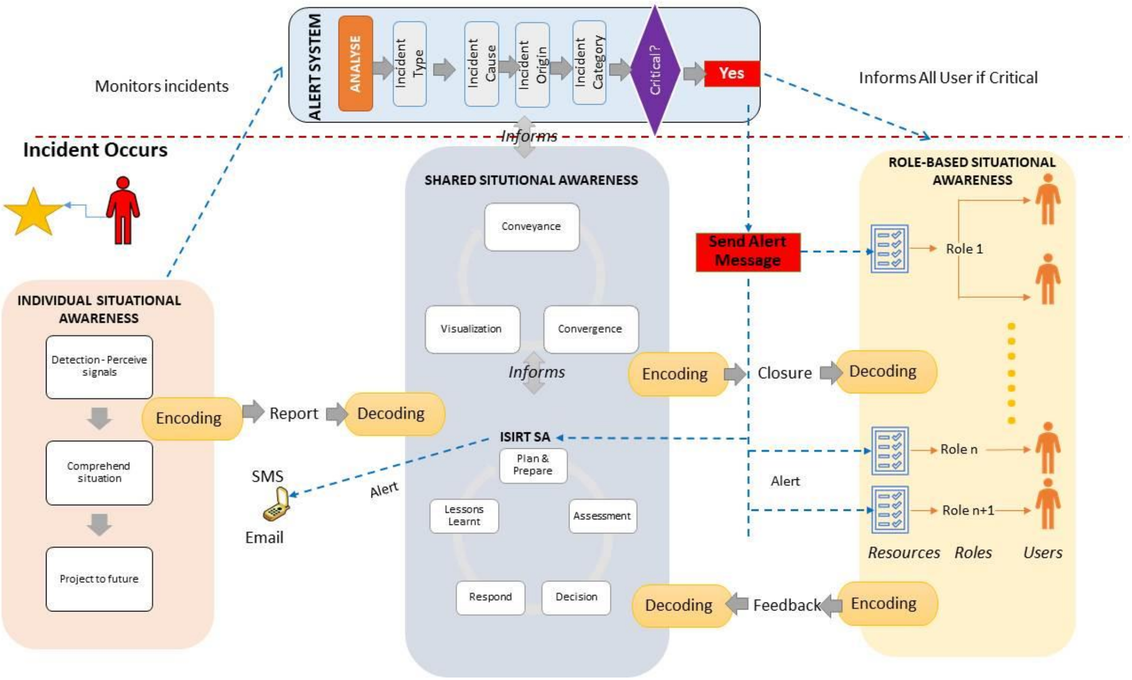


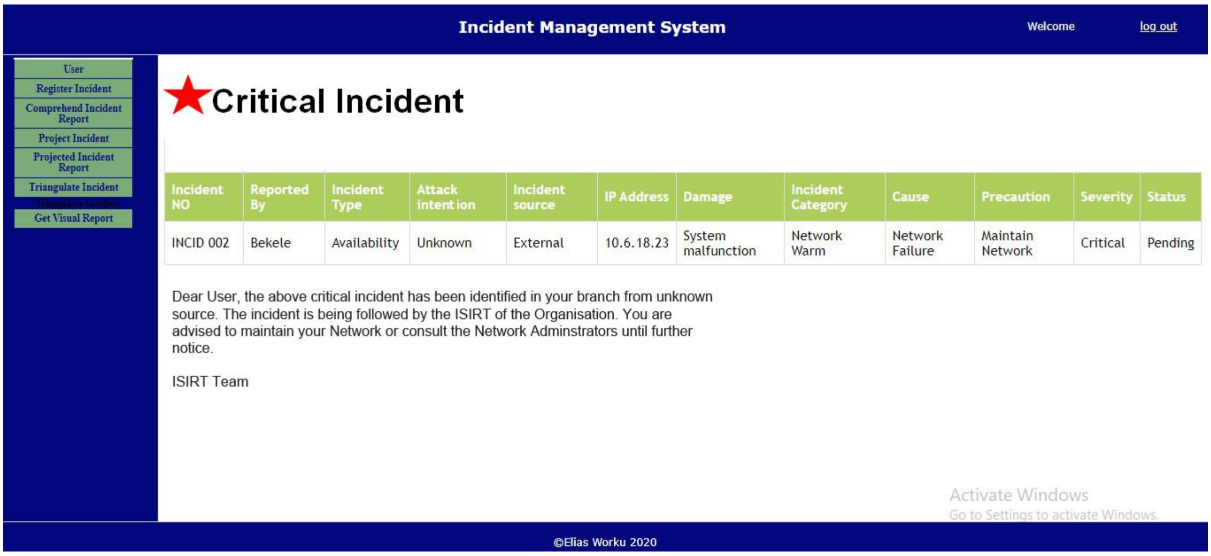
Figure 8-1: Revised CCA^{ISIM} Model after Iteration I

In the revised model (Figure 8-1), an information security incident alert mechanism will be managed in the CCA^{ISIM} model. The revised model intends to alert individuals and shared groups about the identification of a critical security incident. The criticality of the incident depends on the policy and definition of an organisational context. The decision-making process for the alert system considers various parameters of the incident such as incident type, cause, origin, and category. If the incident is considered to be critical, then an incident alert will be reported to the ISIRT and all users. If the incident is not critical, the system will revert to the normal operation of incident management as per the original model concept. The ISIRT will immediately send out further alert information to all users based on their assessment. The incident information dispatched is to all users via various channels of communication.

For instance, a certain organisation may have the following critical incident definition. Thus, if an incident falls into such a category, it will be reported as a critical incident.

If Incident type= "compromise," causes= "deliberate," origin= "External," Category= "Financial loss," then Severity= "Critical."

Figure 8-2 shows a sample interface design of a critical information security incident being disseminated to all users.



★Critical Incident

Incident NO	Reported By	Incident Type	Attack intention	Incident source	IP Address	Damage	Incident Category	Cause	Precaution	Severity	Status
INCID 002	Bekele	Availability	Unknown	External	10.6.18.23	System malfunction	Network Warm	Network Failure	Maintain Network	Critical	Pending

Dear User, the above critical incident has been identified in your branch from unknown source. The incident is being followed by the ISIRT of the Organisation. You are advised to maintain your Network or consult the Network Adminstrators until further notice.

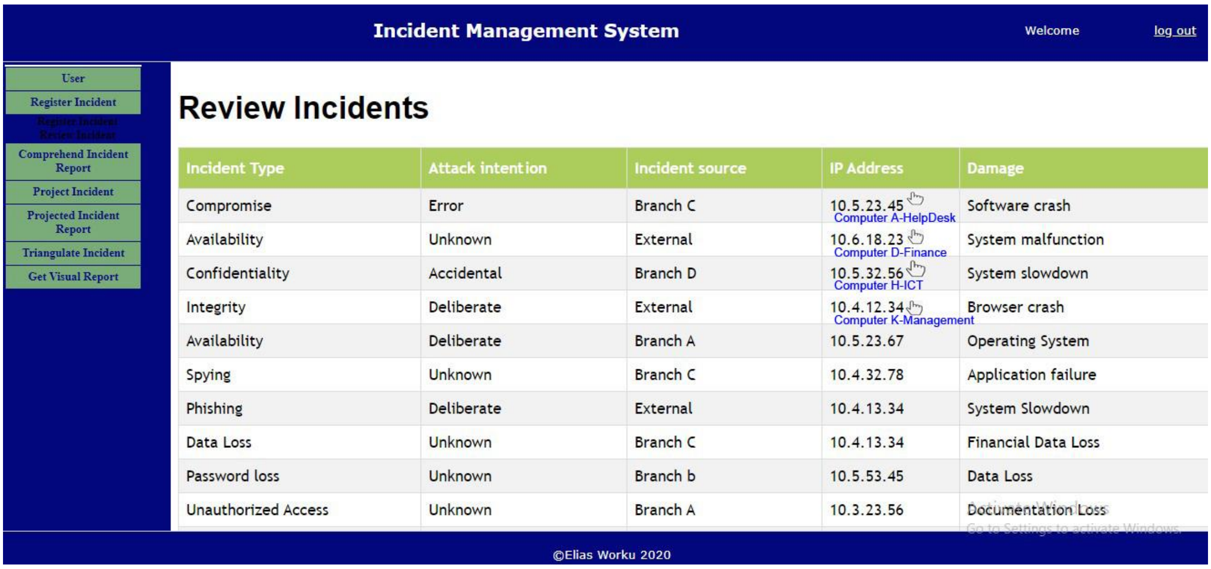
ISIRT Team

Figure 8-2: Critical Incident Information Notification for Users

Figure 8-2 shows how users will be notified of a critical incident that occurred in their organisation when they log into the system. The alerting system enables users to obtain critical incident information via multiple channels. It is envisioned that the system will dispatch such information via various channels such as short messaging services and email.

8.2.2. Enhancement 2: Look-up Feature for IP Addresses

The aim of this recommendation is to provide users with a look-up feature for IP addresses. In this feature, when a user hovers over an IP address of a certain machine, a non-technical identifier of the machine will be revealed for a descriptive and improved identification of the computer with the aim of enhancing the usability of the system. The disclosure of the name takes into consideration the privacy of the users. Figure 8-3 shows an interface design of how the IP address is disclosed. For instance, when hovered, the identifier “Computer A-Helpdesk” is revealed for an IP Address 10.5.23.45 in branch C.



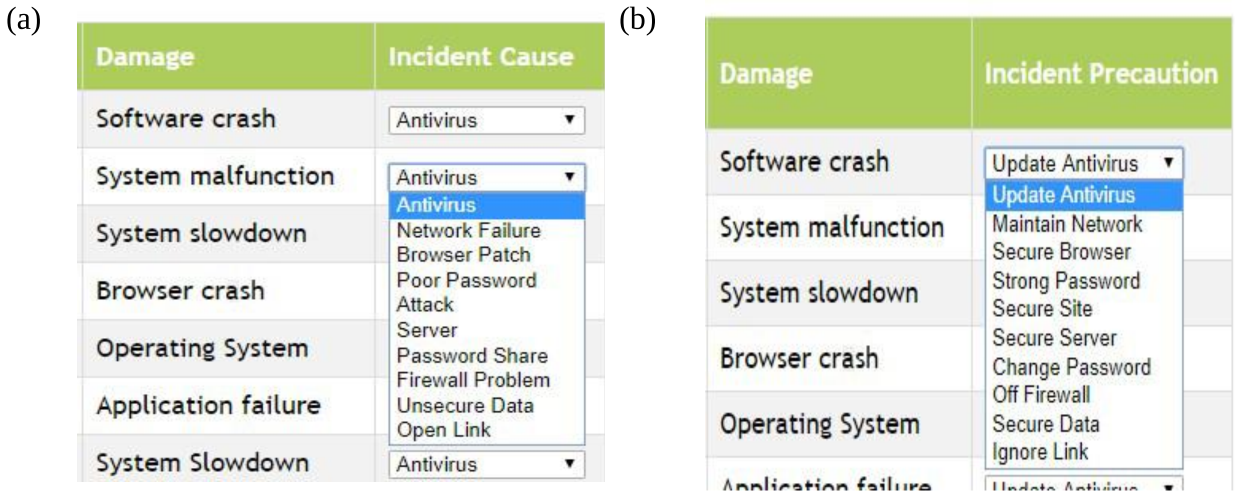
Review Incidents

Incident Type	Attack intention	Incident source	IP Address	Damage
Compromise	Error	Branch C	10.5.23.45 Computer A-HelpDesk	Software crash
Availability	Unknown	External	10.6.18.23 Computer D-Finance	System malfunction
Confidentiality	Accidental	Branch D	10.5.32.56 Computer H-ICT	System slowdown
Integrity	Deliberate	External	10.4.12.34 Computer K-Management	Browser crash
Availability	Deliberate	Branch A	10.5.23.67	Operating System
Spying	Unknown	Branch C	10.4.32.78	Application failure
Phishing	Deliberate	External	10.4.13.34	System Slowdown
Data Loss	Unknown	Branch C	10.4.13.34	Financial Data Loss
Password loss	Unknown	Branch b	10.5.53.45	Data Loss
Unauthorized Access	Unknown	Branch A	10.3.23.56	Documentation Loss

Figure 8-3: A Look-Up Feature of IP Addresses

8.2.3. Enhancement 3: Additional Incident Categories

The respondents recommended including further incident causes, categories and precautions. The incorporation of the incident categories allows users to categorise and manage incidents more easily. It is envisioned that the ISIRT will be responsible for grouping and clustering of the incident categories which then could be selected by users during the processes of incident reporting and handling. The list of incident causes and precautions should be flexible and extensible. The incorporation of additional incident categories is depicted in Figure 8-4.



(a)

Damage	Incident Cause
Software crash	Antivirus ▼
System malfunction	Antivirus ▼
System slowdown	
Browser crash	
Operating System	
Application failure	
System Slowdown	Antivirus ▼

Antivirus
Network Failure
Browser Patch
Poor Password
Attack
Server
Password Share
Firewall Problem
Unsecure Data
Open Link

(b)

Damage	Incident Precaution
Software crash	Update Antivirus ▼
System malfunction	
System slowdown	
Browser crash	
Operating System	
Application failure	Update Antivirus ▼

Update Antivirus
Maintain Network
Secure Browser
Strong Password
Secure Site
Secure Server
Change Password
Off Firewall
Secure Data
Ignore Link

Figure 8-4: Extending the list of Information Security Incident Causes and Precautions

8.3. Data Analysis

In Iteration II, Section III of the questionnaire (Appendix C) was completed by respondents from the expert groups (n=9) in organisations. The respondents were experts who were involved in Iteration I of the data collection. The constructs in this section of evaluation included the same constructs as described in Section 7.4.2 – Abstraction, Originality, Justification and Benefit. (A link to the redacted raw data is referenced in Appendix G.)

Abstraction

In response to Question #1, the majority of the expert user respondents (88.9%; n=8) indicated that the model concept (the application of situational awareness and the Interactive Model of Communication (IMC) can conceptually resolve the problems associated with the poor coordination of awareness and communication of security incidents. The positive response for the abstraction construct established that the enhancements was advantageous –Iteration II (88.9%) compared with Iteration I (77.8%). Only 1 of the expert users indicated a reservation (N/A) on the applications of the model for the coordination and awareness of security incidents. Figure 8-5 (pie chart) demonstrates the responses.

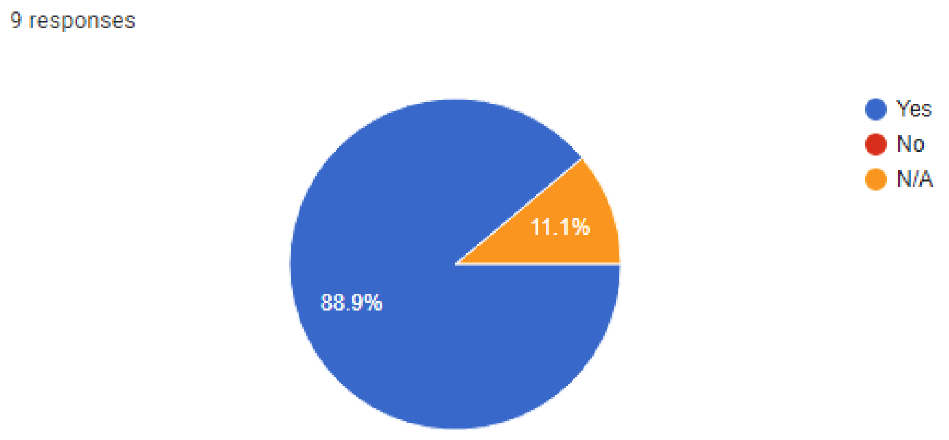


Figure 8-5: Responses for the Abstraction Item (Iteration II)

The remarks by two participants demonstrate a positive attitude to the revisions and the model concept. Cases in point:

> “*The revised model and prototype can potentially resolve the challenges of reporting of information security incidents in organisations for better and effective understanding of incident especially having alert nature”*
>
> [Participant D#1, Expert user]

> *“The communication of critical incidents in organisations through individual's devices such as mobile and email enables quick and effective learning for users”*
>
> [Participant D#2, Expert user]

Originality

In response to Question #2, the majority of the respondents (77.8%; n = 7), indicated that the model concept is unique in its aim of integrating situational awareness and communication models for easing the coordination of incident related security problems. This analysis established that the experts viewed the ‘originality’ construct more positively as compared to Iteration I (66.7%). However, one of the respondents (n=1) responded negatively. This expert was not convinced of the originality. One of the respondents (n=1) responded ‘Not Applicable

(N/A)' on the originality of the model which implies that they are indifferent to this construct. Figure 8-6 (pie chart) demonstrates the responses.

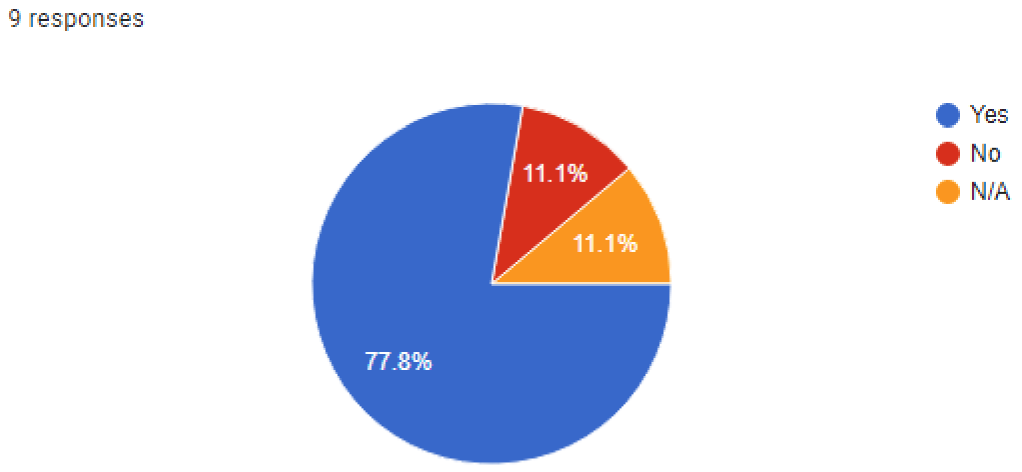


Figure 8-6: Responses for the Originality Item (Iteration II)

The originality of the model concept was confirmed by two participants. Cases in point:

> *"The coordinated nature of communication and awareness for incident management in organisations in this model is a new phenomenon as far as I know",*
>
> [Participant D#1, Expert user]

> *"The system has uniquely approached the problem of information security awareness by integrating reporting and learning systematically. As users are required to adapt to contemporary incident information in organisations, it will be ease to use it by either integrating to existing systems or independently"*
>
> [Participant D#7, Expert user]

Justification

In response to Question #3, (77.8%; n=7) the majority of the respondents indicated that the model concept is justified in a comprehensible manner in the approach for the coordination of communication and awareness efforts in information security management. This is the same result as with Iteration I. Two of the respondents indicated N/A, which implies that the respondent may be indifferent to the revised version. Figure 8-7 demonstrates the responses.

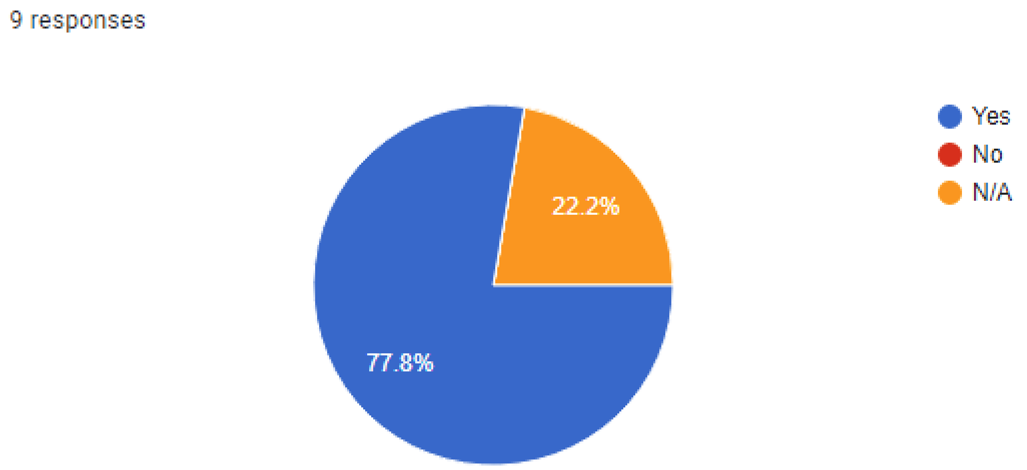


Figure 8-7: Responses for the Justification Item (Iteration II)

Two experts remarked on how the model improvements may enhance the usability for all users. Cases in point:

> *"The improved model and prototype is a bit more justifiable to be applied in a more comprehensive manner for that can suit for all types of users"*
>
> [Participant D#5, Expert user]

> *"The improved model and prototype is better explained and will assist ordinary users to get incident information in a more easier and adaptive manner",*
>
> [Participant D#8, Expert user]

Benefit

Question #3 is related to the benefit of the model and prototype. In response to Question #3, all the respondents (100%) indicated that the model concept will benefit organisations in the coordination of communication and awareness efforts in information security management. The percentage in Iteration I was 66.7% which is a considerable improvement in Iteration II. Figure 8-8 depicts the response rate.

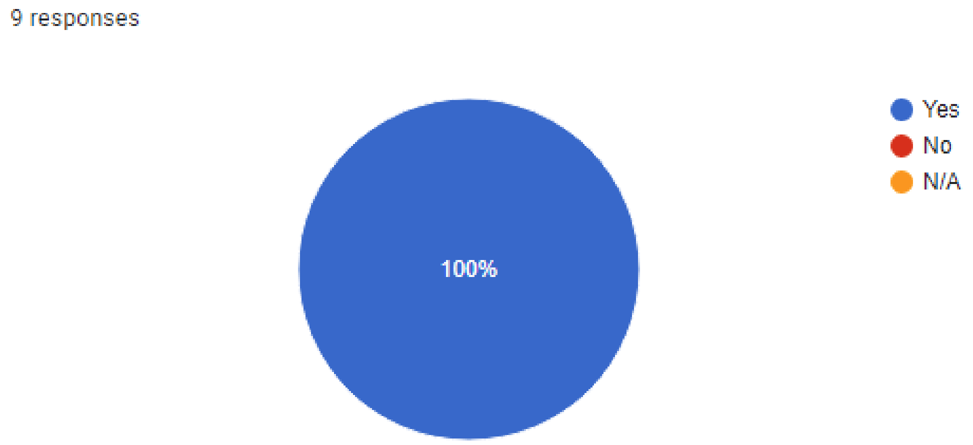


Figure 8-8: Responses for the General Benefit Item (Iteration II)

One participant commented on the ease of use of the application for it is fit for purpose.

> *"The mode[l] and prototype can really benefit organisations by creating awareness and interactive mechanisms for their users and all stakeholders using easy to use application"*

[Participant D#1, Expert user]

Two participants commented positively on the enhancements. Cases in point:

> *"The model and prototype enables users to easily identify computer machines in the management of information security incidents",*

[Participant D#2, Expert user]

> *"The enhanced model and prototype through various improvements such as reporting critical incident and incident categories provides users with improved look and enhances its usability"*

[Participant D#3, Expert user]

In response to Question #5, (77.8%; n=7) of the respondents indicated that the implementation of such a model concept outweighs the cost of its deployment compared to the risks of contemporary information security threats. Two of the expert user respondents indicated a 'Not Applicable N/A' response which implies they are indifferent. The data indicated a lower benefit percentage compared to the previous response (88.9%), in that expert users judged the benefit to be slightly lower as compared to Iteration I. Figure 8-9 depicts the variation in responses.

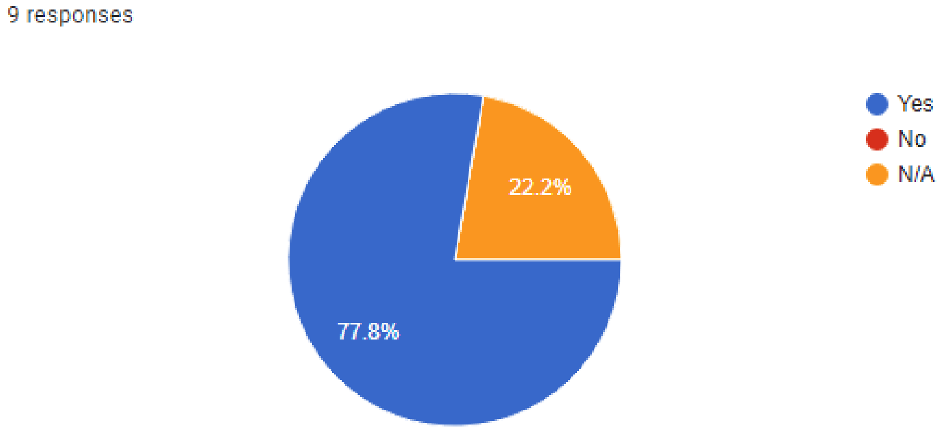


Figure 8-9: Responses for the Cost-Benefit Item (Iteration II)

Regarding the cost-benefit analysis of the system, two participants responded positively. Cases in point:

> *"Such systems are very much adaptive and cost efficient for organisations compared to the risks of being vulnerable to security incidents"*

[Participant D#1, Expert user]

> *"In times of information security threats, organisations are planning for more resources for combating incidents in various means. So it is so beneficial compared to its cost"*

[Participant D#5, Expert user]

However, one participant indicated that the cost-benefit would be difficult to estimate at this juncture. A case in point:

> *"It may be difficult to estimate the cost benefit analysis at this stage"*

[Participant D#9, Expert user]

8.4. Summative Responses

The final question — Question #6 (*"Any further recommendations for improvement for the model concept that you would like to share?")* determined if respondents had any further views on the model:

The revised model and prototype generated an optimistic response. Cases in point:

> *"The model and prototype is great to learn in case of alerting incidents"*

[Participant #D1, Expert user]

> *"It is good model that will help information security experts, users and managers in organisations to enhance their communication and awareness about incidents"*

[Participant D#4, Expert user]

The participants made several recommendations that involve customisations, technical feature integration such as intrusion detection systems (IDS), machine learning and archiving past incidents.

Cases in point:

> *"The alerting mechanism is very critical for efficient incident communication, but it would be more good if the system can have a mechanism to have knowledge base or archive to learn and predict long term incidents"*
>
> [Participant D#2, Expert user]

> *"The system in the future could be more improved if machine learning mechanisms are integrated into it which eases the learning and awareness purposes"*
>
> [Participant D#9, Expert user]

> *"The model might be more improved if there could be some mechanism to directly link to technical means of information security incident management like IDS so that the system could get incident information directly as one element of source of incidents"*
>
> [Participant D#3, Expert user]

The other recommendation is to integrate the system in the existing operational applications for better usability among users. Cases in point:

> *"It will be more relevant if the system works together with existing organisational ERP or operational applications for quick access and better usability"*
>
> [Participant D #6, Expert user]

> *"It will be good if the system could integrate and go inline with new forms of incident situations either globally or specific to the organisational context"*
>
> [Participant D#8, Expert user]

Further improvement of the system could be envisioned after the deployment of the system.

Cases in point:

> *"The system is well conceptualized at this stage. Further improvements could arise once it becomes operational through use"*
>
> [Participant D#7, Expert user]

> *"I think it is good system. However, its application and gaps will be identified once the system is deployed and start working at small level and grow towards larger scale"*
>
> [Participant D#5, Expert user]

8.5. Discussion of Findings – Iteration II

The model and prototype were improved based on the recommendations from expert users and end-users during Iteration I. As the remarks in Iteration I were positive, it was unsurprising that there were fewer suggestions proffered in Iteration II. There was an improvement in the results for most constructs. There was an improvement in the response for the abstraction construct – Iteration II (88.9%) compared to Iteration I (77.8%). Similarly, there was an improvement in the originality construct – Iteration II (77.8%) compared with Iteration I (66.7%). The experts probably felt that the enhancements improved the usability and uniqueness of the model concept. The results for the justification remained unchanged across the iterations (77.8 %). Perhaps the experts who were not convinced in Iteration I regarding the justification of the model remained unconvinced in Iteration II. Typically, experts prefer technical controls over human-centered controls. With regard to the benefit of the system, in Iteration II, all experts were convinced of the advantages of the model concept (100%) unlike the previous Iteration II (66.7%). Perhaps the enhancements assisted in improving their viewpoint such as an alerting system, look-up features for IP addresses and options for more incident categories.

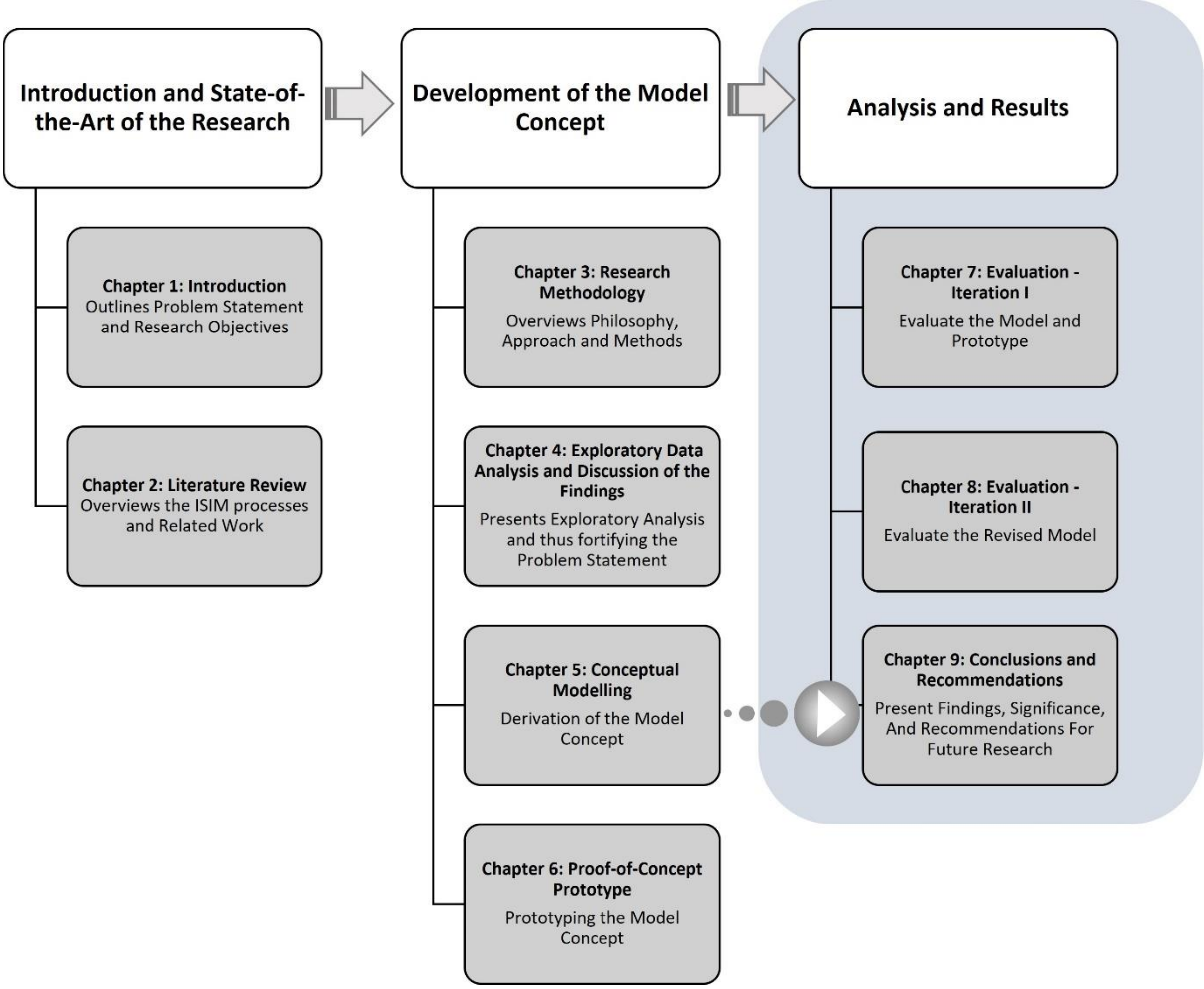
The cost-benefit analysis was higher in Iteration I (88.9%) than in Iteration II (77.8%) as perhaps it is difficult to estimate this cost at this juncture. The experts indicated there were too many unknowns at this point.

8.6. Chapter Summary

This chapter analysed the evaluation of the model after enhancement. The model concept received an encouraging acceptability rating among the respondents. However, some suggestions were also raised by the respondents that can potentially serve as further improvement for the model and prototype such as integration of machine learning, knowledge-based systems, archiving systems and IDS. The next chapter discusses the conclusion and recommendation of the study.

CHAPTER NINE

RESEARCH ROADMAP



Introduction and State-of-the-Art of the Research

Chapter 1: Introduction
Outlines Problem Statement and Research Objectives

Chapter 2: Literature Review
Overviews the ISIM processes and Related Work

Development of the Model Concept

Chapter 3: Research Methodology
Overviews Philosophy, Approach and Methods

Chapter 4: Exploratory Data Analysis and Discussion of the Findings
Presents Exploratory Analysis and thus fortifying the Problem Statement

Chapter 5: Conceptual Modelling
Derivation of the Model Concept

Chapter 6: Proof-of-Concept Prototype
Prototyping the Model Concept

Analysis and Results

Chapter 7: Evaluation - Iteration I
Evaluate the Model and Prototype

Chapter 8: Evaluation - Iteration II
Evaluate the Revised Model

Chapter 9: Conclusions and Recommendations
Present Findings, Significance, And Recommendations For Future Research

CHAPTER 9: CONCLUSIONS AND RECOMMENDATIONS

9.1. Introduction

This chapter reflects on the general conclusions and recommendations of the study. This study considered the issues surrounding the lack of coordination of awareness and communication efforts within Information Security Incident Management (ISIM) as a response to the escalating attack vectors in the online world. This chapter commences with an overview of the study (Section 9.2). This is followed by an account of how the objectives of the study were accomplished (Section 9.3). The key contributions of the study and the recommendations are presented in Section 9.4 and Section 9.5 respectively. The implications for theory and practice are considered in Section 9.6. This chapter culminates with the limitations, future research directions and concluding remarks in Section 9.7, Section 9.8, and Section 9.9, respectively.

9.2. Overview of the Thesis

The coordination of communication and awareness efforts in the process of ISIM has been identified as an important approach in reducing the severity of information security incidents. The study posited that a human-centered ISIM approach that was collaborative, shared, participatory and proactive will assist users in cognising incident information thereby improving the responsiveness to information security incidents. However, based on the findings of the exploratory study in the sampled organisations, it was found that the efforts of awareness and communication were practiced in a disjointed manner.

Organisations are often reliant on an elevated level of technology adoption to manage information security incidents. Consequently, a human-centered approach is overlooked as a solution to improving ISIM. From the exploratory study (Chapter 4), it was observed that most organisations do not have systematic proactive reporting and awareness mechanisms for their employees that can support their communication and cyber-controlling policies and strategies of the organisation. As a result, most employees and stakeholders are not trained to identify and manage information security incidents. The management of information security incidents in a standardised approach is a new phenomenon to most organisations in the study. It is possible to infer that most of the organisations have emphasised the need for general ICT policy and technical installation of information security equipment rather than the proactive and human-based approach such as applying communication and awareness efforts in order to involve all employees in the process.

The findings from the exploratory study served as a foundation for the framework of a conceptual model that unifies and subsumes the Interactive Model of Communication (IMC) and situational awareness towards the enhancement of awareness and communication practices within ISIM in organisations. The conceptual model designated a **C**oordinated **C**ommunication and **A**wareness approach towards enhancing **I**nformation **S**ecurity **I**ncident **M**anagement (CCA$^{\text{ISIM}}$). The CCA$^{\text{ISIM}}$ has the potential to enhance the ISIM activities of organisations for improved awareness and reporting of incident information that was practised in an isolated and unplanned approach.

The CCA$^{\text{ISIM}}$ enables all users (both technical and non-technical employees) to proactively engage in the management of information security incidents. The model was evaluated via two iterations. The model received high acceptability among all users.

9.3. Accomplishing the Objectives of the Study

The study aimed to address the following research questions:

- **RQ1**: To what extent are strategies for awareness and communication efforts integrated into organisational ISIM practices?
- **RQ2**: How do organisations integrate communication and awareness efforts into their ISIM processes and practices?
- **RQ3**: To what extent is the integration of stakeholders' and end-users' participation instigated within the processes of incident awareness and communication efforts within ISIM practices?
- **RQ4**: How should organisations enhance the coordination of awareness and communication efforts within the processes of ISIM practices?

The research approach for this study can be viewed within a framing of a Design Science Research (DSR) approach. Research questions **RQ1**, **RQ2** and **RQ3** were addressed through the exploratory study which aimed to confirm the problem statement and to identify the objectives of the study. The definitive research question (**RQ4**) was addressed using modelling and prototyping. The developed model and prototype were evaluated by a group of experts and end-users for their feedback and improvement.

The aim of this research was to study how communication and awareness efforts can be integrated towards enhancing the processes of ISIM. The specific objectives that guided the main research objective are:

Objective 1: *To assess the integration of strategies for communication and awareness efforts within ISIM practices.*

This objective was achieved by examining the integrated strategies for communication and awareness efforts within the organisations studied (Chapter 4, Section 4.7). In the studied organisations, most organisations did not integrate communication and awareness efforts into their ISIM policies and practices. It was found that there was limited integration of communication and awareness efforts into organisational ISIM practices – most of the processes related to account usage and basic antivirus installation. Thus, the integration of awareness and communication efforts in organisational ISIM was found to be extremely limited and uncoordinated.

Objective 2: *To identify the strategies leveraged by organisations to integrate communication and awareness efforts within their ISIM processes and practices.*

This objective was achieved through studying the information processes, policies, and procedures of the organisational setup (Chapter 4, Section 4.7). The strategies for communication and awareness efforts were found to be addressed via conventional means of information security awareness mechanisms which had limited standards and procedures.

Objective 3: *To assess the integration of stakeholders' and end-users' participation within the processes of incident awareness and communication efforts within ISIM practices.*

This objective was also met by empirically analysing the data from end-users on the level of participation and the reasons for participation (Chapter 4, Section 4.7.1 and Section 4.7.2). Accordingly, the study revealed that there was limited end-user and stakeholder participation in the process of ISIM. The integration of stakeholder and end-user participation that is applied in the process of incident communication and awareness efforts within ISIM processes was found to be inadequate. Moreover, the participation of all users such as end-users in the awareness and communication efforts of ISIM was scant.

The findings related to the previous objectives were also confirmed by the literature review conducted in Chapter 2. However, as the findings are limited to the studied organisations, the results are not generalisable.

Objective 4: *To develop and evaluate a conceptual model to enhance the coordination of communication and awareness efforts within the processes of ISIM practices.*

This objective was achieved through the design and development of the conceptual model – CCA^{ISIM} . The development and design of the model concept was presented in Chapter 5. The interface prototype for the problem raised was presented in Chapter 6. This study proposed a model which theoretically would enhance the coordination of communication and awareness efforts within the processes of ISIM practice. The model concept and prototype were evaluated among a group of information security experts and end-users for system acceptability using the Technology Acceptance Model (TAM). Based on the evaluation and feedback, the proposed model was positively accepted among organisational users (end-users and expert users) as a viable solution to the problem. In addition, the users suggested further improvements to increase the model’s acceptability among organisations.

9.4. Key Contributions

The key contribution of this study arises from the identification of the problem with the current approaches to ISIM and a proposed solution to address the problem. The problem is defined by a lack of coordination of awareness and communication efforts among all stakeholders in an organisation, which negatively affects the responsiveness to information security incidents. This issue was confirmed by an exploratory study conducted within Ethiopian organisations. This study then proposed a novel conceptual model to address the challenges identified by the empirical study. The rationale behind the study is that it approached the problems associated with ISIM from a collaborative, human-based and proactive perspective. Thus, the model will contribute and serve as a benchmark in adopting communication and awareness efforts within ISIM. The model can potentially enhance the comprehensive power of bringing diverse users together including end-users through interaction and sharing incident information. The theories (i.e., situational awareness and IMC) that underpinned the model may assist in delivering a shared and unified understanding of ISIM. This presentation of theories of the situational awareness and IMC provide a solution space to reason about how a shared understanding of information security incidents can be enhanced. This solution space can be applied to other information technology problems such as insider threat management and software risk management.

There have been extant studies which endeavoured to address ISIM through awareness and communication mechanisms (Ahmad et al., 2021; Husák et al., 2022). However, these studies often fail to incorporate non-IT personnel. The model propositioned by the current study demonstrated empirically how situational awareness and the IMC for enhancing incident communication can support the integration of all users. The model and prototype have multifaceted contributions for academia and industry. First, the model contributed to bridging the gap that exists within communication and awareness mechanisms related to the processes of ISIM. Second, the model can provide some insight on how to achieve proactive ISIM in organisations integrating the participation of all users by improving the coordination of communication and awareness practices of ISIM.

Another contribution of this study is the methodological approach used. The application of the DSR approach was enhanced with the TAM to study technological acceptance of the conceptual model – CCA^{ISIM} which enabled one to consider the problem from an empirical viewpoint rather than relying entirely on expert judgment which is opinion based. This provided quantitative data to support the typical approach of qualitative expert judgement for DSR studies. The questionnaire devised can be used and adapted for other DSR related studies. The questionnaire also allows non-experts to be included in the study.

Moreover, this study can assist countries with a low advancement of ISIM practices such as Ethiopia in several ways. The findings of the study may assist in adopting suitable ISIM standards, coordinating incident awareness within organisational settings, instigating end-users within the process of ISIM practices and cultivating a shared information security incident understanding.

9.5. Recommendations

Based on the research study and findings, the following key points are recommended as critical suggestions for information security stakeholders such as experts, end-users, and management.

9.5.1. Integration of Reporting Policies within ISIM

Due to the lack of managerial commitment and the lack of skill, reporting and awareness policies related to ISIM practices are not clearly defined. These policies should be integrated and forwarded to decision-makers for approval. Therefore, policies related to reporting, awareness and communication efforts should also be included in the policy documents. Organisations need to develop a culture of publicising their information security policy in order to increase awareness.

9.5.2. Requirements for Standardised ISIM in Organisations

The organisations in the study did not have standardised ISIM systems. This was either due to the lack of planning or the poor relative importance of responding to information security incidents. Organisations need to proactively work on adapting and creating their own standardised ISIM approaches.

9.5.3. Strong Managerial Commitment to Support Proactive Security Communications

To improve the managerial solutions, both middle-level and top-level managers or any other managerial bodies are required to prioritise and plan for information security incidents. This planning includes:

- Recruiting of information security professionals such as ISIRTs.
- Formulating appropriate ISIM policies.
- Ensuring the enforcement of formulated ISIM policies.
- Allocating an adequate budget for policy formulation and implementation for ISIM.
- Follow-up of information security incident practices.

9.6. Implications for Theory and Practice

As ISIM processes were practised in a disjointed manner, the model can best enhance the management of incidents through coordinated communication and awareness formation mechanisms. This model can also be applied in smaller to medium organisations that are vulnerable to information security threats. The model will assist organisations by introducing routine ISIM processes while improving the understanding of incident information. The role-based tier of the model assists in deploying the right incident information to the right individuals. This study demonstrated the applicability of situational awareness and communications protocols such as IMC within information security. However, the shared situational awareness model is not clearly espoused. It is unclear how individuals go from having situational awareness to having a shared mental model of the situation. This implies that there is a need to develop a theory to show how the iterative transition from individual awareness to a shared awareness occurs.

9.7. Limitations

Since the study was limited to organisations in Ethiopia with a purposively framed limited sample size, the findings cannot be generalisable to all contexts. In both phases of the study, the number of organisations suitable for the research area were limited. The sampling was limited purposively to organisations that were more likely to be vulnerable to information security incidents and hence more suitable to addressing the problem statement. Moreover, the study dealt with organisations who are primed towards implementing ISIM practices which implies that the participants were able to evaluate the proposed models with a deeper insight. This sampling procedure does introduce biasness, however, this was counteracted by including both qualitative and quantitative data collection methods, in order to fully understand the context of the study. The study does not exhaustively explore all the organisations at various levels of ISIM such as medium and small organisations. Thus, the study cannot provide a complete assessment of the national context which may have an impact on the applicability of the model.

9.8. Future Research Directions

A future research direction could involve exploring a more standardised and universal model that can fit any organisations to facilitate the practice of ISIM. Future research may also involve exploring the situational awareness model and communication protocols in a more dynamic, extensive, and knowledge-based context to incorporate advanced technologies such as machine learning and data mining. The study did not exhaustively demonstrate and prototype all the functions in the model such as conveyance and convergence which were strategies related to shared situational awareness. Thus, further study could be done exploring the role of conveyance, convergence, and utilising expertise from past experiences from an ISIM perspective in real-life contextual settings. This may assist in improving the shared situational awareness model for information security.

The role of culture could be investigated with regard to ISIM processes in organisations. Culture may affect how stakeholders perceive and communicate incident information. The research focus was more intraorganisational and the notion of interorganisational situational awareness and communication efforts within ISIM was not taken into consideration and this could be another research direction to explore. Furthermore, the issue of dealing with incomplete incident information within the model concept and reacting in that situation needs additional investigation. It may be prudent to consider how situational awareness could assist by addressing the gaps with current incident information so that ISIRTs could react more swiftly.

9.9. Chapter Summary

The main aim of this study is to explore and develop a model for coordinating awareness and communication efforts to support the processes of ISIM. It was found that awareness and communication efforts within ISIM were practised in a disjointed and uncoordinated manner. The exploratory findings in Phase I served as a basis for a conceptual model proposal that subsumes the IMC and situational awareness for enhancing ISIM processes.

There are limited studies that consider ISIM practices within a real-world context. This study has contributed to providing empirical data pertaining to the integrated aspects of communication and awareness mechanisms for ISIM within the Ethiopian context. This may be useful for countries with low advancement of information security practices. The power of integrating all users in ISIM practices was also considered in this study, thus advocating for a human-centric approach. The study provides a benchmark for organisations to include ISIM processes within their practice. The benchmark for ISIM processes should be proactive and human-centric in order to improve responsiveness to information security incidents.

The use of communication and awareness formation within the ISIM practice contributes to the body of knowledge by applying appropriate theoretical models within the processes of planning, detection, assessment, response, and lessons learnt. This study addressed the gap of empirical studies on the nexus between communication and awareness facets within ISIM within a limited context. However, the study may be more applicable to contexts where the uptake of ISIM practices is low.

REFERENCES

Ab Rahman, N. H., & Choo, K. K. R. (2015). A survey of information security incident handling in the cloud. *Computers and Security,* 49: 45–69. https://doi.org/10.1016/j.cose.2014.11.006

Abu-Dalbouh, H. M., Al-Buhairy, M., & Al-Motiry, I. (2017). Applied the technology acceptance model in designing a questionnaire for Mobile Reminder System. *Computer and Information Science.* 10(2): 15-24. https://doi.org/10.5539/cis.v10n2p15

Adane, K. (2022). The Current Status of cyber-security in Ethiopia. *SSRN Electronic Journal. The IUP Journal of Information Technology,* 16(3): 2020 https://doi.org/10.2139/ssrn.3545189

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: Its antecedents and measures. *Procedia Computer Science,* 72: 361–373. https://doi.org/10.1016/j.procs.2015.12.151

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams - Challenges in supporting the organisational security function. *Computers and Security*, 31(5): 643–652. https://doi.org/10.1016/j.cose.2012.04.001

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organisations develop situation awareness for incident response: A case study of management practice. *Computers & Security,* 101: 102122. https://doi.org/https://doi.org/10.1016/j.cose.2020.102122

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*(6): 717–723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

Ahmed, M., Sharif, L., Kabir, M., & Al-Maimani, M. (2012). Human errors in information security. *International Journal of Advanced Trends in Computer Science and Engineering,*1(3):82–87. https://doi.org/https://www.warse.org/pdfs/ijatcse01132012.pdf

Aladenusi, T. (2022). Nigeria cybersecurity outlook 2022. *Deloitte*. [Online] Available from: https://www2.deloitte.com/za/en/ghana/pages/risk/articles/nigeria-cybersecurity-outlook-2022.html. [Accessed: 29 December 2022].

Albers, A. and Lohmeyer, Q. (2012). Advanced systems engineering–towards a model-based and human-centered methodology. In *Proceedings of Tools and Methods of Competitive Engineering, In International symposium series on tools and methods of competitive engineering,* Karlsruhe, Germany, May 7-11, 2012, pp. 407-416.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organisations. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, Hilton Waikoloa Village, Hawaii, USA, January 3-6, 2018, pp.5085–5094. https://doi.org/10.24251/hicss.2018.635

Ang, S. H. (2014). Research design for business & management. *Research Design for Business & Management*, 1-336. London: SAGE Publications Ltd. https://doi.org/10.4135/9781473909694

Ani, U. P. D., & Agbanusi, N. C. (2014). A comparative assessment of computer security incidence handling. *British Journal of Mathematics & Computer Science*, 4(22): 3120-3134. https://doi.org/10.9734/bjmcs/2014/11874

Baker, K. A. (2002). Organisational Communication. In *Change Management and Knowledge Management, Chapter 13*. [Online] Available from: https://pdf4pro.com/view/chapter-13-organizational-communication1-2d1f26.html. [Accessed: 22 March 2018].

Balozian, P., & Leidner, D. (2017). Review of IS security policy compliance: Toward the building blocks of an IS security theory, *The Database for Advances in Information Systems*, 48(3): 11-43. ACM SIGMIS Database https://doi.org/10.1145/3130515.3130518

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., & Yen, J. (2010). Cyber SA: Situational awareness for cyber defense. *Advances in Information Security*, 46: 3–13. https://doi.org/10.1007/978-1-4419-0140-8_1

Bariff, M. L., & Ginzberg, M. J. (1982). MIS and the behavioral sciences: Research patterns and prescriptions. *The Database for Advances in Information Systems,* 14(1): 19–26. ACM SIGMIS Database. https://doi.org/10.1145/1017702.1017707

Barker, R., & Angelopulo, G. C. (2005). Integrated Organisational Communication (*First Edition)*, Cape Town: Juta & Co Ltd. https://books.google.com.et/books?id=D7rkS-Q-mYUC

Barnlund, D. C. (2008). Communication Theory :A Transactional Model of Communication *(2nd Edition), pp. 47–57. New Brunswick, New Jersey*. Routledge Publisher, https://www.taylorfrancis.com/chapters/edit/10.4324/9781315080918-5/transactional-model-communication-dean-barnlund

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security,* 61: 32-45.

Bashir, M., Afzal, M. T., & Azeem, M. (2008). Reliability and validity of qualitative and operational research paradigm. *Pakistan Journal of Statistics and Operation Research,* 4(1): 35. https://doi.org/10.18187/pjsor.v4i1.59

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information and Management*, *51*(1): 138–151. https://doi.org/10.1016/j.im.2013.11.004

British Columbia Campus. (2020). Introduction to professonal communications. [Online] Available from: at https://pressbooks.bccampus.ca/professionalcomms/chapter/3-2-the-communication-process-communication-in-the-real-world-an-introduction-to-communication-studies [Accessed 25 April 2023].

Belsis, M. A., Simitsis, A., & Gritzalis, S. (2005). Workflow based security incident management. In P. Bozanis & E. N. Houstis (Eds.), *Advances in Informatics* (pp. 684–694). Springer Berlin Heidelberg.

Bendy, G. and Meister, D. (1999). Theory of activity and situation awareness. *International Journal of Cognitive Ergonomics*, 3(1): 63–72.

Bernsmed, K., & Tøndel, I. A. (2013). Forewarned is forearmed: indicators for evaluating information security incident management. In *2013 Seventh International Conference on IT Security Incident Management and IT Forensics*, Nuremberg, Germany, 12-14 March 2013, pp. 3-14. IEEE.,. https://doi.org/10.1109/IMF.2013.14

Berntsen, K.E., Sampson, J. and Østerlie, T. (2004). Interpretive research methods in computer science. *Science*, 1–14, *Norwegian University of Science and Technology, Method Essay,* https://www.academia.edu/11848786/Interpretive_research_methods_in_computer_science

Bless, C., Higson-Smith, C., & Kagee, A. (2006). Fundamentals of Social Research Methods: An African Perspective *(4th Edition), Cape Town:* Juta & Co Ltd. https://books.google.com.et/books?id=7aKGSIsNk-IC

Bolstad, C.A., Cuevas, H.M. and Costello, A.M. (2005). Improving situation awareness through cross-training. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* Orlando, FL, October 12-15, 2005, Vol. 49, No. 25, pp. 2159-2163. https://doi.org/10.1177/154193120504902509

Bolstad, C. A., & Endsley, M. R. (2000). The effect of task load and shared displays on team situation awareness. In *Proceedings of the Human Factors and Ergonomics Society annual meeting,* Marietta, GA, May 22-25, Vol. 44, No. 1, pp. 189-192. Sage CA: Los Angeles, CA:SAGE Publications. https://journals.sagepub.com/doi/10.1177/154193120004400150

Bolstad, C.A., Gonzalez, C. and Graham, J. (2004). Automated Communication Analysis for Interactive Situation Awareness Assessment. *Sa Technologies Marietta ga. Defense Techincal Information Center* [Online] Available from: https://www.researchgate.net/publication/235049356_Automated_Communication_Analysis_for_Interactive_Situation_Awareness_Assessment. [Accessed: 28 October 2020].

Bonett, D.G. and Wright, T.A. (2015). Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *Journal of Organizational Behavior*, *36*(1): pp.3-15. https://doi.org/10.1002/job.1960

Bradley, J. (1993). Methodological Issues and Practices in Qualitative Research. *The Library Quarterly: Information, Community, Policy,* *63*(4), 431–449. http://www.jstor.org/stable/4308865

Brown, R., & Lee, R. M. (2019). The evolution of cyber threat intelligence (CTI): 2019 SANS CTI Survey. *SANS Institute.* [Online] Available from: https://www. sans. org/white-papers/38790/ [Accessed: 12 July 2021].

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *Management Information Systems Quarterly*, 34: 523–548. https://doi.org/10.2307/25750690

Businesstopia. (2018). Models of Communication. [Online] Available from: at https://www.businesstopia.net/communication. [Accessed: 15 June 2020].

Caballero, A. (2013). Information security essentials for IT managers: Protecting mission-critical systems. In *Computer and Information Security Handbook, Book Chapter, 2nd* Edition, Elsevier. pp. 379-407. Morgan Kaufmann. https://doi.org/10.1016/b978-0-12-416688-2.00001-5

Caelli, K., Ray, L., & Mill, J. (2003). 'Clear as Mud': Toward Greater Clarity in Generic Qualitative Research. *International Journal of Qualitative Methods*, 2(2): 1–13. https://doi.org/10.1177/160940690300200201

Carstensen, A.-K., & Bernhard, J. (2019). Design science research – a powerful tool for improving methods in engineering education research. *European Journal of Engineering Education*, 44(1–2): 85–102. https://doi.org/10.1080/03043797.2018.1498459

Charitoudi, K. (2013). A socio-technical approach to cyber risk management and impact assessment. *Journal of Information Security*, 04(01): 33–41. https://doi.org/10.4236/jis.2013.41005

Charness, N. and Boot, W.R. (2016). Technology, gaming, and social networking. In *Handbook of the Psychology of Aging (Eighth Edition)*, Tallahassee, FL, USA. (pp. 389-407), Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-411469-2.00020-0

Chawla, D. and Sondhi, N. (2011). Assessing the role of organizational and personal factors in predicting turn-over intentions: A case of school teachers and BPO employees. *Decision*, 38(2):5.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). An organisational psychology perspective to examining computer security incident response teams. *IEEE Security Privacy*, 12(5): 61–67. https://doi.org/10.1109/MSP.2014.85

Cheung, S.K. (2014). Information security management for higher education institutions. In *Proceeding of the First Euro-China Conference on Intelligent Data Analysis and Applications, Intelligent Data analysis and its Applications, Volume I:* Shenzhen, China, June 13-15, *2014*, pp. 11-19. Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-07776-5_2#citeas

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, 800(61): 1-147. https://doi.org/10.6028/NIST.SP.800-61r2

Converse, S., Cannon-Bowers, J. and Salas, E. (1993). Shared mental models in expert team decision making. *Current issues in Individual and Group Decision Making*, pp.221-246. Lawrence Erlbaum Associates, Inc.

Couper, M. P. (2000). Web surveys: A review of issues and approaches. *Public Opinion Quarterly*, 64(4): 464–494. https://doi.org/10.1086/318641

D'Amico, A. and Kocka, M. (2005). Information assurance visualizations for specific stages of situational awareness and intended uses: lessons learned. In *IEEE Workshop on Visualization for Computer Security, 2005.(VizSEC 05).* (pp. 107-112). IEEE. https://ieeexplore.ieee.org/document/1532072?arnumber=1532072

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Quarterly, 13*(3): 319–339. https://doi.org/10.2307/249008

Davis, F. D., & Venkatesh, V. (2004). Toward preprototype user acceptance testing of new information systems : implications for software project management. *IEEE Transactions on Engineering Management, 51*(1): 31–46. https://doi.org/10.1109/TEM.2003.822468

Da Veiga, A. & Eloff, J.H.P. (2007). An information security governance framework. *Information Systems Management*, 24(4):361-372. https://doi.org/10.1080/10580530701586136

Dennis, A. R., Fuller, R. M., & Valacich, J. S. (2008). Media, tasks, and communication processes: A theory of media synchronicity. *Management Information Systems Quarterly, 32*(3): 575–600. http://www.jstor.org/stable/25148857

Dennis, A.R. and Valacich, J.S. (1999). Rethinking media richness: Towards a theory of media synchronicity. In *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences,* Maui, HI, USA, January 05-08, 1999, pp. 1-10. IEEE. https://doi.org/10.1109/hicss.1999.772701

Dervin, B. (1998). Sense-making theory and practice: an overview of user interests in knowledge seeking and use. *Journal of Knowledge Management,* 2(2): 36–46. https://doi.org/10.1108/13673279810249369

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security,* 92: 101747. https://doi.org/10.1016/j.cose.2020.101747

Dodson, R. (2001). Information incident management. *Information Security Technical Report*, *6*(3): pp.45-53. https://doi.org/10.1016/s1363-4127(01)00307-7

Dominguez, C. (1994).. Situation awareness: papers and annotated bibliography (pp.5-15). *Technical Report No. AL/CF-TR-1994-0085. Armstrong Laboratory, Wright-Patterson Air Force Base,* OH (1994) Ohio: Armstrong Laboratory. McMillan, G. (Eds.)

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin,* 46(1): 78-109. https://www.tandfonline.com/doi/abs/10.1080/03050718.2020.1748075

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, 14(4): 532–550. http://www.jstor.org/stable/258557

Endsley, M. R. (2001). A model of inter-and intrateam situational awareness: implications for design, training and measurement. *New Trends in Cooperative Activities*, 46-68. https://www.semanticscholar.org/paper/A-model-of-inter-and-intrateam-situation-awareness%3A-Endsley-Jones/82e77d0b9927b5c2291c96d40e632e77c6b39e94

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors Society Annual Meeting, Patuxent River*, MD, Los Angeles, June 23-28, (Vol. 32, No. 2, pp. 97-101). Sage Publications. http://journals.sagepub.com/doi/pdf/10.1177/154193128803200221#articleCitationDownloadContainer

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Sage Journals*, *37*(1): 32–64. http://journals.sagepub.com/doi/pdf/10.1518/001872095779049543#articleCitationDownloadContainer

Endsley, M.R. (1990). A methodology for the objective measurement of pilot situation awareness. *AGARD, Situational Awareness in Aerospace Operations (SEE N 90-28972 23-53)*, (*AGARD-CP-478) (pp. 1/1–1/9). Neuilly Sur Seine, France: NATO-AGARD.*

Entin, E.B. and Entin, E.E. (2000). Assessing team situation awareness in simulated military missions. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Los Angeles, Angeles, CA , July 01-05, 2000, (Vol. 44, No. 1, pp. 73-76). SAGE Publications.

Erbacher, R. F. (2012). Visualization design for immediate high-level situational assessment. In *Proceedings of the Symposium on Visualization for Cyber-security,* October 15 2012, Seattle, WA, USA, pp. 17–24. https://doi.org/10.1145/2379690.2379693

Fade, S. A. (2003). Communicating and judging the quality of qualitative research: the need for a new language. *Journal of Human Nutrition and Dietetics*, *16*(3): 139–149. https://doi.org/https://doi.org/10.1046/j.1365-277X.2003.00433.x

FDRE (Federal Democratic Republic of Ethiopia). (2016). National Information and Communication Technology (ICT) Policy and Strategy, *Policy document*, [Online] Available from: https://comesabusinesscouncil.org/wp-content/uploads/2020/04/6-ICT-Policy-and-Strategy.pdf [Accessed: 13 March 2022].

Floodeen, R., Haller, J., & Tjaden, B. (2013). Identifying a shared mental model among incident responders. In H. Morgenstern, R. Ehlert, F. Freiling, S. Frings, O. Goebel, D. Guenther, S. Kiltz, J. Nedon, & D. Schadt (Eds.), *Seventh International Conference on IT Security Incident Management and IT Forensics*, Nuremberg, Germany, 12-14 March 2013, pp. 15–25. IEEE. https://doi.org/10.1109/IMF.2013.21

Foulger, D. (2004). Models of the communication process. Research Chapter, *Brooklyn, New Jersey*, pp.1-13.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security*, 46: 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Gregg, D. G., Kulkarni, U. R., & Vinzé, A. S. (2001). Understanding the philosophical underpinnings of software engineering research in information systems. *Information Systems Frontiers*, 3: 169-183.

Golfashani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, *8*(4): 597–607. http://nsuworks.nova.edu/tqr%0Ahttp://nsuworks.nova.edu/tqr/vol8/iss4/6%0Ahttps://nsuworks.nova.edu/tqr/vol8/iss4/6

Goodall, J.R., Lutters, W.G. and Komlodi, A. (2004). I know my network: Collaboration and expertise in intrusion detection. In *Proceedings of the 2004 ACM conference on Computer Supported Cooperative Work*, Chicago, Illinois, USA, November 9-10, pp. 342-345. https://doi.org/10.1145/1031607.1031663

Harviainen, J. T., & Melkko, R. (2022). Organisational information creation through a design game: A sense-making perspective. *Library & Information Science Research*, *44*(3): 101172. https://doi.org/https://doi.org/10.1016/j.lisr.2022.101172

Hassan, N. R., Mingers, J., & Stahl, B. (2018). Philosophy and information systems: where are we and where should we go? *European Journal of Information Systems*, *27*(3): 263–277. https://doi.org/10.1080/0960085X.2018.1470776

Henriquez, M. (2021). The top data breaches of 2021. *Security Magazine*. [Online] Available from: https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021, [Accessed: 21 January 2022]

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2008). Design science in information systems research. *Management Information Systems Quarterly*, *28*(1): 6.

Holtgrewe, U. (2014). New new technologies: The future and the present of work in information and communication technology. *New Technology, Work and Employment*, *29*(1): 9–24. https://doi.org/10.1111/ntwe.12025

Hove, C. and Tårnes, M. (2013). Information security incident management: an empirical study of current practice *(Master's thesis, Institutt for telematikk), Norwegian University of Science and Technology*, https://daim.idi.ntnu.no/masteroppgaver/008/8935/masteroppgave.pdf

Hove, C., Tårnes, M., Line, M.B. and Bernsmed, K. (2014). Information security incident management: identified practice in large organizations. *In 2014 Eighth International Conference on IT Security Incident Management & IT forensics,* Münster, Germany, May 12-14, 2014, pp. 27-46. IEEE. https://doi.org/10.1109/IMF.2014.10

Howard, M.D., Bhattacharyya, R., Chelian, S.E., Phillips, M.E., Pilly, P.K., Ziegler, M.D., Sun, Y. and Wang, H. (2015). The neural basis of decision-making during sensemaking: Implications for human-system interaction. *In 2015 IEEE Aerospace Conference, Big Sky,* MT, USA, March 07-14, 2015, pp. 1-16. IEEE., https://doi.org/10.1109/AERO.2015.7118968

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4): 247–255. https://doi.org/https://doi.org/10.1016/j.istr.2008.10.010

Hunnebeck, L. and ITIL, R. (2011). Service design. *London: The Stationary Office (TSO)*. [Online] Available from: https://www.academia.edu/42170397/ITIL_Service_Design [Accessed: 22 September 2021].

Husák, M., Jirsík, T. and Yang, S.J. (2020). SoK: Contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual Event*, Ireland, August 25-28, 2020, pp. 1-10. https://doi.org/10.1145/3407023.3407062

Husák, M., Sadlek, L., Špaček, S., Laštovička, M., Javorník, M. and Komárková, J. (2022). CRUSOE: A toolset for cyber situational awareness and decision support in incident handling. *Computers & Security*, 115:102609. https://doi.org/10.1016/j.cose.2022.102609

Hwang, W. and Salvendy, G. (2010). Number of people required for usability evaluation: the 10±2 rule. *Communications of the ACM*, *53*(5):130-133. https://doi.org/10.1145/1735223.1735255

IBM Security. (2022). X-Force Threat Intelligence Index 2022. [Online] Available from: at: https://www.ibm.com/downloads/cas/ADLMYLAZ. [Accessed: 23 July 2022].

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, 31(1): 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Imamverdiyev, Y. (2013). An information security incident prioritization method. In *2013 7th International Conference on Application of Information and Communication Technologies*, Baku, Azerbaijan, 23-25 October 2013, pp. 1-5. IEEE. https://doi.org/10.1109/ICAICT.2013.6722750

INSA (2021). Informaton and Network Security Administration. National cyber security policy and strategy. [Online] Availabe online from: https://www.insa.gov.et/documents/20124/0/National+Cyber+security+Policy%26+StrategyFDRE.docx/03b2d42e-5cb3-f29e-f8f8-fe4ad3d94586?t=1639143692057&download=true. [Accessed 14 September 2021]

INSA (2013). Informaton and Network Security Administration. INSA Reestablishment Proclamation. [Online] Available from: http://www.insa.gov.et/documents/10184/106611/የኢንፎርሜሽን+መረብ+ደህንነት+ኤጀንሲ++እንደገና+ማቋቋሚያ+አዋጅ+ቁ+808-2006+%28Proclamation+No.+808-2013%29.pdf/245a0c67-160f-410b-9490-cfc2fe947ea0?version=1.0 [Accessed 18 February 2018]

Interpol. (2021). African cyberthreat assessment report. *Interpol*, *October*, 1–34. [Online] Available from: https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf [Accessed: 11 January 2022].

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. *2019 International Conference on Cyber-security and Protection of Digital Services (Cyber-security),* Oxford, UK, 03-04 June 2019, pp.1–4, IEEE.

https://doi.org/10.1109/CyberSecPODS.2019.8885240

ISACA. (2012). COBIT 5: Enabling Processes. [Online] Available from: at https://books.google.com.et/books?id=BCpNJtPMCigC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false, USA, ISACA [Accessed: 02 September 2022].

ISO/IEC (2005). International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27002, *Information Technology—Security Techniques—Code of practice for Information Security Management*. [Online] Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en [Accessed: 22 May 2010].

ISO/IEC. (2016). International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27035*: Information Technology — Security Techniques — Information Security Incident Management*. [Online] Available from: https://www.iso.org/standard/44379.html. [Accessed: 29 June 2018]

ITRC. (2023). Identity Theft Resource Center's 2022 annual aata breach report reveals near-record number of compromises. [Online] Available from: https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/. [Accessed: 07 June 2023].

Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., & Longva, O. H. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, *2*(1–2): 26–37. https://doi.org/10.1016/j.ijcip.2009.02.004

Jaferian, P., Hawkey, K., Sotirakopoulos, A., Velez-Rojas, M., & Beznosov, K. (2014). Heuristics for evaluating IT security management tools. *Human-Computer Interaction*, *29*(4): 311–350. https://doi.org/10.1080/07370024.2013.819198

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5): 973–993. https://doi.org/https://doi.org/10.1016/j.jcss.2014.02.005

Janowitz, M. (1961). Television in the lives of our children, *The Impact of Educational Television, Science*, 133(3458):1066-1067. Stanford University Press, Stanford, Calif., 1961. University of Illinois Press,Urbana. https://doi.org/10.1126/science.133.3458.1066

Jashapara, A. (2004). Knowledge management: An integrated approach. Pearson Education. *(1st Edition), Harlow, Essex*. https://books.google.com.et/books/about/Knowledge_Management.html?hl=pl&id=p5Pwvx65TSMC&redir_esc=y, Financial Times

Jeong, K. D., Park, J., Kim, M., & Noh, B.-N. (2008). A security coordination model for an inter-organisational information incidents response supporting forensic process. In *Fourth International Conference on Networked Computing and Advanced Information Management*, Gyeongju, Korea (South),02-04 September 2008, pp.143–148, IEEE. https://doi.org/10.1109/NCM.2008.126

Johnson, E. C. (2006). Security awareness: Switch to a better programme. *Network Security, 2006*(2): 15–18. https://doi.org/10.1016/S1353-4858(06)70337-3

Jones, M., Mccarthy, R. V, & Halawi, L. (2010). Utilizing the technology acceptance model to assess the employee adoption of information systems security measures. *Issues In Information Systems, 11*. Nova Southeastern University https://doi.org/10.48009/1_iis_2010_9-16

Jonker, C. M., Van Riemsdijk, M. B., & Vermeulen, B. (2011). Shared mental models. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6541 LNAI*(Section 2), 132–151. https://doi.org/10.1007/978-3-642-21268-0_8

Jonker, D., Langevin, S., Schretlen, P. and Canfield, C. (2012). Agile visual analytics for banking cyber "big data". *In 2012 IEEE Conference on Visual Analytics Science and Technology (VAST)*, Seattle, WA, USA, 14-19 October 2012, pp. 299-300. IEEE. https://doi.org/10.1109/VAST.2012.6400507

Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32: 489–496. https://doi.org/https://doi.org/10.1016/j.procs.2014.05.452

Jossey,B. (1999). Basic communication model. jsmith library, 25 (3): 2-289. [Online] Available from: https://home.snu.edu/~jsmith/library/body/v25.pdf [Accessed: 11 April 2023]

Jupp, V. (2006). The SAGE Dictionary of Social Research Methods, *(1st Edition)*, London, UK: SAGE Publications Ltd. https://doi.org/10.4135/9780857020116 NV - 0

Kaufhold, M.A., Fromm, J., Riebe, T., Mirbabaie, M., Kühn, P., Basyurt, A.S., Bayer, M., Stöttinger, M., Eyilmez, K., Möller, R. and Fuch, C. (2021). CYWARN: Strategy and technology development for cross-platform cyber situational awareness and actor-specific cyber threat communication. *Workshop-Proceedings Mensch und Computer 2021-Workshopband*, Ingolstadt, Germany, September 05-08, 2021, pp. 1–9. https://doi.org/10.18420/muc2021-mci-ws08-263

Keick, K. E. (1985). Cosmos vs. chaos: Sense and nonsense in electronic contexts. *Organisational Dynamics*, 14(2): 51–64. https://doi.org/https://doi.org/10.1016/0090-2616(85)90036-1

Kemp, S. (2021). Data portal digital Ethiopia. Kepios. [Online] Available from: https://datareportal.com/reports/digital-2021-ethiopia. [Accessed: 05 June 2022].

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, 106: 102267. https://doi.org/10.1016/j.cose.2021.102267

King, W., & He, J. (2006). A meta-analysis of the technology acceptance model. *Information & Management*, 43: 740–755. https://doi.org/10.1016/j.im.2006.05.003

Knight, R. and Nurse, J.R. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, 99:102036.

https://doi.org/10.1016/j.cose.2020.102036

Kossakowski, K.P., Allen, J., Alberts, C., Cohen, C. and Ford, G. (1999). Responding to Intrusions. [Online]Available from: https://apps.dtic.mil/sti/citations/ADA360500 [Accessed: 02 March 2022].

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organisational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, *28*(7): 509–520. https://doi.org/https://doi.org/10.1016/j.cose.2009.04.006

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4): 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Kuechler, W., & Vaishnavi, V. (2012). A framework for theory development in design science research: multiple perspectives. *Journal of the Association for Information Systems*, *13*(6), 3. https://doi.org/1756-0500-5-79 [pii]\r10.1186/1756-0500-5-79

Kurapati, S., Kolfschoten, G. L., Verbraeck, A., Corsi, T. M., & Brazier, F. (2013a). Exploring shared situational awareness in supply chain disruptions. In *Proceedings of the 10th International Conference on Information Systems for Crisis Response and Management*, Baden-Baden, Germany, 12-15 May 2013, pp. 151-155. ISCRAM.

Kurapati, S., Kolfschoten, G. L., Verbraeck, A., Corsi, T. M., & Brazier, F. (2013b). Exploring Shared Situational Awareness using Serious Gaming in Supply Chain Disruptions *(SlideShare Presentation)*. [Online] Available from: https://www.slideshare.net/streamspotter/exploring-shared-situational-awareness-using-serious-gaming-in-supply-chain-disruptions. [Accessed: 09 February 2018].

Kurapati, S., Kolfschoten, G.L., Verbraeck, A., Drachsler, H., Specht, M. and Brazier, F.M. (2012). A Theoretical framework for shared situational awareness in sociotechnical systems, In *Proceedings of the 2nd Workshop on Awareness and Reflection in Technology-Enhanced Learning,* Saarbrücken, Germany, September 12, 2012, (pp. 47-53), *ARTEL@ EC-TEL*

Leach, J. (2003). Improving user security behavior. *Computers & Security*, 22: 685–692. https://doi.org/10.1016/S0167-4048(03)00007-5

Leedy, P.D. and Ormrod, J.E. (2005). *Practical research (Ninth edition),* Saddle River, NJ, Boston, USA: Pearson Education.

Leu, D. J., & Kinzer, C. K. (2000). The convergence of literacy instruction with networked technologies for information and communication. *Reading Research Quarterly*, *35*(1): 108–127. https://doi.org/10.1598/RRQ.35.1.8

Li, Y. and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports,* 7 (8176-8186). https://doi.org/https://doi.org/10.1016/j.egyr.2021.08.126

Lincoln, Y. S. (1995). Emerging criteria for quality in qualitative and interpretive research. *Qualitative Inquiry, SAGE Journals,* 1(3): 275–289. http://qix.sagepub.com/content/1/3/275.full.pdf+html

Lincoln, Y. S., & Guba, E. G. (1986). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New Directions for Program Evaluation*, 1986(30): 73–84. https://doi.org/https://doi.org/10.1002/ev.1427

Linderoth, G., Hallas, P., Lippert, F. K., Wibrandt, I., Loumann, S., Møller, T. P., & Østergaard, D. (2015). Challenges in out-of-hospital cardiac arrest – A study combining closed-circuit television (CCTV) and medical emergency calls. *Resuscitation*, *96*: 317–322. https://doi.org/https://doi.org/10.1016/j.resuscitation.2015.06.003

Line, M.B. and Albrechtsen, E. (2016). Examining the suitability of industrial safety management approaches for information security incident management. *Information & Computer Security*, 24(1):20-37. https://doi.org/10.1108/ICS-01-2015-0003

Line, M. B, Tøndel, M, Jaatun, I, & Martin. G. (2016). Current practices and challenges in industrial control organizations regarding information security incident management - Does size matter? Information security incident management in large and small industrial control organizations. *International Journal of Critical Infrastructure Protection*, 12: 12–26. https://doi.org/10.1016/j.ijcip.2015.12.003

Line, M. B. (2013). A case study: Preparing for the smart grids - Identifying current practice for information security incident management in the power industry. In *2013 Seventh International Conference on IT Security Incident Management and IT Forensics*, Nuremberg, Germany, March 12-14, 2013, pp. 26–32. IEEE. https://doi.org/10.1109/IMF.2013.15

Line, M.B. (2015). Understanding information security incident management practices *(Doctoral dissertation, PhD thesis, Norwegian University of Science and Technology (NTNU))*. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2359707

Lovászová, G., & Michaličková, V. (2016). Classroom learning activities based on real-time response processing, *11th International Scientific Conference on Distance Learning in Applied Informatics, Štúrovo, Slovakia, May 02-04, 2016,* Vol. 1999. pp. 1–6. Wolters Kluwer

Lu, S. and Kokar, M.M. (2015). A situation assessment framework for cyber security information relevance reasoning. *In 2015 18th International Conference on Information* Fusion, Washington, DC, USA, 06-09 July 2015, pp. 1459-1466. IEEE.

Lumen Learning. (2016). Communication for professsionals. [Online] Available from: https://courses.lumenlearning.com/suny-esc-communicationforprofessionals/chapter/communication-process-overview/#:~:text=The interactive or interaction model,contexts (Schramm%2C 1997). [Accessed: 03 July 2022].

Lunenburg, F. C. (2010). Communication: The process, barriers, and improving effectiveness. *Schooling*, *1*(1): 1-10. [Online] Available from: http://unesdoc.unesco.org/images/0026/002610/261016S.pdf [Accessed: 23 October 2019]

Manley, B. and McIntire, D. (2020). A guide to effective incident management communications. *Technical report*. *Carnegie Mellon University. Software Engineering Institute* , [Online] Available from: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=651816 [Accessed: 12 April 2022].

Manyazewal, T., Woldeamanuel, Y., Blumberg, H.M., Fekadu, A. and Marconi, V.C. (2021). The potential of digital health technologies in African context, Ethiopia, 4 (125), 1-13. https://doi.org/10.1101/2021.03.27.21254466

Marinos, L., & Lourenço, M. (2019). ENISA threat landscape report 2018: 15 top cyberthreats and trends. *European Union Agency For Network and Information Security (ENISA)*. DOI 10.2824/622757

Marshall, S. (2016). Quality as sense-making. *Quality in Higher Education*, 22(3): 213–227. https://doi.org/10.1080/13538322.2016.1263924

Maynard, M. T., & Gilson, L. L. (2014). The role of shared mental model development in understanding virtual team effectiveness. *Group & Organisation Management*, *39*(1): 3–32. https://journals.sagepub.com/doi/10.1177/1059601113475361

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research*, *2*. https://doi.org/10.1177/2333393615597674

McQuail, D., & Windahl, S. (2015). Communication models for the study of mass communications (2nd Edition). *Pearson Education, London, UK, Routledge*. https://books.google.com.et/books?id=rn5ACwAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Metzger, S., Hommel, W., & Reiser, H. (2011). Integrated security incident management - Concepts and real-world experiences. In *Proceedings of the 6th International Conference on IT Security Incident Management and IT Forensics,* Stuttgart, Germany,10-12 May 2011, pp. 107–121, IEEE. https://doi.org/10.1109/IMF.2011.15

Miloslavskaya, N., & Tolstoy, A. (2020). IoTBlockSIEM for information security incident management in the internet of things ecosystem. *Cluster Computing*, 23(3): 1911–1925. https://doi.org/10.1007/s10586-020-03110-5

MINT (2021). Ministry of Innovation and Technology. Innovation and ICT Policy. [Online] Available from: https://mint.gov.et/?lang=en. [Accessed: 25 May 2022]

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers and Security*, 109: 102383. https://doi.org/10.1016/j.cose.2021.102383

Mlekus, L., Bentler, D., Paruzel, A., Kato-Beiderwieden, A.-L., & Maier, G. W. (2020). How to raise technology acceptance: user experience characteristics as technology-inherent determinants. *Gruppe. Interaktion. Organisation. Zeitschrift Für Angewandte Organisationspsychologie (GIO)*, 51(3): 273–283. https://doi.org/10.1007/s11612-020-00529-7

Moise, G. (2008). Communication models used in the online learning environment. In *Proceedings of the 3rd International Conference on Virtual Learning,* Cape Town, South Africa, June 26-27, 2008, Vol.254, pp. 247-254. https://ceur-ws.org/Vol-2401/PAPER_5.PDF

Morse, J.M., Barrett, M., Mayan, M., Olson, K. and Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International Journal of Qualitative Methods*, 1(2):13-22. https://doi.org/10.1177/160940690200100202

Mujinga, M., Eloff, M., & Kroeze, J. (2018). System usability scale evaluation of online banking services: A South African study. *South African Journal of Science, 114*. https://doi.org/10.17159/sajs.2018/20170065

Munkvold, B. E., & Bygstad, B. (2016). The Land of Confusion–Clearing up some common misunderstandings of interpretive research. In *NOKOBIT-Norsk Konferanse for Organisasjoners Bruk av Informasjonsteknologi* (Vol. 24, No. 1). Bibsys Open Journal Systems.

Nielsen, J. (2010). User Experience Re-Mastered, In C. Wilson (Ed.), (pp. 3–22). London: Morgan Kaufmann Publishers. https://doi.org/https://doi.org/10.1016/B978-0-12-375114-0.00004-9

Nofi, A. A. (2000). Defining and measuring shared situational awareness center for naval analyses. *Technical Report CRM D0002895.A1/Final, November*. [Online] Available from: https://www.cna.org/reports/2000/D0002895.A1.pdf [Accessed: 22 December 2018].

Nordby, H. (2011). The nature and limits of interactive communication: A philosophical analysis. *International Journal of Media, Technology and Lifelong Learning* Seminar.net, 7(1). https://doi.org/10.7577/seminar.2414

Noskova, T., Pavlova, T., Yakovleva, O., Malach, J., & Kostolányová, K. (2016). Approach to selecting ICT tools for formative assessment, *11th International Scientific Conference on Distance Learning in Applied Informatics,* Štúrovo, Slovakia, May 02-04, 2016, Vol. 1999. pp. 1–6. Wolters Kluwer

Nyman, M. and Große, C. (2019). Are you ready when it counts? IT consulting firm's information security incident management. In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019),* Sundsvall, Sweden, February 23-25, 2019 (pp. 26-37). https://doi.org/10.5220/0007247500260037

Nyre-Yu, M., Gutzwiller, R. S., & Caldwell, B. S. (2019). Observing cyber security incident response: qualitative themes from field research. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* Seattle, Washington, USA, October 28-November 01, 2019, (Vol. 63, No. 1, pp. 437-441). SAGE Publications. https://doi.org/10.1177/1071181319631016

O'Brien, A., Read, G.J. and Salmon, P.M. (2020). Situation awareness in multi-agency emergency response: Models, methods and applications. *International Journal of Disaster Risk Reduction*, 48:101634. https://doi.org/10.1016/j.ijdrr.2020.101634

O'leary, Z. (2007). The social science jargon buster: The key terms you need to know. *(1st Edition).* London. Sage Publications. https://us.sagepub.com/en-us/nam/the-social-science-jargon-buster/book229115

Oates B. (2006). Researching information systems and computing, *(1st Edition)*, London: SAGE Publications. https://dl.acm.org/doi/book/10.5555/1202299

Olav Sveen, F., Sarriegi, J. M., Rich, E., & Gonzalez, J. J. (2007). Toward viable information security reporting systems. *Information Management & Computer Security*, 15(5): 408-419. https://doi.org/10.1108/09685220710831143

Osterle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A. and Sinz, E.J. (2011). Memorandum on design-oriented information systems research. *European Journal of Information Systems*, 20(1):7-10. https://doi.org/10.1057/ejis.2010.55

Oppenheim, C., Stenson, J., & Wilson, R. M. S. (2004). Studies on information as an asset III: Views of information professionals. *Journal of Information Science*, *30*(2): 181–190. https://doi.org/10.1177/0165551504042809

Oriola, O., Adeyemo, A. B., Papadaki, M., & Kotzé, E. (2021). A collaborative approach for national cybersecurity incident management. *Information and Computer Security*, 29(3): 457–484. https://doi.org/10.1108/ICS-02-2020-0027

Padayachee, K. (2015). An insider threat neutralisation mitigation model predicated on cognitive dissonance (ITNMCD). *South African Computer Journal*, 56(1): 50-79. https://doi.org/10.18489/sacj.v56i1.263

Padayachee, K. (2021). A theoretical underpinning for examining insider attacks leveraging the Fraud Pentagon. In *Human Aspects of Information Security and Assurance:* In *Proceedings of the 15th IFIP WG 11.12 International Symposium,* HAISA 2021, Virtual Event, July 7–9, 2021, (pp. 179-188), *Part of the IFIP Advances in Information and Communication Technology (IFIPACIT) Book series, Volume 613,* Springer International Publishing.

Padayachee, K., & Worku, E. (2020). A coordinated communication & awareness approach for information security incident management: An empirical study on Ethiopian organisations, *The African Journal of Information Systems,* 12(2): 1.

Padayachee, K., & Worku, E. (2017). Shared situational awareness in information security incident management. *12th International Conference for Internet Technology and Secured Transactions (ICITST),* Cambridge, UK ,11-14 December 2017, pp. 479–483, IEEE. https://doi.org/10.23919/ICITST.2017.8356454

Palmqvist, M. (2022). Are we focusing on the right things?: A systematic literature review on causes of cybersecurity incidents. [Online] Available from: https://www.diva-portal.org/smash/get/diva2:1666986/FULLTEXT01.pdf [Accessed: 15 January 2023].

Papastergiou, S., Mouratidis, H., & Kalogeraki, E. M. (2019). Cyber security incident handling, warning and response system for the European critical information infrastructures (cybersane). In *20th International Conference on Engineering Applications of Neural Networks (EANN), Communication in Computer and Information Science Book series,* Crete, Greece, May 24-26, 2019, pp. 476-487. Springer International Publishing.

Peffers, K., Rothenberger, M., Tuunanen, T. and Vaezi, R. (2012). Design science research evaluation. In *Proceedings of the 7th International conference In Design Science Research in Information Systems. Advances in Theory and Practice (DESRIST),* Las Vegas, NV, USA, May 14-15, 2012. pp. 398-410. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-29863-9_29

Peffers, K., Tuunanen, T., Gengler, C.E., Rossi, M., Hui, W., Virtanen, V. and Bragge, J. (2020). Design science research process: A model for producing and presenting information systems research. In *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology*, Claremont, California, USA, pp. 83-16. 2006, *arXiv preprint arXiv:2006.02763*.

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information systems*, 24(3): 45-77.

Perera, C., Zaslavsky, A., Christen, P., Compton, M. and Georgakopoulos, D. (2013). Context-aware sensor search, selection and ranking model for Internet of Things middleware. In *14th International Conference on Mobile Data Management (MDM)*, Milan, Italy, 03-06, June 2013,Vol. 1, pp. 314-322). IEEE. https://doi.org/10.1109/SURV.2013.042313.00197

Persad, K., & Padayachee, K. (2015). The factors that influence customer e-services adoption. *South African Computer Journal*, *56*(1): 80-106. https://doi.org/10.18489/sacj.v56i1.209

Petersons, A. and Khalimzoda, I. (2016). Communication models and common basis for multicultural communication in Latvia. In *Proceedings of the International Scientific Conference,* Rēzekne, Latvia, May 27-28, 2016,Vol. 4, pp. 423-433. https://doi.org/10.17770/sie2016vol4.1555

Ponterotto, J. G. (2005). Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science. *Journal of Counseling Psychology, 52*, 126–136. https://www.semanticscholar.org/paper/Qualitative-research-in-counseling-psychology%3A-A-on-Ponterotto/7fe9b067babc0812c1f31b04626397111635fa9d

Posthumus, S. and Von Solms, R. (2004). A framework for the governance of information security. *Computers & security,* 23(8): 638-646. https://doi.org/10.1016/j.cose.2004.10.006

Potgieter, B.C., Botha, J.H. and Lew, C. (2005). Evidence that use of the ITIL framework is effective, In *18th Annual Conference of the National Advisory Committee on Computing Qualifications,* Tauranga, New Zealand, 10-13 July 2005, pp. 160-167. ITIL

Pöyhönen, J., Nuojua, V., Lehto, M., & Rajamäki, J. (2019). Cyber situational awareness and information sharing in critical infrastructure organisations. *Information & Security: An International Journal*, 43(2): 236–256. https://doi.org/10.11610/isij.4318

Proença, D., & Borbinha, J. (2018). Information security management systems-a maturity model based on ISO/IEC 27001. In *Proceedings of the 21st International Conference on Business Information Systems (BIS),* Berlin, Germany, July 18-20, 2018, Vol. 320, pp. 102-114. Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-93931-5_8

Purao, S., & Storey, V. C. (2008). Evaluating the adoption potential of design science efforts: The case of APSARA. *Decision Support Systems*, 44(2): 369–381. https://doi.org/10.1016/j.dss.2007.04.007

Rapanyane, M. B., & Sethole, F. R. (2020). The rise of artificial intelligence and robots in the 4th Industrial Revolution: implications for future South African job creation. *Contemporary Social Science*, 15(4): 489–501. https://doi.org/10.1080/21582041.2020.1806346

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety science*, 27(2-3):183-213.

Reba, B.B. (2005). Ethiopian Telecommunications Agency State of Cyber Security in Ethiopia. [Online] Available from: https://www.scribd.com/document/481126981/STATE-OF-CYBER-SECURITY-IN-ETHIOPIA [Accessed: 11 February 2018]

Reid, R. and Van Niekerk, J. (2014). From information security to cyber security cultures, In *Proceedings of the 2014 Information Security South Africa (ISSA) Conference*, Johannesburg, South Africa, August 13-14, 2015, pp. 1-7. IEEE https://doi.org/10.1109/ISSA.2014.6950492

Reiter, B. (2013). The epistemology and methodology of exploratory social science research : Crossing popper with marcuse. *Government and International Affairs Faculty Publications*. *Univerity of South Florida*, *Paper 99*. [Online] Available from: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1099&context=gia_facpub [Accessed: 02 March 2022].

Riebe, T., Kaufhold, M. A., & Reuter, C. (2021). The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: An empirical study. In *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), Málaga Spain, September 22-24, pp. 1-30, Association for Computing Machinery. https://doi.org/10.1145/3479865.

Salas, E., Stout, R.J. and Cannon-Bowers, J.A. (1994). The role of shared mental models in developing shared situational awareness. *Situational Awareness in Complex Systems*, pp. 297-304. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315087924-18/role-shared-mental-models-developing-team-situational-awareness-implications-training-renée-stout-janis-cannon-bowers-eduardo-salas

Salmon, P. M., Stanton, N. A., Walker, G. H., Baber, C., Jenkins, D. P., McMaster, R., & Young, M. S. (2008). What really is going on? Review of situation awareness models for individuals and teams. *Theoretical Issues in Ergonomics Science*, *9*(4): 297–323. https://doi.org/https://doi.org/10.1080/14639220701561775

Sandberg, J., & Alvesson, M. (2011). Ways of constructing research questions: gap-spotting or problematization?. *Organization*, 18(1):23-44. https://www.semanticscholar.org/paper/Ways-of-constructing-research-questions%3A-or-Sandberg-Alvesson/4d3a728dcf892e41a465a4dc8a1afb43f87e3627

Sapienza, Z.S., Iyer, N. and Veenstra, A.S. (2015). Reading Lasswell's Model of communication backward: Three scholarly misconceptions. *Mass Communication and*

Society Society, 18(5): 599–622. https://www.tandfonline.com/doi/full/10.1080/15205436.2015.1063666

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, 7: 1-29. https://doi.org/10.1186/s40537-020-00318-5

Sarker, S., Chatterjee, S., & Xiao, X. (2013). How “sociotechnical” is our IS research? An assessment and possible ways forward. *Thirty Fourth International Conference on Information Systems,* Milan, Italy, December 15-18, pp. 1–24, ICIS. https://pdfs.semanticscholar.org/e3ca/6fe6e62dac801e9d3b0fe07a1a0d89b53657.pdf

Sarker, S., Chatterjee, S., Xiao, X., & Elbanna, A. (2019). The sociotechnical axis of cohesion for the IS discipline: Its historical legacy and its continued relevance. *Management Information Systems Quarterly,* 43(3): 695-720. https://doi.org/10.25300/MISQ/2019/13747

Saunders, M., Lewis, P., & Thornhill, A. (2009). Understanding Research Philosophies and Approaches. *Research Methods for Business Students*, 4, 106-135. https://www.scirp.org/(S(351jmbntvnsjt1aadkozje))/reference/referencespapers.aspx?referenceid=2807274

Saunders, M., Lewis, P. and Thornhill, A. (2019). Research methods for business students' Chapter 4: Understanding research philosophy and approaches to theory development, (pp. 128–171) Cambridge Management and Leadership School

Scarfone, K., Grance, T., & Masone, K. (2008). Computer security incident handling guide. *NIST Special Publication*, 800(61): 38. [Online] Available from: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf [Accessed: 09 May 2019]

Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys & Tutorials*, 23(4):2525–2556. https://doi.org/10.1109/COMST.2021.3117338

Schramm W. (1997). The Beginnings of Communication Study in America: A personal memoir *(1st Edition),* London*:* SAGE Publications. https://us.sagepub.com/en-us/nam/the-beginnings-of-communication-study-in-america/book3053

Schramm, W. (1954). *The process and effects of mass communication (2nd Edition),* Univerity of Illionois press, Urbana, III. https://books.google.com.et/books/about/The_Process_and_Effects_of_Mass_Communic.html?id=qAYEAQAAIAAJ&redir_esc=y

Sellnow, D.D. (2005). *Confident public speaking. (*2nd Edition). Rhode Island, United States: Thomson/Wadsworth. Cengage Learning

Sikolia, D., Biros, D., Mason, M. and Weiser, M. (2013). Trustworthiness of grounded theory methodology research in information systems. In *Proceedings of the Eighth Midwest Association for Information Systems Conference,* Normal, Illinois, USA, May 24-25, 2013, pp. 1-5. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1006&context=mwais2013*AIS*

Electronic Library (AISeL). MWAIS

Siponen, M. T. (2000). A conceptual foundation for organisational information security awareness. *Information Management & Computer Security,* 8(1): 31–41. https://doi.org/https://doi.org/10.1108/09685220010371394

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. *In New Approaches for Security, Privacy and Trust in Complex Environments:* In *Proceedings of the IFIP International Information Security Conference, part of the IFIP International Federation for Information Processing Book Series,* Sandton, South Africa, 14–16 May 2007, Vol 232, pp. 133-144. Springer Publishing. https://doi.org/https://doi.org/10.1007/978-0-387-72367-9_12

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information and Management*, *48*(7): 296–302. https://doi.org/10.1016/j.im.2011.07.002

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end-user security behaviors. *Computers and Security*, *24*(2): 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Stanton, N. A., Chambers, P. R., & Piggott, J. (2001). Situational awareness and safety. *Safety science, 39*(3): 189-204. https://doi.org/10.1016/S0925-7535(01)00010-8

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., Zaccaro, S. J., Dalal, R. S., & Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Security & Privacy,* 13(4): 20–29. https://doi.org/10.1109/MSP.2015.71

Syahrial, H., Prabowo, H., Budiastuti, D., & Gaol, F. L. (2019). Information security policy compliance model at Indonesian government institutions: A conceptual framework. In *Proceedings of the International Conference on Data Engineering,* Macao, China , April 08-11, 2019,pp. 393-401. Springer Singapore.

Tamassia, R., Palazzi, B., & Papamanthou, C. (2009). Graph drawing for security visualization. In *Graph Drawing: 16th International Symposium, GD 2008, Heraklion, Crete, Greece, September 21-24, 2008. Revised Papers 16* (pp. 2-13). Springer Berlin Heidelberg. https://link.springer.com/content/pdf/10.1007/978-3-642-00219-9_2.pdf

Thangavelu, M., Krishnaswamy, V. and Sharma, M., (2020). Comprehensive Information Security Awareness (CISA) in Security Incident Management (SIM): A Conceptualization. *South Asian Journal of Management, 27*(2), 160–188. https://www.proquest.com/openview/647b8bbb346265a37c4ef957f8b94f8b/1?pq-origsite=gscholar&cbl=46967

Thangavelu, M., Krishnaswamy, V., & Sharma, M. (2021). Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study. *Computers & Security,* 109: 102401. https://doi.org/https://doi.org/10.1016/j.cose.2021.102401

Tompkins, P. (1984). Functions of communication in organizations. In C. Arnold & J. W. Bowers (Eds.), *Handbook of Rhetorical and Communication Theory* (pp. 659-719). New

York: Allyn & Bacon

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45: 42–57. https://doi.org/https://doi.org/10.1016/j.cose.2014.05.003

UOM. (2019). University of Minnesota. Communications in the real world. [Online] Available from: at https://open.lib.umn.edu/communication/chapter/1-2-the-communication-process [Accessed: 23 April 2023].

Urquhart, C., Lam, L., Cheuk, B., & Dervin, B. (2016). Sense-Making/Sense-making. *Oxford Bibilographis*. [Online] Available from: https://doi.org/10.1093/obo/9780199756841-0112 [Accessed: 11 July 2020]

Valecha, R., Sharman, R., Rao, H.R. and Upadhyaya, S. (2012). Messaging model for emergency communication. In *Proceedings of the Mid-West Association of Information Systems (MWAIS)*.5-2012, Las Vegas, NV, 2012, pp. 1-7. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1002&context=mwais2012

Van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. *Computers & Security*, 113: 102535. https://doi.org/https://doi.org/10.1016/j.cose.2021.102535

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication*, 20: 113–132. https://doi.org/10.23962/10539/23573

van Wyk, Q., van Biljon, J. and Schoeman, M. (2020). Knowledge visualization for sensemaking: Applying an elaborated action design research Process in Incident Management Systems. In *Proceedings of the 15th International Conference on Design Science Research in Information Systems and Technology, In designing for Digital Transformation. Co-Creating Services with Citizens and Industry*, Kristiansand, Norway, December 2–4, 2020, pp. 142-153. Springer International Publishing.

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers and Security*, 105: 102239. https://doi.org/10.1016/j.cose.2021.102239

Velten, J. C., & Arif, R. (2016). The influence of snapchat on interpersonal relationship development and human communication. *The Journal of Social Media in Society*, 5(2): 5–43. https://thejsms.org/index.php/JSMS/article/view/152

Villegas-Ch, W., Ortiz-Garces, I., & Sánchez-Viteri, S. (2021). Proposal for an implementation guide for a computer security incident response team on a university campus. *Computers*, 10(8): 102. https://doi.org/10.3390/computers10080102

Vroom, C. and von Solms, R. (2002). A practical approach to information security awareness in the organization. S*ecurity in the Information Society: Visions and Perspectives, Springer US*, 86 (19-37). https://doi.org/10.1007/978-0-387-35586-3_2

Vroom, C. and Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, 23(3): 191–198. https://doi.org/10.1016/j.cose.2004.01.012

Wang, K., Guo, X., & Yang, D. (2022). Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks. *Electronics,* 11(10): 1659. https://doi.org/10.3390/electronics11101659

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security,* 44: 1–15. https://doi.org/10.1016/j.cose.2014.04.005

Weber, S. (2010). Design Science Research: Paradigm or Approach?" (2010). In P*roceedings of the Sixteenth Americas Conference on Information Systems,* Lima, Peru, August 12-15, 2010.pp. 1-8. AISEL. https://aisel.aisnet.org/amcis2010/214

Weick, K.E. (1995). Sensemaking in organizations *(Vol. 3). Sage. Thousand Oaks, London, CA*: Sage.https://us.sagepub.com/en-us/nam/sensemaking-in-organizations/book4988

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sense-making. *Organisation Science,* 16(4): 409–421. https://doi.org/10.1287/orsc.1050.0133

Weick, K. E. (2009). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Studi Organizzativi,* (2008/2). https://doi.org/10.3280/so2008-002009

Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security,* 18(1): 26–42. https://doi.org/10.1108/09685221011035241

Wood, J. T. (2014). Communication in our lives *(7th Edition). Ceneage Learning .Boston, Wadsworth*. [Online] Available from: http://staffnew.uny.ac.id/upload/132310007/pendidikan/ebook-julia-t-wood-communication-our-lives-2008.pdf [Accessed: 17 April 2022].

Wooding, S., Anhal, A., & Valeri, L. (2003). Raising citizen awareness of information security: A practical guide. *Report, eAware consortium*. [Online] Available from: https://clusit.it/wp-content/uploads/whitepapers/eaware_practical_guide.pdf [Accessed 02 September 2019].

Yang, S. J., Byers, S., Holsopple, J., Argauer, B., & Fava, D. (2008). Intrusion activity projection for cyber situational awareness. In *2008 IEEE International Conference on Intelligence and Security Informatics,* Taipei, Taiwan, 17-20 June 2008, pp. 167-172. IEEE, https://doi.org/10.1109/ISI.2008.4565048

Yilma, K. M. (2014). Developments in cybercrime law and practice in Ethiopia. *Computer Law and Security Review*, 30(6): 720–735. https://doi.org/10.1016/j.clsr.2014.09.010

Yohannes, T., Lessa, L., & Negash, S. (2019). Information security incident response management in an Ethiopian bank: A Gap Analysis. *Twenty-Fifth Americas Conference on Information Systems,* Cancun, Mexico, August 15-17,2019, pp. 1–13. AISEL https://aisel.aisnet.org/amcis2019/adv_info_systems_research/adv_info_systems_research/22/

Yufik, Y. (2014). Situational awareness, sensemaking, and situation understanding in cyber warfare. *Cybersecurity Systems for Human Cognition Augmentation, 1-18, Advances in Information Security, Book Series, Volume 61,* Springer International Publishing.

https://doi.org/10.1007/978-3-319-10374-7_1

Zamani, E. D., Pouloudi, N., Giaglis, G., & Wareham, J. (2021). Accommodating practices during episodes of disillusionment with Mobile IT. *Information Systems Frontiers*, 23: 453-475. https://doi.org/10.1007/s10796-019-09972-4

Zhang, S., le Fever, H. T., & le Zhang S, F. H. (2013). An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model. *Journal of Economics, Business and Management*, 1(4): 391-395. https://doi.org/10.7763/joebm.2013.v1.84

APPENDICES

APPENDIX A: Survey Questionnaire and Interview Questions – Phase I

TITLE OF THE STUDY:

A Coordinated Communication and Awareness Approach towards the enhancement of Information Security Incident Management

Consent Statement

- The aim of this research is to explore and develop an information security incident management model by integrating awareness and communication aspects with stakeholders' and end-users' participation.
- The research objective is not intended to exhaustively and explicitly study your routine organisational practice of information security policies or any data related matters pertaining to your organisation or employees.
- The responses that you provide for the researcher in this interview questionnaire will be kept confidential and anonymous. The data collected will only be used for research purposes. Moreover, any personally or organisationally identifying information will not be published.
- The researcher will record your interview or the parts thereof which will help with the analysis of the research. Your name, address and any personal affiliation will be kept private and coded for research purposes only. You have the right not to respond to all or some of the questions which you are not interested in. Moreover, in case you are not interested in responding to all or some of the questions ahead, you have the right to withdraw from the interview.

PART 1: INTERVIEW QUESTIONNAIRE (EXPERTS and END-USERS)

Background

1.1. How many employees currently work in your organisation?

1.2. To which of the following organisational categories does your organisation belong?

Organisational category	**Specialization**
Government organisation	□Education □Service □Health □Military □Technology □Energy
Non-governmental organisation	□Local NGO □International NGO
Private Sector	□Commercial □Non-commercial
Corporate organisation	□
Security organisation	□
Public relations & Marketing	□
Other	□

1.3. Which of the following Information systems does your organisation deploy and utilize?

□ Business and Commercial Information Systems
□ Customer Information Systems
□ Employee Management
□ Data and Information Security
□ National Security Systems
□ Telecom & Network systems
□ Other___________________________________

1.4. Which of the following information security mechanisms does your organisation utilize?

Information security mechanism	**Specific methods**
Technical Information Security	□Antivirus and Anti-spyware □Firewall □Virtual private network □Encryption & Decryption □Intrusion and Detection System (IDS) □Endpoint □Backup and restore □Wireless security
Physical Information security	□Room □Human security □Hardware
System and Data Security	□Systems and network security □Business communications security □Web and application security
Non-Technical Information security	□Security employee training and awareness □Security policies and procedures □Policy: Corporate security policy, password policy, hiring and disciplinary policy
Other	□

1.5. Which of the following aspects of information security awareness issues are addressed in your organisational information security policy document?

□ Security incident handling
□ Risk awareness
□ Account usage (Username and Password)
□ Internet application (Email, Downloading, and social media utilization)
□ Software installation
□ Antivirus installation and usage
□ Other__________________________

1.6. Does your organisation have a specific policy document on information security incident management issues?

1.7. If your answer to the above question is 'NO', provide possible reasons for the lack of information security and incident management policies?

2. Information security incident management

2.1. Which of the following role-players in your organisation is assigned the responsibility of developing incident management processes?

□ ICT office
□ Management or Executive body
□ National regulatory body
□ Organisational stakeholders
□ Other ____________________________

2.2 Which of the following management levels plays an active role in awareness and communication regarding information security incident management?

□ Top-Level Management
□ Middle-Level Management
□ Low-Level Management
□ Not Applicable

2.3. Describe the role that management currently plays/should play in information security incident awareness?

2.4. Describe the role that management currently plays/should play in information security incident communication?

2.5. Which of the following standards does your organisation currently comply?

□ ISO/IEC 27001
□ ISO/IEC 27002 Standard
□ ISO/IEC 27035 Standard
□ The ITIL Framework
□ NIST Special Publication 800-61
□ ENISA - Good Practice Guide for Incident Management
□ Nor SIS - Guideline for Incident Management
□ SANS: Incident Handler's Handbook
□ COBIT 5
□ ISMM
□ IEEE 802.11
□ Other __________________

2.6. If your organisation uses any of the above information security management standards, how does it implement this with respect to information security incident management processes?

2.7. If your organisation does not apply any of the above information security incident management standards, provide possible reasons for the lack of standard usage.

2.8. Does your organisation have any formal agreement with employees regarding information security incident management process issues?

□ Yes
□ No

2.9. If your answer to the above question is 'NO', provide possible reasons for the lack of such agreement between the organisation and the employees.

2.10 Assess your organisations information security incident management processes

No	**How does the organisation manage the following incident management processes?**	**Does it have a formal document?**	**Do they plan for it?**	**Is it supported by ICT systems?**	**Is it supported by Decision Makers?**
1	Incident preparation and definition				
2	Incident identification/detection				
3	Incident assessment and analysis				
4	Incident response				
5	Incident awareness, understanding, anticipation and knowledge of employees				
6	Incident communication and reporting				
7	Information security policy efficiency				

2.11. Rate the level of information security incident awareness and risk understanding of employees with respect to the following indicators? **(***Excellent, Very good, Good, Satisfactory, Fair, Poor)*

No	**Information security incident awareness indicators**	**Top-Level Mgt**	**Middle-Level Mgt**	**Low-Level Mgt**	**End-Users**	**ICT Experts**
1	Knowledge about ICT system and components					
2	Information security competence					
3	Reporting security incidents					

4	Up-to-date knowledge about relevant threats					
5	Learning from previous incidents					

2.12. Does your organisation have a specific workflow for information security incident management processes?

□ Yes

□ No

2.13 If you have answered 'YES' to the previous question, comment on the following aspects:

2.13.1 How is it prepared and maintained?

2.13.2. How is it communicated to the members of the incident management team?

2.14. Which of the following methods support managers in increasing awareness of information security incident management policies in your organisation?

No	Awareness raising methods	Description and specific tools
1	□**Promotional methods**	Screen savers, Banners on the intranet, Hyperlinks from the intranet homepage to the security page, Articles in the internal publication, Posters, Puzzles and games, Pre-printed note pads or sticky notes, T-shirts, Mugs and cups, Mouse pads, Stickers
2	□**Enforcing methods**	Underwriting security principles, Confidentiality agreements, Required awareness exam or test, Disciplinary actions for non-compliance, Inclusion in annual evaluations or, promotion criteria, Rewarding mechanisms
3	□**Educational methods**	Slide presentation, training, brief targeted session, Online learning module, Demonstration, Video, Workshops
4	□**Informational methods**	Leaflets, Short articles or news stories, Intranet security web site postings, E-mail warnings, Information security guides, Tips-of-the-month, Flash cards, Newsletters
5	□**Digital methods**	CD-ROM or DVD materials, simulated production, Audio-visual tools, Online methods, Closed Circuit TV
6	□**Face-to-face guidance method**	

2.15. Which of the following reporting mechanisms does your organisation use to communicate to the staff about information security incidents?

□ Telephone reporting

□ Manual/paper based reporting

□ Face-to-face contact or meeting
□ Electronic means (E-mail, Social media, Mobile phone)
□ Audio-visual/Multimedia format
□ Special software application for incident reporting
□ Other______________________________

2.16. How would you assess the level of an employee's communication experience with respect to information security incident management among different clusters of employees in your organisation?

No	**Employee Cluster**	**Excellent**	**Very Good**	**Good**	**Satisfactory**	**Fair**	**Poor**
1	Top-Level management						
2	Middle-Level management						
3	Low-Level management						
4	End-users						
5	ICT Experts						

2.17. How frequently does your organisation communicate information security incidents?
□ When an incident happens
□ Quarterly
□ Bi-annually
□ Weekly
□ Annually
□ Monthly
□ Other_________________________

2.18. How does your organisation communicate and report information security incidents to employees?

2.19. In your opinion, what should be done to improve the awareness and communication strategies among employees and stakeholders in order to enhance information security incident management in your organisation?

2.20. What kind of challenges does your organisation face regarding information security incident communication and awareness cases?

2.21. In your opinion, how can communication with regard to information security incident management be effectively integrated into your organisational information security policy?

3. Information Security Incident Management and End-users' involvement

3.1. Identify the role and relation of the various stakeholders with regard to Information security incident management issues in your organisation.

Stakeholder	**Role**
All staff members	
Line management	
Executive management and boards of directors	
Field staff	
Laptop users	
IT department	
IT help desk	
System and/or data owners	
E-mail users	
Vendors and suppliers	
Other__________________	

3.2. Does your organisation involve end-users in the process of information security incident awareness and communication matters?

□ Yes
□ No

3.3. If your answer is 'YES' to the above question, describe how your organisation involves end-users in the process of information security and incident management policy issues?

3.4. If your answer is 'NO' to question No 3.2, describe the reason why your organisation does not involve end-users in the process of information security policy awareness and communication matters.

3.5. Which information security incident cases, regarding end-users, are taken into account by the organisation?

□ All security cases
□ Only non-technical cases
□ Only technical cases
□ Some higher level policy issues
□ Other__________________________

PART 2: Interview Questions (End-Users Only)

1. Have you ever been involved in the setting of information incident security management guidelines in your organisation?

2. If your answer to the above question is 'YES', describe your level of participation.

3. Have you ever participated in an information security incident awareness program?

4. If your answer to the above question is ‘YES’, describe your role with regard to communication and awareness aspects to improve information security incident management in your organisation?

5. If your answer to the question 3 is 'NO', what should your organisation put into practice to involve end-users and stakeholders to become aware and communicate with them, in order to improve information security incident management?

6. In your opinion, how can your organisation plan and prepare better information security management through awareness and communication mechanisms?

NOTE:

This questionnaire was published in a journal for the purposes of attaining feedback on the consistency of some the arguments of the research.

APPENDIX B: Evaluation Survey Questionnaire – Phase II—Iteration I

The following questions are derived from the design science and evaluation constructs. The questionnaire is divided into three sections. The first section presents the biographical data, the second section comprises the model acceptance and the third section incorporates the model validity and reliability.

SECTION I: BIOGRAPHICAL INFORMATION

A. Indicate your gender

	Male
	Female

B. Select your job title (category) from the list below:

	IT Security Manager
	IT Security Administrator
	IT Security Consultant
	IT Security Incident Response Team Member
	IT Security Incident Manager
	IT Security Auditor
	IT Risk Analysis Officer
	IT Security Academic
	End-User
	Other

C. Indicate your age in years

D. Indicate your years of experience in IT Security

E. Indicate your country of residence

SECTION 2: MODEL ACCEPTANCE

The following questions are designed to evaluate the proposed model and prototype. The aim of the questionnaire is to obtain the opinions of experts and users about the proposed model and prototype. This section consists of **11** questions. There are five response options available (from Strongly Agree to Strongly Disagree) for each question.

Kindly select the most appropriate option below.

Construct	Question	Reference
Intent to Use	1. Assuming I had access to a system similar to the prototype, I intend to use it in an incident response scenario to assist in the coordination of communication and awareness efforts with respect to responding and resolving information security incidents. [ ] Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree Comment: __________	Adapted from (Davis & Venkatesh, 2004)
	2. Assuming I had access to a system similar to the prototype, I intend to use it to enhance my awareness about organisational information security incidents. [ ] Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree Comment: __________	Adapted from (Davis & Venkatesh, 2004)
Intent to Use	3. Given that I had access to the system, I predict that I would use the system of communication and awareness towards achieving collaborative and proactive information security incident reporting. [ ] Strongly Agree [ ] Agree [ ] Neutral	Adapted from (Davis & Venkatesh, 2004)

	[ ] Disagree [ ] Strongly Disagree Comment: __________	
Perceived Usefulness	4. Using a system based on the model concept will increase my effectiveness in reporting an information security incident. [ ] Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree Comment: __________	Adapted from (Davis & Venkatesh, 2004)
	5. I would find a system based on the model concept useful towards achieving a shared, interactive and participatory platform for the coordination and management of information security incidents. [ ] Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree Comment: __________	Adapted from (Purao & Storey, 2008) and (Davis & Venkatesh, 2004)
	6. I would find a system based on the model concept valuable towards enhancing my effectiveness in an incident response scenario by maximising the coordination of communication and awareness efforts with respect to information security incidents. [ ] Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree Comment: __________	Adapted from (Purao & Storey, 2008) and (Davis & Venkatesh, 2004)
Ease of Use	7. I would find a system based on the model concept easy to use in an incident response scenario. [ ] Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree Comment: __________	Adapted from (Purao & Storey, 2008) , (Mujinga, Eloff, & Kroeze, 2018) and

		(Davis & Venkatesh, 2004)
	8. Interacting with the system will not require huge mental effort. [ ] Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree Comment: _________	Adapted from (Davis & Venkatesh, 2004)
	9. My interaction with a system based on the model concept will enable a shared mental model of an information security incident thereby easing the incident management process. [ ] Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree Comment: _________	Adapted from (Davis & Venkatesh, 2004)
Compatibility and Scalability	10. Using the system would be compatible with my own existing organisational system design. [ ] Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree Comment: _________	Adapted from (Purao & Storey, 2008) and (Padayachee, 2015)
	11. If the system is scalable, it will potentially be used by many users on a wider scale in an incident response scenario. [ ] Strongly Agree [ ] Agree [ ] Neutral [ ] Disagree [ ] Strongly Disagree Comment: _________	Adapted from (Albers & Lohmeyer, 2012) and (Padayachee, 2015)

SECTION 3: MODEL VALIDITY AND RELIABILITY

The following are open-ended questions to be completed by information security experts as part of the evaluation process for the model and prototype.

Kindly take your time when answering the questions below.

Construct	**Question**	**Reference**
Abstraction	12. Do you think that the model concept (the application of situational awareness and the Interactive Communication Model) can conceptually resolve the problems associated with the poor coordination of awareness and communication of security incidents? [ ] Yes [ ] No Please give reasons for your answer__________________	(Osterle et al., 2011)
Originality	13. Is the model concept unique in its aim of integrating situational awareness and communication models for easing the coordination of incident related security problems? [ ] Yes [ ] No Please give reasons for your answer__________________	(Osterle et al., 2011)
Justification	14. Is the model concept justified in a comprehensible manner in the approach for the coordination of communication and awareness efforts in information security management? [ ] Yes [ ] No Please give reasons for your answer__________________	(Osterle et al., 2011)

Benefit	15. Will the model concept benefit organisations in the coordination of communication and awareness efforts in information security management? [ ] Yes [ ] No Please give reasons for your answer___________________	(Osterle et al., 2011)
	16. Does the implementation of such a model concept outweigh the cost of its deployment compared to the risks of contemporary information security threats? [ ] Yes [ ] No Please give reasons for your answer___________________	(Osterle et al., 2011)

Thank you for your cooperation!

APPENDIX C: Evaluation Survey Questionnaire – Phase II—Iteration II

Questionnaire for Information Security Experts (Online)

Procedure

The participants were provided with a summarised report with respect to the outcome of Iteration I, model improvement considerations, and a description of the model refinements via email. Thereafter the participants were invited to evaluate the refined model and they completed the questionnaire through an online link.

The following open-ended questions were completed by the information security experts as part of the evaluation process for the refined model concept.

Note: The original clearance application had the same questions except for the last question which merely requests any further recommendations.

INSTRUCTIONS: Kindly respond to the questions below. If you have not changed your opinion since Iteration I, you may skip the question.

Construct	Question	Reference
Abstraction	1. Do you think that the model concept (the application of situational awareness and the Interactive Communication Model) can conceptually resolve the problems associated with the poor coordination of awareness and communication of security incidents? [ ] Yes [ ] No [ ] N/A Please give reasons for your answer___________________	(Osterle et al., 2011)

Originality	2. Is the model concept unique in its aim of integrating situational awareness and communication models for easing the coordination of incident related security problems? [ ] Yes [ ] No [ ] N/A Please give reasons for your answer___________________	(Osterle et al., 2011)
Justification	3. Is the model concept justified in a comprehensible manner in the approach for the coordination of communication and awareness efforts in information security management? [ ] Yes [ ] No Please give reasons for your answer___________________	(Osterle et al., 2011)
Benefit	4. Will the model concept benefit organisations in the coordination of communication and awareness efforts in information security management? [ ] Yes [ ] No [ ] N/A Please give reasons for your answer___________________	(Osterle et al., 2011)
	5. Does the implementation of such a model concept outweigh the cost of its deployment compared to the risks of contemporary information security threats? [ ] Yes [ ] No [ ] N/A Please give reasons for your answer___________________	(Osterle et al., 2011)

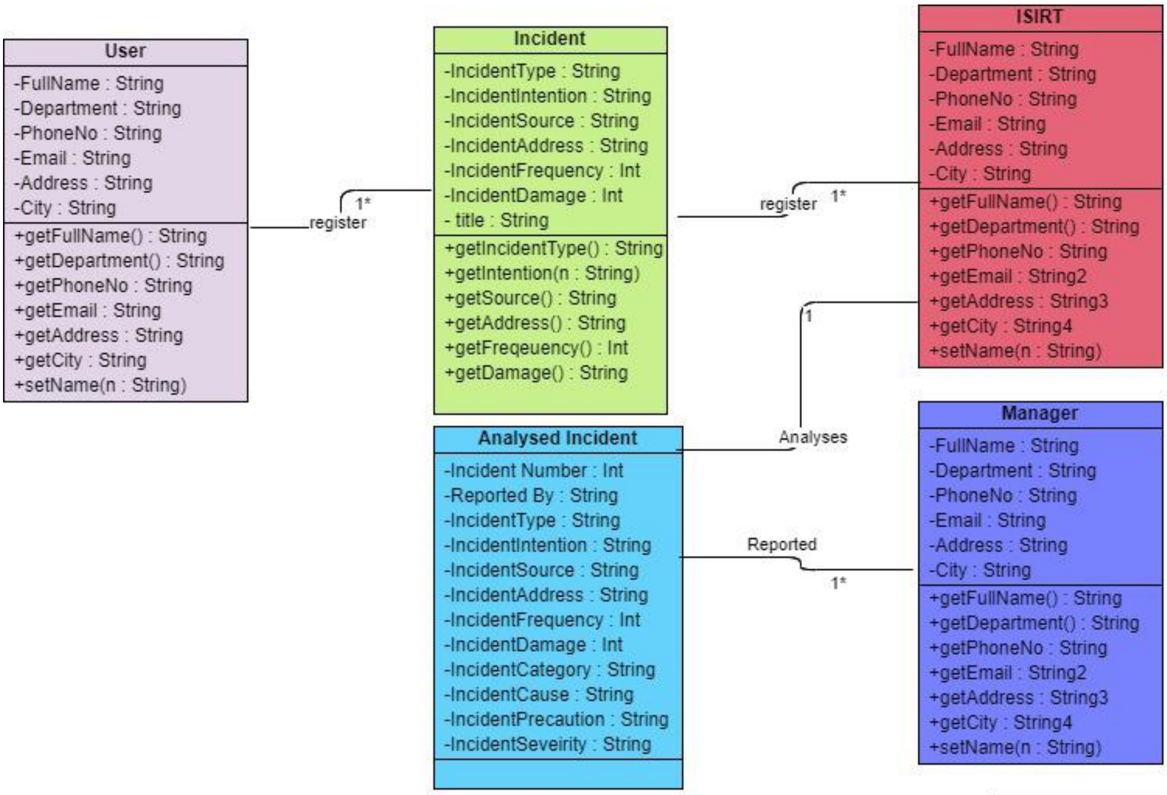
	6. Any further recommendations for improvement for the model concept that you would like to share? ____ ____ ____	

Thank you for your cooperation!

APPENDIX D: Class Diagram of the Prototype

A Class Diagram is used to characterise a certain set of objects, which have common attributes, operations, and relationships. With the modelling and specific requirements, six classes are identified namely User, ISIRT, User, Manager and Managed Incident. The class diagram is depicted below.

The figure shows the class diagram of the integrated communication and awareness model. The analysed incident information added information such as incident category and severity which are basically derived from the original incident information.



The **ISIRT** class has attributes such as Employee ID, Name, Sex, Birthdate and Address. In addition, they have operations of registration of incidents, analysing incident and deciding the severity of incidents. Also, the ISIRT ranks incident, convey and converge incidents to other users.

The **Manager** class has attributes of Full Name, Department, Phone No, Email, Address and City with operations of dissemination of report and producing the summary report.

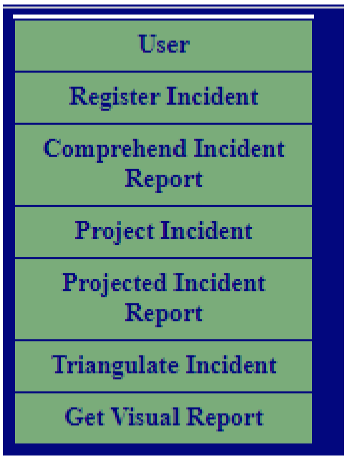
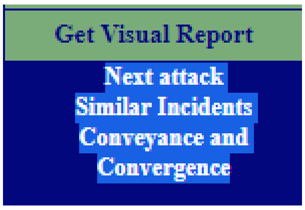
The **User** class has attributes of Full Name, Department, Phone No, Email, Address and City. Users are required to register and review incident information. The user registers the incident, gets the comprehended report, and projects the incident as part of the individual situational awareness.

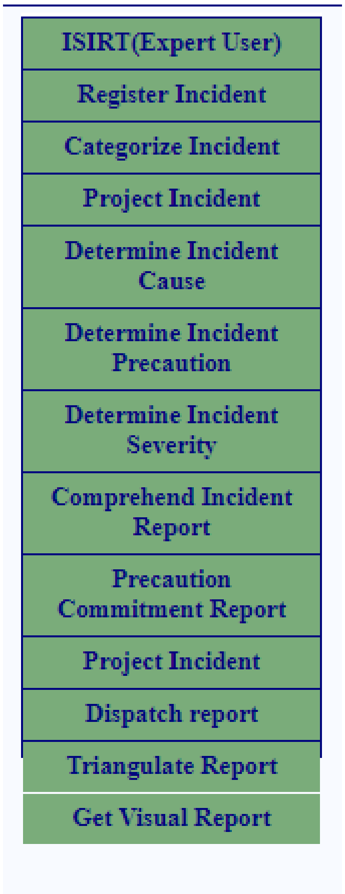
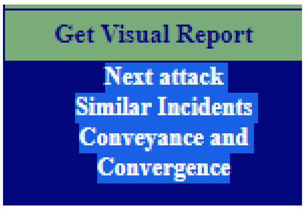
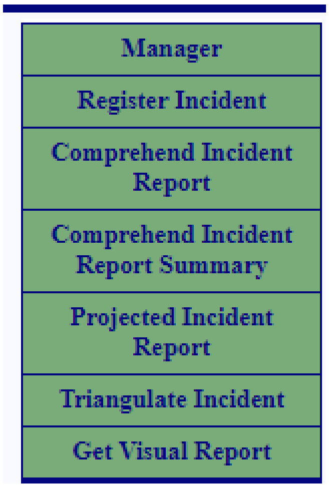
The **Incident** class is a normal class having incident attributes such as Incident Type, Incident Intention, Incident Source, IP Address, Incident Frequency, Incident Damage. The incident information is stored in the central repository or database for various tasks to be done by different stakeholders of the organisation (end-user, ISIRT or manager).

APPENDIX E: User Type and Prototype Functional Access Roles

User Type and Prototype Functional Access Roles

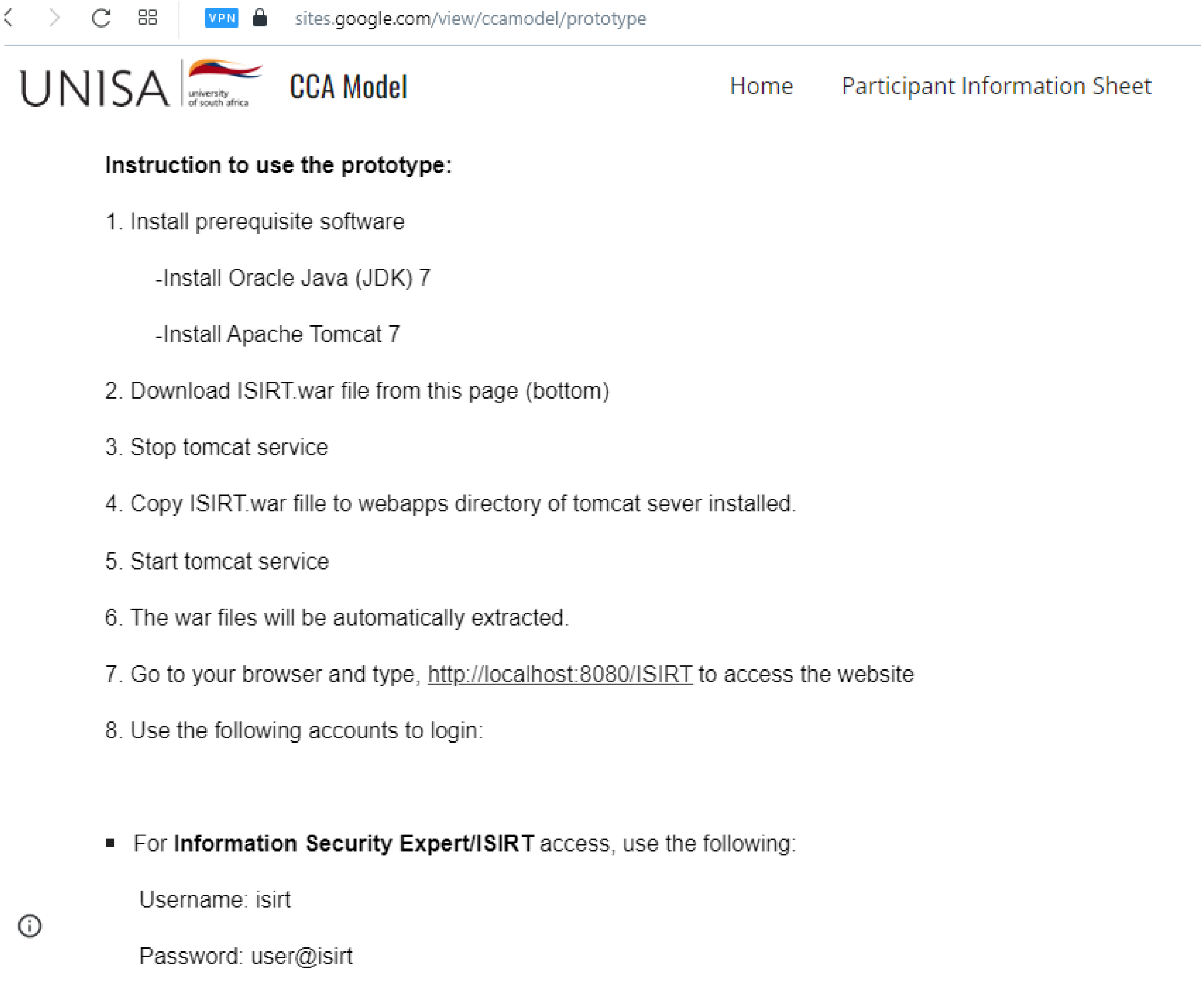
The following table shows the various functions that users access according to their role.

No	User Type	Description	Functions
1	**End-User**	End-users have access to incident registration, receiving comprehension reports, projecting incident, triangulating incident and getting visualised incident information.	 User Register Incident Comprehend Incident Report Project Incident Projected Incident Report Triangulate Incident Get Visual Report  Get Visual Report Next attack Similar Incidents Conveyance and Convergence

2	**ISIRT/Expert User**	The ISIRT or Expert Users have more advanced functions. They are able to analyse the incident, categorise the incident, determine incident precaution, comprehend incident, and prepare commitment or compliance report.	 ISIRT(Expert User) Register Incident Categorize Incident Project Incident Determine Incident Cause Determine Incidents Precaution Determine Incident Severity Comprehend Incident Report Precaution Commitment Report Project Incident Dispatch report Triangulate Report Get Visual Report  Get Visual Report Next attack Similar Incidents Conveyance and Convergence
3	**Management**	The management also functions similar to the end-users. However, there are also different functions which are important in planning and decision-making processes such as summarised reports.	 Manager Register Incident Comprehend Incident Report Comprehend Incident Report Summary Projected Incident Report Triangulate Incident Get Visual Report

			Get Visual Report Next attack Similar Incidents Conveyance and Convergence

Prototype Demo site and War file for readers



sites.google.com/view/ccamodel/prototype
UNISA university of south africa
CCA Model
Home
Participant Information Sheet

Instruction to use the prototype:

1. Install prerequisite software

-Install Oracle Java (JDK) 7

-Install Apache Tomcat 7

2. Download ISIRT.war file from this page (bottom)

3. Stop tomcat service

4. Copy ISIRT.war fille to webapps directory of tomcat sever installed.

5. Start tomcat service

6. The war files will be automatically extracted.

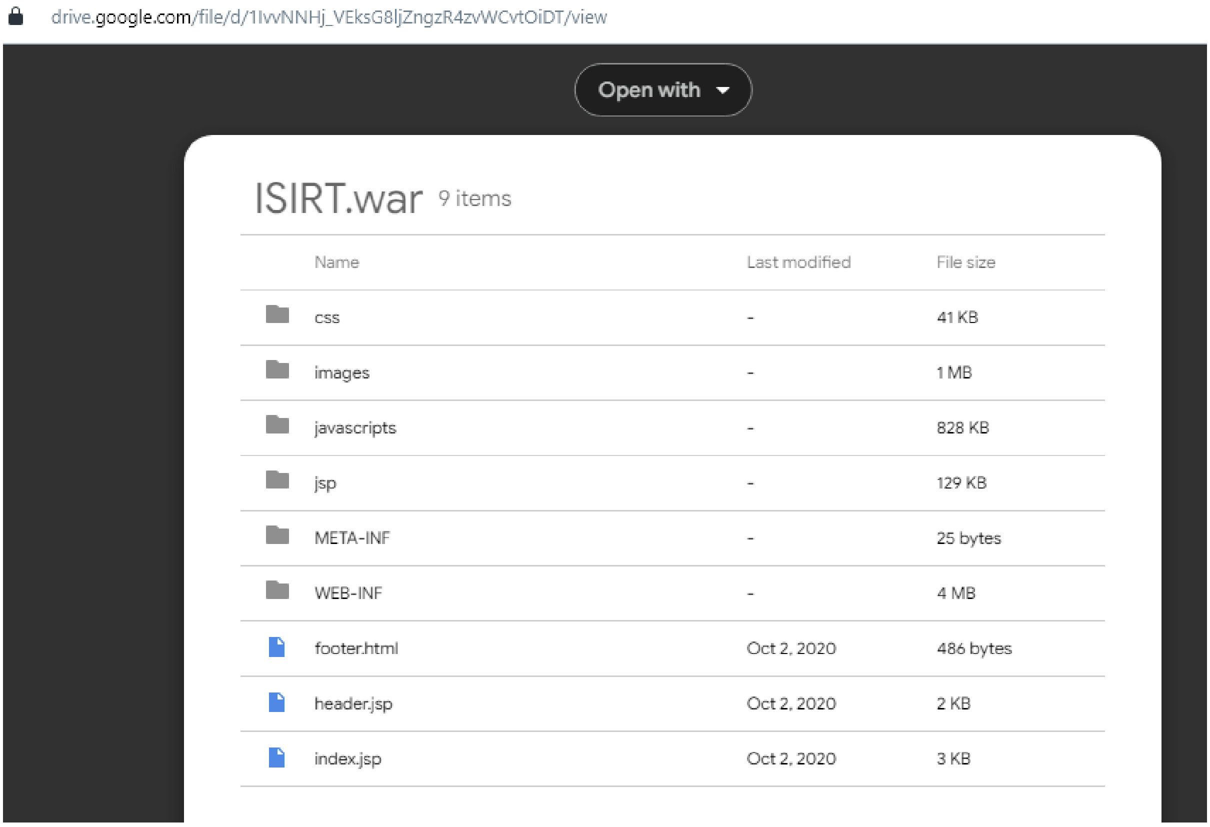
7. Go to your browser and type, http://localhost:8080/ISIRT to access the website

8. Use the following accounts to login:

- For **Information Security Expert/ISIRT** access, use the following:

  Username: isirt

  Password: user@isirt



drive.google.com/file/d/1IvvNNHj_VEksG8ljZngzR4zvWCvtOiDT/view

ISIRT.war 9 items

Name	Last modified	File size
css	-	41 KB
images	-	1 MB
javascripts	-	828 KB
jsp	-	129 KB
META-INF	-	25 bytes
WEB-INF	-	4 MB
footer.html	Oct 2, 2020	486 bytes
header.jsp	Oct 2, 2020	2 KB
index.jsp	Oct 2, 2020	3 KB

APPENDIX F: Source Code for the Interface Design

```
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
    pageEncoding="ISO-8859-1" import="javax.servlet.http.HttpSession" %>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title></title>
<%
String loginName="";
//loginName=(String) request.getSession().getAttribute("loginName");
%>
<style type="text/css">
body {
      font-family:verdana,arial,sans-serif;
      font-size:10pt;
      margin:1px;
      //background-color:#76AC78;
      //background-color:#368f27;
      //background-color:#008050;
      //background-color:#76AC78;
      background-color:#000080


      }
h2{ color:#A7C942;}
h3{color:black;}
h4{color:blue;
   font-family:verdana,arial,sans-serif;}
   ul {

    list-style-type: none;

    margin: 0;

    padding: 0;



}



li {



    float:right;

    display: inline;



}

a {

    display: block;

    width: 120px;

    //color:#ff9428;

    color:#FFFFCC;

    font-family:verdana,arial,sans-serif;

}

a.welcome {

    display: block;

    width: 150px;

    color:white;

    font-family:verdana,arial,sans-serif;

}

p.h {
    font-size: 20px;

    font-weight: 900;

    color:white;

    text-align: center;



}

</style>

</head>

<body>

<table align="right" >

<tr>

<td>

<P>

<p class="h"  "align="center">Incident Management System</p>

</td>

<td width="600px" align="center">

<ul>

<li><a href="Logout" target="_parent">log out</a></li>

<li ><a class="welcome">Welcome </a></li>

 </ul>

 </td>

</table>

</body>

</html>


<%@ page language="java" contentType="text/html; charset=ISO-8859-1"

    pageEncoding="ISO-8859-1"%>
```

```
<!DOCTYPE html>

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">

<title>Triangulate Availability and Emergency</title>



<style>

body {

  font-family: Arial;

  font-size: 17px;

  padding: 8px;

}

#incidents {

  font-family: "Trebuchet MS", Arial, Helvetica, sans-serif;

  border-collapse: collapse;

  width: 100%;

}



#incidents td, #incidents th {

  border: 1px solid #ddd;

  padding: 8px;

}



#incidents tr:nth-child(even){background-color: #f2f2f2;}



#incidents tr:hover {background-color: #ddd;}



#incidents th {
  padding-top: 12px;

  padding-bottom: 12px;

  text-align: left;

  /*background-color: #4CAF50;*/

  background-color: #AAcd55;

  color: white;

}

</style>

</head>

<body>

<h1> Triangulate Incident</h1>

<table id="incidents">

<tr><td>Incident   Type</td><td>Availability   </td><td>   and   Incident
Severity</td><td>Emergency</tr>

  <tr>

    <th>Incident NO</th>

    <th>Reported By</th>

    <th>Incident Type</th>

    <th>Attack intension</th>

    <th>Incident source</th>

    <th>IP Address</th>

    <th>Damage</th>

     <th>Incident Category</th>

    <th>Cause</th>

    <th>Precaution</th>

    <th>Severity</th>

    <th>Status</th>

  </tr>

</table>
```

```
</body>

</html>




<%@ page language="java" contentType="text/html; charset=ISO-8859-1"

      pageEncoding="ISO-8859-1"%>

<!DOCTYPE html>

<html>

<%

boolean sessionRedirect=false;

String errMessage= (String) request.getAttribute("error");

if (errMessage!=null){

      errMessage= (String) request.getAttribute("error");


}else{

      errMessage= "";

}


%>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">


<title>ISIRT Login</title>

<script type="text/javascript">


function breakout()

{

if (window.top != window.self)
```

```
 {

  sessionRedirect=true;

  window.top.location="http:localhost/ISIRT/index.jsp";


  }

}

</script>

<style type="text/css">

#div1{

     background-color:;

     position:absolute;

     width:100px;

     height:100px;

     top:10px;

     left:40%;

     background: ;

    }

  #div2{

     position:absolute;

     width:500px;

     height:10px;

     z-index:15;

     top:140px;

     left:33%;

     background:;

     text-align:center;


    }
```

```
   #div3 {
     position:absolute;
     background-color;
     color: black;
     width: 500px;
     height: 300px;
     font-weight: bold;
     align:center;
     top:265px;
     left:33%;
    }
img.logo{
   width: 300px;
   height: 150px;
   background: ;
   -moz-border-radius: 100px / 50px;
   -webkit-border-radius: 100px / 50px;
   border-radius: 100px / 50px;
   }
  h2{
    color:navy;
     font-family: "Open Sans";
    font-style: normal;
    font-weight: 300;
  }
  h1{
    color:navy;
    font-family: "Open Sans";
    font-style: normal;

    font-weight: 400;

  }

  td{

   font-family: "Open Sans";

  }

  <link type="text/css" rel="stylesheet" href="css/styles.css" />

</style>

</head>

<body onLoad="javascript:breakout()">

<div >

<div     id="div1"     ><img     class="logo"     src="images/isirtlogo.png"
alt="ISRIT"></div>

</div>



<div id="div2">



<h1>Incident Management System </h1>

</div>



<div id="div3">



                                          <br>

                                          <h2   style="color:   black;font-
family: Arial, Trebuchet, Verdana" align="center">Account LogIn</h2>

                                           <hr color="green">

                                    <form           action="Controlservlet"
method="post">

                                                <!--                  <form
action="./jsp/checkersmenu.jsp"> -->
```

```
                                          <table align="center">

                                    <tr>

                                                      <td     style="color:
black;    font-family:    Arial,    Trebuchet,    Verdana"    align="left"
align="left">Username</td>

                                                </tr>

                                                <tr>

                                                      <td><input
type="text" name="user_name" maxlength="45" width="30"></td>

                                                </tr>



                                                <tr>

                                                      <td     style="color:
black; font-family: Arial, Trebuchet, Verdana" align="left">Password</td>

                                                </tr>

                                                <tr>

                                                      <td><input
type="password" name="password" Maxlength="45"></td>

                                                </tr>

                                                <tr>

                                                      <td       colspan="2"
align="left"><input type="submit"

                                                            Value="Login"
style="width: 150px; height: 120px, font-color:green"></td>

                                                </tr>

                                                <tr>

                                                <td><font    face="verdana"
color="blue" size=0.5></font></td>

                                                </tr>

                                                <tr>

                                                <td><font    face="verdana"
color="red" size=0.5><%=errMessage%></font></td>

                                                </tr>
                                          </table>

                                    </form>



                                    <br><br>

                                    <p    style="color:    navy;font-family:
Arial, Trebuchet, Verdana;font-size:15px" align="center">&copy Fasika 2020.
Software Developer

</div>

</body>

</html>



Project

<%@ page language="java" contentType="text/html; charset=ISO-8859-1"

      pageEncoding="ISO-8859-1"%>

<!DOCTYPE    html    PUBLIC    "-//W3C//DTD    HTML    4.01    Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">

<title>Expert User Menu</title>

<script type="text/javascript" src="../javascripts/jquery.min.js"></script>

<script                                              type="text/javascript"
src="../javascripts/animatedcollapse.js"></script>

<script type="text/javascript" language="javascript"

      src="../javascripts/jquery.js"></script>

<link type="text/css" rel="stylesheet" href="../css/styles.css" />

<script type="text/javascript">

      $(document).ready(

                  function() {

                        //slides  the  element  with  class  "menu_body"  when
paragraph with class "menu_head" is clicked
```

```
                        $("#secondary p.menu_head").click(
                                    function() {
                                          $(this).css({
                                                backgroundImage            :
"url(image/down.png)"

      }).next("div.menu_body").slideToggle(300).siblings(

      "div.menu_body").slideUp("slow");
                                          $(this).siblings().css({
                                                backgroundImage            :
"url(image/left.png)"
                                          });
                                    });
                  });
</script>
</head>
<body bgcolor="#000080">
<!--  <body bgcolor="#F8FAFF">-->
      <div id="bd">
            <div id="secondary" class="menu_list">
                  <p class="menu_head">User</p>
                  <p class="menu_head">Register Incident</p>
                  <div class="menu_body">
                        <a                      href="registerincident.jsp"
target="content">Register Incident</a>



                        <a                        href="reviewincident.jsp"
target="content">Review Incident</a>
           </div>
```

```
                  <p class="menu_head">Comprehend Incident Report</p>

                  <div class="menu_body">

                  <a href="getcomprehendincidentreport.jsp"
target="content">Get comprehend Incident Report</a></div>



           <p class="menu_head">Project Incident</p>

                  <div class="menu_body">

                  <a href="projectincidentuser.jsp"
target="content">Project Incident</a></div>

                  <p class="menu_head">Projected Incident Report</p>

                  <div class="menu_body">

                  <a href="getprojectedincidentreport.jsp"
target="content">Get Projected Incident Report</a></div>

                  <p class="menu_head">Triangulate Incident</p>

                  <div class="menu_body">

                  <a href="triangulateincidentreport.jsp"
target="content">Triangulate Incident</a></div>

            <p class="menu_head">Get Visual Report</p>

                  <div class="menu_body">

                  <a href="nextattackreport.jsp" target="content">Next
attack</a>

                  <a href="similarincidentreport.jsp"
target="content">Similar Incidents</a>

                  <a href="visualreport.jsp" target="content">Conveyance
and Convergence</a>

                  </div>

            </div>

      </div>

</body>

</html>
```

Triangulation

APPENDIX F: Source Code for the Interface Design

```
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
    pageEncoding="ISO-8859-1"%>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Triangulate Emergency</title>

<style>
body {
  font-family: Arial;
  font-size: 17px;
  padding: 8px;
}
#incidents {
  font-family: "Trebuchet MS", Arial, Helvetica, sans-serif;
  border-collapse: collapse;
  width: 100%;
}

#incidents td, #incidents th {
  border: 1px solid #ddd;
  padding: 8px;
}

#incidents tr:nth-child(even){background-color: #f2f2f2;}

#incidents tr:hover {background-color: #ddd;}
```

```
#incidents th {
  padding-top: 12px;
  padding-bottom: 12px;
  text-align: left;
  /*background-color: #4CAF50;*/
  background-color: #AAcd55;
  color: white;
}
</style>
</head>
<body>
<h1> Comprehend Incident Report</h1>
<table id="incidents">
<tr><td>Incident Severity</td><td>Emergency</td></tr>
  <tr>
    <th>Incident NO</th>
    <th>Reported By</th>
    <th>Incident Type</th>
    <th>Attack intension</th>
    <th>Incident source</th>
    <th>IP Address</th>
    <th>Damage</th>
     <th>Incident Category</th>
    <th>Cause</th>
    <th>Precaution</th>
    <th>Severity</th>
    <th>Status</th>
  </tr>

<tr><td>INCID       001</td><td>Abebe</td><td>compromise</td><td>Error</td>
      <td>Branch C</td> <td>10.5.23.45</td><td>Software
crush</td><td>Trojan  Horse</td><td>Antivirus</td><td>Update  Antivirus</td>
      <td>Emergency</td><td>Resolved</td></tr>

<tr><td>INCID           008</td><td>Habtamu</td><td>Data           Loss</td>
      <td>Unknown</td>  <td>External</td> <td>10.4.13.34</td>
      <td>Financial Data Loss</td><td>Phishing</td>   <td>Server</td>
      <td>Secure Server</td>  <td>Emergency</td>
      <td>Resolved</td></tr>

<tr><td>INCID       0013</td><td>Petros</td><td>Email       Attafchment</td>
      <td>Accidental</td>     <td>Branch D</td> <td>10.3.6.67</td>
      <td>System slowdown</td><td>Phishing</td> <td>Open          Link</td>
      <td>Ignore Link</td>    <td>Emergency</td>      <td>Resolved</td>

</tr>

</table>

</body>

</html>



Determine Incidne

<%@ page language="java" contentType="text/html; charset=ISO-8859-1"

    pageEncoding="ISO-8859-1"%>

<!DOCTYPE html>

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">

<title>Review Incident</title>



<style>

body {

  font-family: Arial;

  font-size: 17px;

  padding: 8px;
```

```
}
#incidents {
  font-family: "Trebuchet MS", Arial, Helvetica, sans-serif;
  border-collapse: collapse;
  width: 100%;
}


#incidents td, #incidents th {
  border: 1px solid #ddd;
  padding: 8px;
}


#incidents tr:nth-child(even){background-color: #f2f2f2;}


#incidents tr:hover {background-color: #ddd;}


#incidents th {
  padding-top: 12px;
  padding-bottom: 12px;
  text-align: left;
  /*background-color: #4CAF50;*/
  background-color: #AAcd55;
  color: white;
}
.btn {
  background-color: #4CAF50;
  color: white;
  padding: 12px;
  margin: 10px 0;

  border: none;

  width: 50%;

  border-radius: 3px;

  cursor: pointer;

  font-size: 17px;

}


.btn:hover {

  background-color: #45a049;

}

</style>

</head>

<body>

<h1> Catagorie Incident Report</h1>

<form action="" method="post">

<table id="incidents">

  <tr>

    <th>Incident NO</th>

    <th>Reported By</th>

    <th>Incident Type</th>

    <th>Attack intension</th>

    <th>Incident source</th>

    <th>IP Address</th>

    <th>Damage</th>

     <th>Incident Cause</th>

<tr><td>INCID       001</td><td>Abebe</td><td>compromise</td><td>Error</td>
      <td>Branch C</td> <td>10.5.23.45</td><td>Software crush</td><td>

<select name="cause" id="cause">
```

```
  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID                  002</td><td>Bekele</td><td>Availability</td>
      <td>Unknown</td>  <td>External</td> <td>10.6.18.23</td>
      <td>System malfunction</td><td>

<select name="cause" id="cause">

  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID                003</td><td>Chala</td><td>Confidentiality</td>
      <td>Accidental</td>     <td>Branch D</td> <td>10.5.32.56</td>
      <td>System slowdown</td><td>

<select name="cause" id="cause">
```

```
  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID                     004</td><td>Demeke</td><td>Integrity</td>
      <td>Deliberate</td>     <td>External</td> <td>10.4.12.34</td>
      <td>Browser crush</td><td>

<select name="cause" id="cause">

  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID                   005</td><td>Elias</td><td>Interception</td>
      <td>Unknown</td>  <td>Branch A</td> <td>10.5.23.67</td>
      <td>Operating System</td><td>

<select name="cause" id="cause">
```

```
  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID 006</td><td>Fekade</td><td>Spying</td>  <td>Unknown</td>
      <td>External</td> <td>10.4.32.78</td>     <td>Application
failure</td><td>

<select name="cause" id="cause">

  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID 007</td><td>Genet</td><td>Phishing</td> <td>Deliberate</td>
      <td>External</td> <td>10.4.13.34</td>     <td>System
Slowdown</td><td>

<select name="cause" id="cause">
```

```
  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID           008</td><td>Habtamu</td><td>Data           Loss</td>
      <td>Unknown</td>  <td>External</td> <td>10.4.13.34</td>
      <td>Financial Data Loss</td><td>

<select name="cause" id="cause">

  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID        009</td><td>Kalkidan</td><td>Password        loss</td>
      <td>Unknown</td>  <td>Branch b</td> <td>10.5.53.45</td>     <td>Data
Loss</td><td>

<select name="cause" id="cause">
```

```
  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID     0010</td><td>Lemelem</td><td>Unauthorized     Access</td>
      <td>Unknown</td>  <td>Branch A</td> <td>10.3.23.56</td>
      <td>Documentation Loss</td><td>

<select name="cause" id="cause">

  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID      0011</td><td>Nardos</td><td>Malicious      Content</td>
      <td>Unknown</td>  <td>Branch C</td> <td>10.5.23.56</td>     <td>Login
Attempt</td><td>

<select name="cause" id="cause">
```

```
  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID 0012</td><td>Mamo</td><td>Data Error</td>     <td>Error</td>
      <td>Branch F</td> <td>10.4.56.87</td>     <td>Documentation
Theft</td><td>

<select name="cause" id="cause">

  <option value="antivirus">Antivirus</option>

  <option value="networkfailure">Network Failure</option>

  <option value="browserpatch">Browser Patch</option>

  <option value="poorpassword">Poor Password</option>

  <option value="attack">Attack</option>

  <option value="server">Server</option>

  <option value="passwordshare">Password Share</option>

  <option value="firewallproblem">Firewall Problem</option>

  <option value="unsecuredata">Unsecure Data</option>

  <option value="openlink">Open Link</option>

</select></td></tr>

<tr><td>INCID       0013</td><td>Petros</td><td>Email       Attafchment</td>
      <td>Accidental</td>     <td>Branch D</td> <td>10.3.6.67</td>
      <td>System slowdown</td><td><select name="cause" id="cause">

  <option value="antivirus">Antivirus</option>
  <option value="networkfailure">Network Failure</option>
  <option value="browserpatch">Browser Patch</option>
  <option value="poorpassword">Poor Password</option>
  <option value="attack">Attack</option>
  <option value="server">Server</option>
  <option value="passwordshare">Password Share</option>
  <option value="firewallproblem">Firewall Problem</option>
  <option value="unsecuredata">Unsecure Data</option>
  <option value="openlink">Open Link</option>
</select>
</td></tr>
<tr><td colspan="3"><input type="submit" value="Save" class="btn"></td></tr>
</table>
</form>
</body>
</html>
```

APPENDIX G: Links to Research Procedure and Survey Data

The details of the research procedures and the anonymised raw data for both phases of the study may be accessed from the following website addresses:

- The outcome of the survey for the exploratory study is located at:

  https://drive.google.com/drive/folders/10En52E8YkWiWaBkO-ZYc62tfugzVjmP6?usp=sharing

- The interview transcription for the exploratory study is located at:

  https://drive.google.com/drive/folders/106HZ7yFHL-Km4PEjE0CbqDxg3OFHBryK?usp=sharing

- The Model and Prototype demonstration is available online:

  Research website: CCA Model (google.com)

- The actual interface prototype and details of its instruction on how to use is available:

  CCA Model - Prototype (google.com)

- The outcome of the survey of evaluation for Iteration I by end-users is located at:

  https://drive.google.com/file/d/1pIJElSM_A7TedtFkRkO8Pa38pgP8lxY9/view?usp=sharing

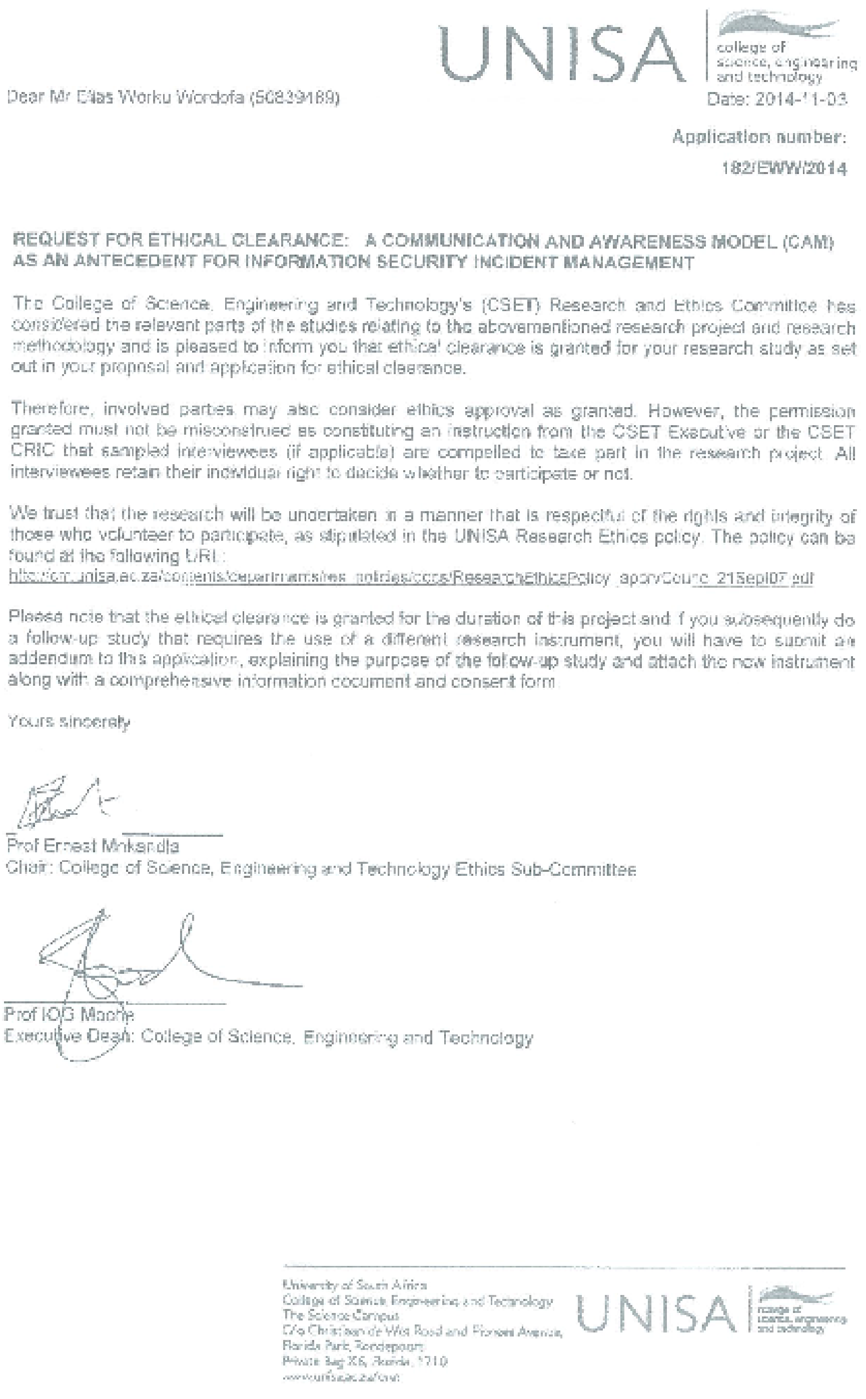
- The outcome of the survey of evaluation for Iteration I by Expert users is located at:

  https://drive.google.com/file/d/1IN-Q0Y9F0qoCzlSBLsCXRGXtK7KDY8r2/view?usp=sharing

- The outcome of the survey of evaluation for Iteration II by information security experts is located at:

  https://drive.google.com/file/d/1_zxO57sxWP4kZk4LKIKKxLQjcunoOQah/view?usp=sharing

APPENDIX H: Ethical Clearance – Phase I



UNISA | college of science, engineering and technology

Dear Mr Elias Worku Wordofa (50839189)

Date: 2014-11-03

Application number:
182/EWW/2014

REQUEST FOR ETHICAL CLEARANCE: A COMMUNICATION AND AWARENESS MODEL (CAM) AS AN ANTECEDENT FOR INFORMATION SECURITY INCIDENT MANAGEMENT

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your research study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CRIC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:
http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

Please note that the ethical clearance is granted for the duration of this project and if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

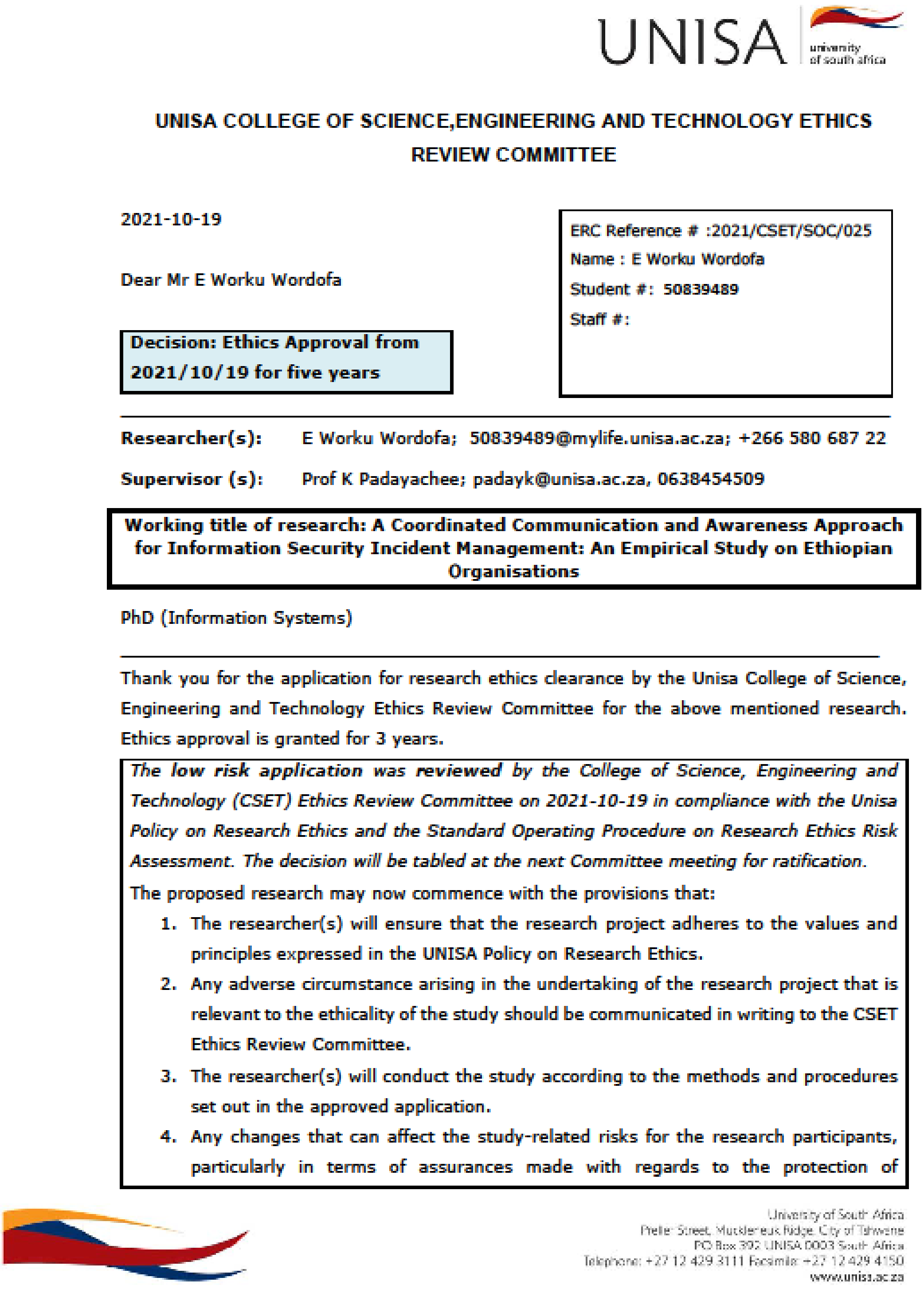
Prof Ernest Mnkandla
Chair: College of Science, Engineering and Technology Ethics Sub-Committee

Prof IOG Moche
Executive Dean: College of Science, Engineering and Technology

University of South Africa
College of Science, Engineering and Technology
The Science Campus
C/o Christiaan de Wet Road and Pioneer Avenue,
Florida Park, Roodepoort
Private Bag X6, Florida, 1710
www.unisa.ac.za/cset

UNISA | college of science, engineering and technology

APPENDIX I: Ethical Clearance – Phase II



UNISA university of south africa

UNISA COLLEGE OF SCIENCE,ENGINEERING AND TECHNOLOGY ETHICS REVIEW COMMITTEE

2021-10-19

Dear Mr E Worku Wordofa

Decision: Ethics Approval from 2021/10/19 for five years

ERC Reference # :2021/CSET/SOC/025
Name : E Worku Wordofa
Student #: 50839489
Staff #:

Researcher(s): E Worku Wordofa; 50839489@mylife.unisa.ac.za; +266 580 687 22

Supervisor (s): Prof K Padayachee; padayk@unisa.ac.za, 0638454509

Working title of research: A Coordinated Communication and Awareness Approach for Information Security Incident Management: An Empirical Study on Ethiopian Organisations

PhD (Information Systems)

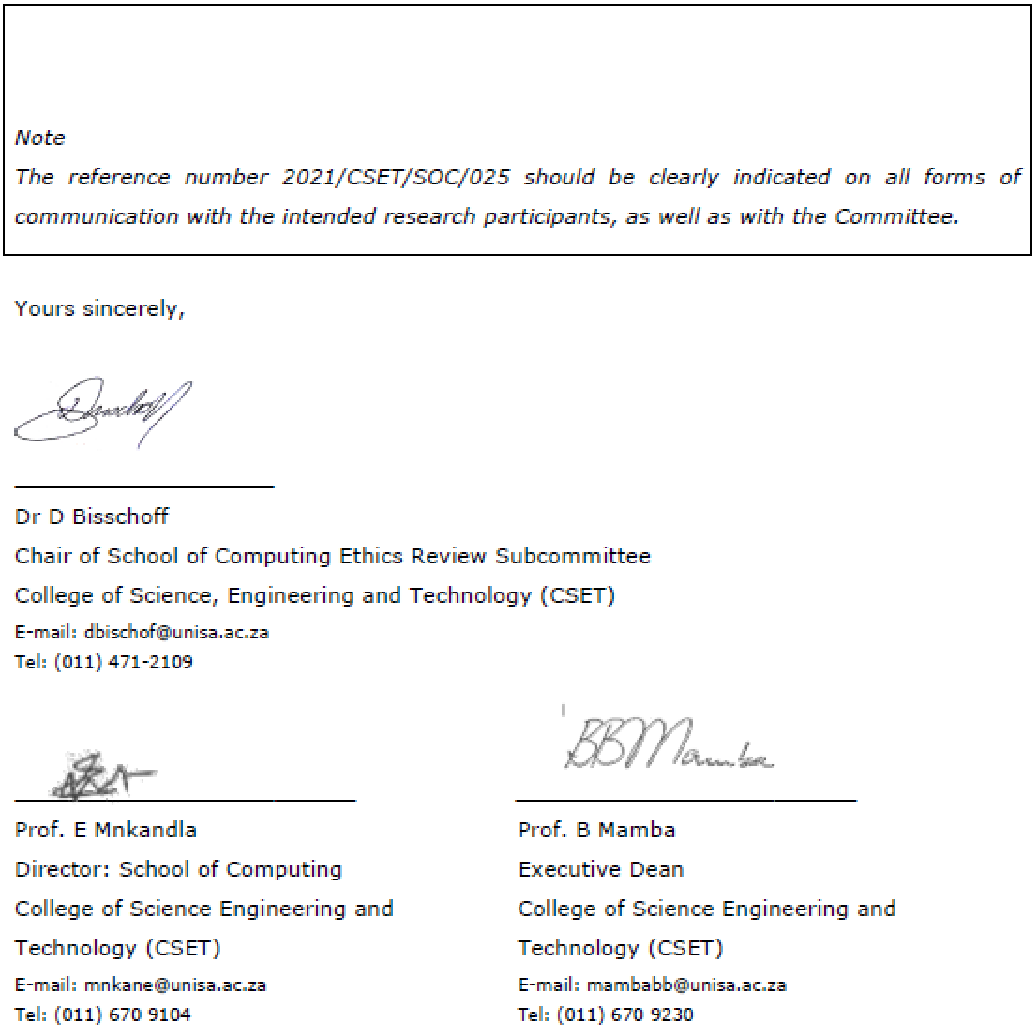
Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

*The **low risk application** was **reviewed** by the College of Science, Engineering and Technology (CSET) Ethics Review Committee on 2021-10-19 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision will be tabled at the next Committee meeting for ratification.*

The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CSET Ethics Review Committee.
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za



Note

The reference number 2021/CSET/SOC/025 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,

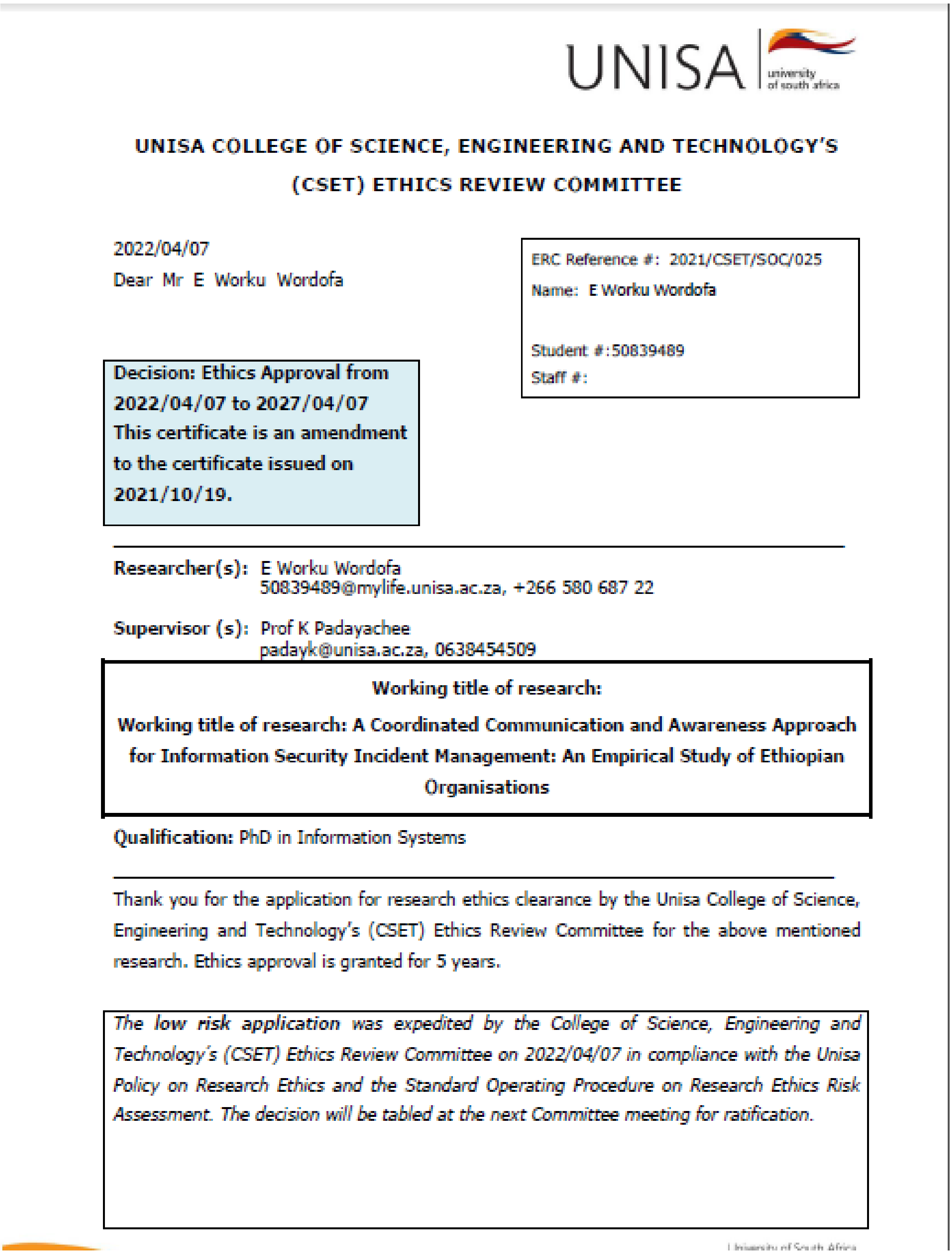
Dr D Bisschoff
Chair of School of Computing Ethics Review Subcommittee
College of Science, Engineering and Technology (CSET)
E-mail: dbischof@unisa.ac.za
Tel: (011) 471-2109

Prof. E Mnkandla
Director: School of Computing
College of Science Engineering and
Technology (CSET)
E-mail: mnkane@unisa.ac.za
Tel: (011) 670 9104

BBMamba

Prof. B Mamba
Executive Dean
College of Science Engineering and
Technology (CSET)
E-mail: mambabb@unisa.ac.za
Tel: (011) 670 9230

APPENDIX J: Ethical Clearance Amendment – Phase II



UNISA university of south africa

UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S (CSET) ETHICS REVIEW COMMITTEE

2022/04/07

Dear Mr E Worku Wordofa

ERC Reference #: 2021/CSET/SOC/025

Name: E Worku Wordofa

Student #:50839489

Staff #:

Decision: Ethics Approval from 2022/04/07 to 2027/04/07 This certificate is an amendment to the certificate issued on 2021/10/19.

Researcher(s): E Worku Wordofa
50839489@mylife.unisa.ac.za, +266 580 687 22

Supervisor (s): Prof K Padayachee
padayk@unisa.ac.za, 0638454509

Working title of research:

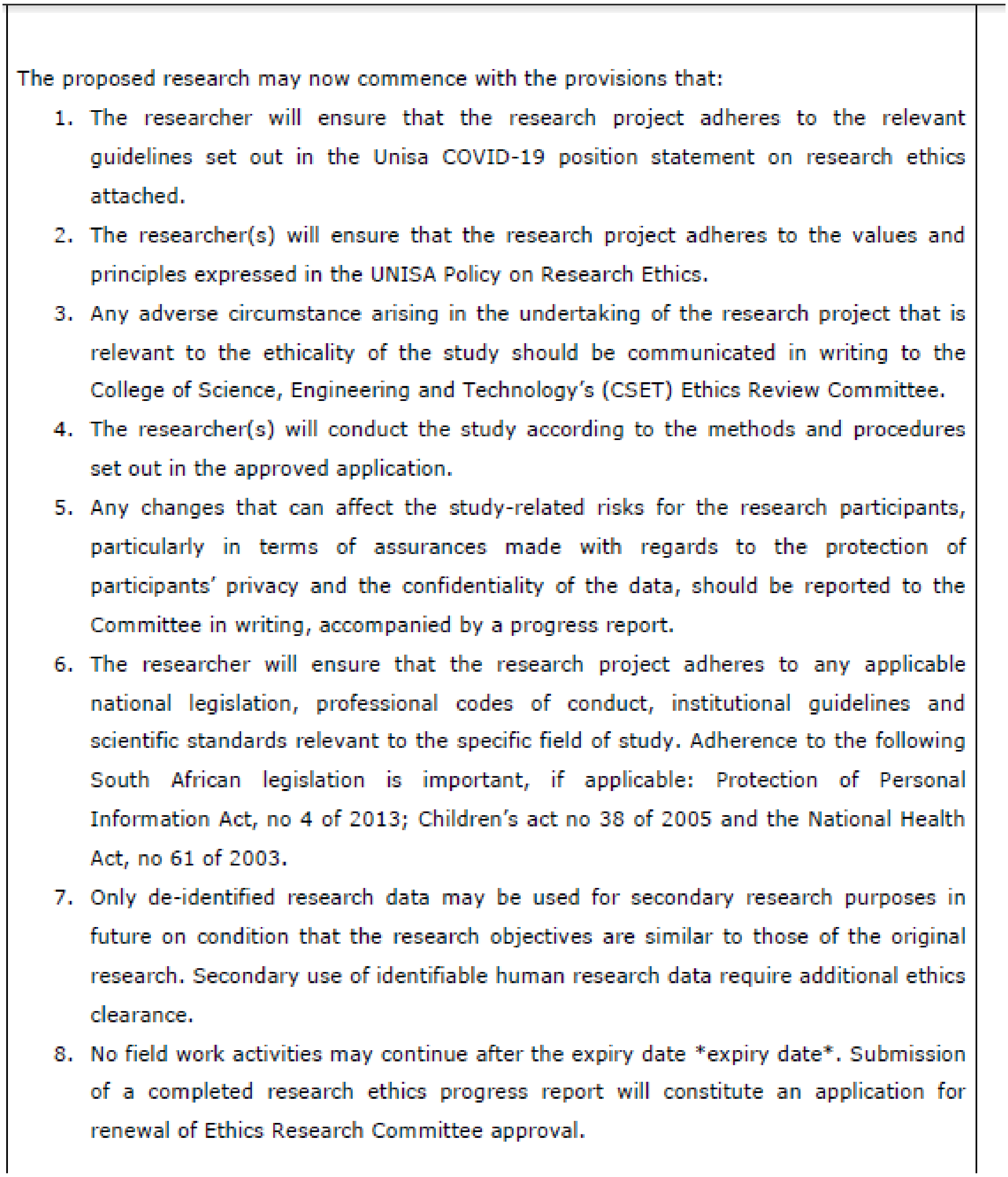
Working title of research: A Coordinated Communication and Awareness Approach for Information Security Incident Management: An Empirical Study of Ethiopian Organisations

Qualification: PhD in Information Systems

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Ethics Review Committee for the above mentioned research. Ethics approval is granted for 5 years.

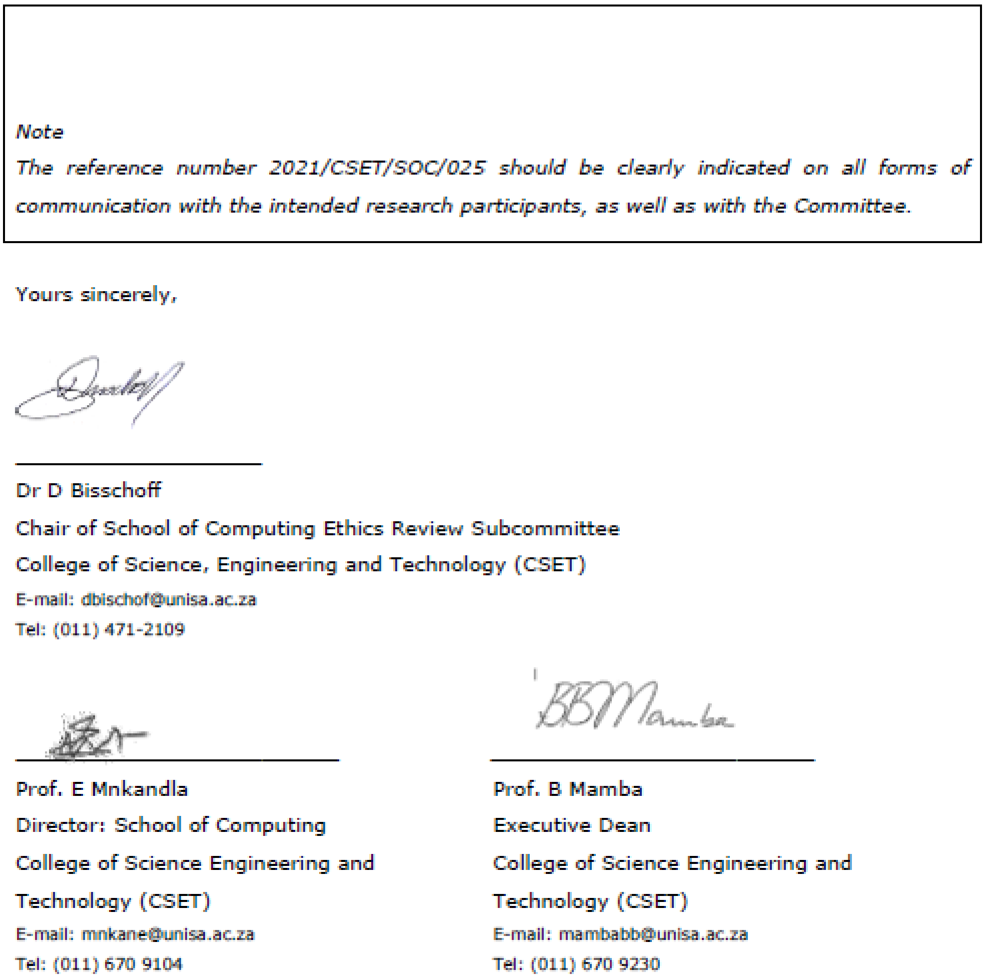
*The **low risk application** was expedited by the College of Science, Engineering and Technology's (CSET) Ethics Review Committee on 2022/04/07 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision will be tabled at the next Committee meeting for ratification.*

University of South Africa



The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa COVID-19 position statement on research ethics attached.
2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the College of Science, Engineering and Technology's (CSET) Ethics Review Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data require additional ethics clearance.
8. No field work activities may continue after the expiry date *expiry date*. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.



Note

The reference number 2021/CSET/SOC/025 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,

Dr D Bisschoff
Chair of School of Computing Ethics Review Subcommittee
College of Science, Engineering and Technology (CSET)
E-mail: dbischof@unisa.ac.za
Tel: (011) 471-2109

Prof. E Mnkandla
Director: School of Computing
College of Science Engineering and
Technology (CSET)
E-mail: mnkane@unisa.ac.za
Tel: (011) 670 9104

BBMamba

Prof. B Mamba
Executive Dean
College of Science Engineering and
Technology (CSET)
E-mail: mambabb@unisa.ac.za
Tel: (011) 670 9230

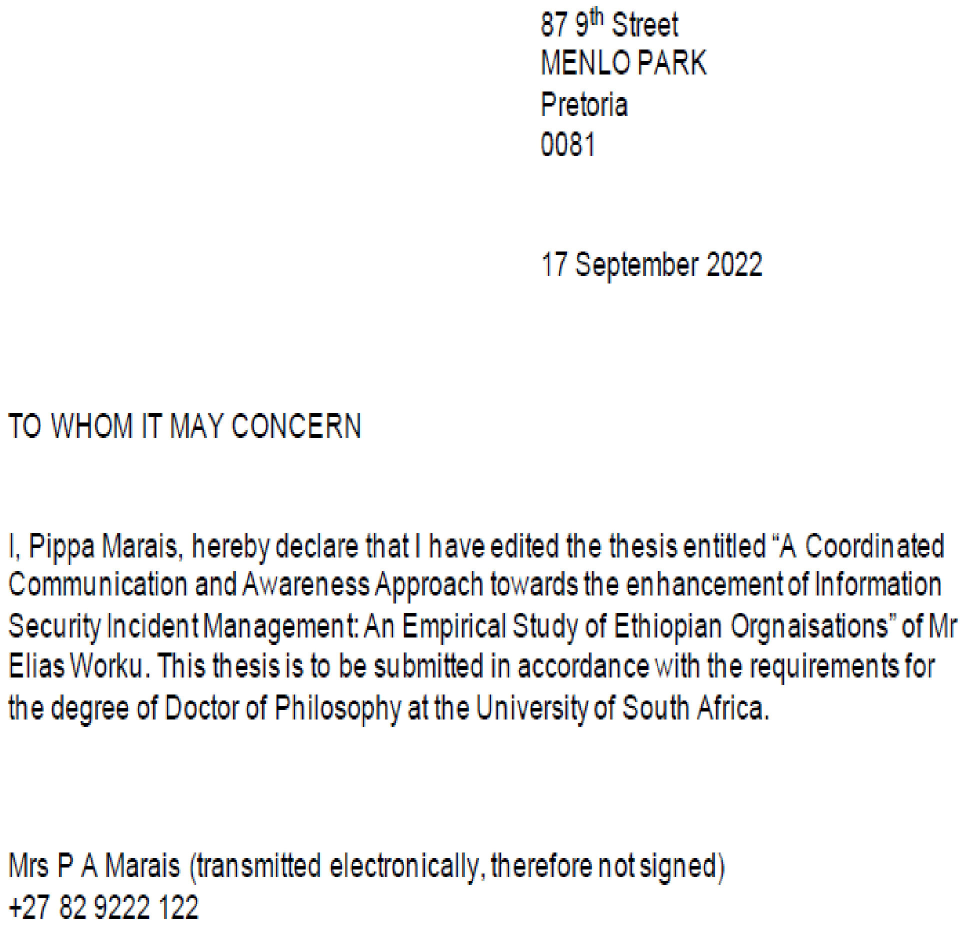
APPENDIX K: Publications Emanating from the Research

The research study produced two articles:

Padayachee, K., & Worku, E. (2020). A coordinated communication & awareness approach for information security incident management: An empirical study on Ethiopian organisations, *The African Journal of Information Systems: Vol. 12 : Iss. 2 , 1.*

Padayachee, K., & Worku, E. (2017). Shared situational awareness in information security incident management. *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), 11-14 December 2017, Cambridge, UK* ,479–483, IEEE. https://doi.org/10.23919/ICITST.2017.8356454

APPENDIX L: Certificate of Editing



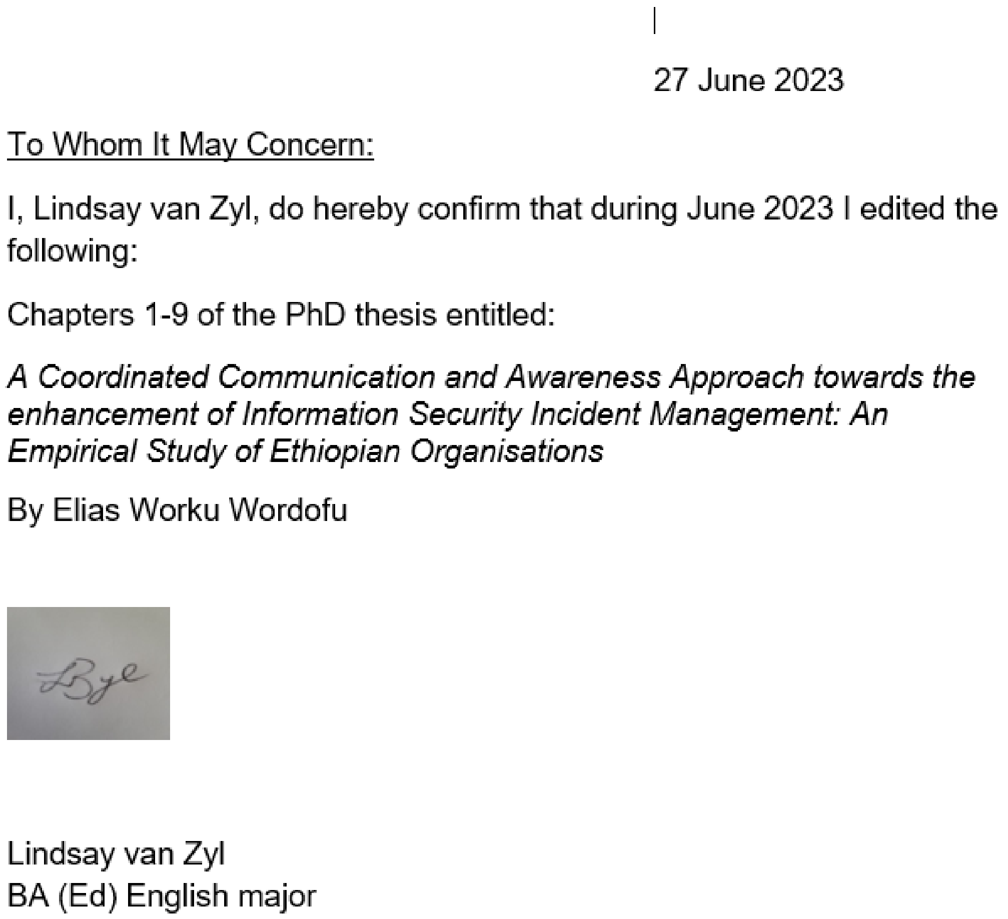
87 9th Street
MENLO PARK
Pretoria
0081

17 September 2022

TO WHOM IT MAY CONCERN

I, Pippa Marais, hereby declare that I have edited the thesis entitled "A Coordinated Communication and Awareness Approach towards the enhancement of Information Security Incident Management: An Empirical Study of Ethiopian Orgnaisations" of Mr Elias Worku. This thesis is to be submitted in accordance with the requirements for the degree of Doctor of Philosophy at the University of South Africa.

Mrs P A Marais (transmitted electronically, therefore not signed)
+27 82 9222 122



27 June 2023

To Whom It May Concern:

I, Lindsay van Zyl, do hereby confirm that during June 2023 I edited the following:

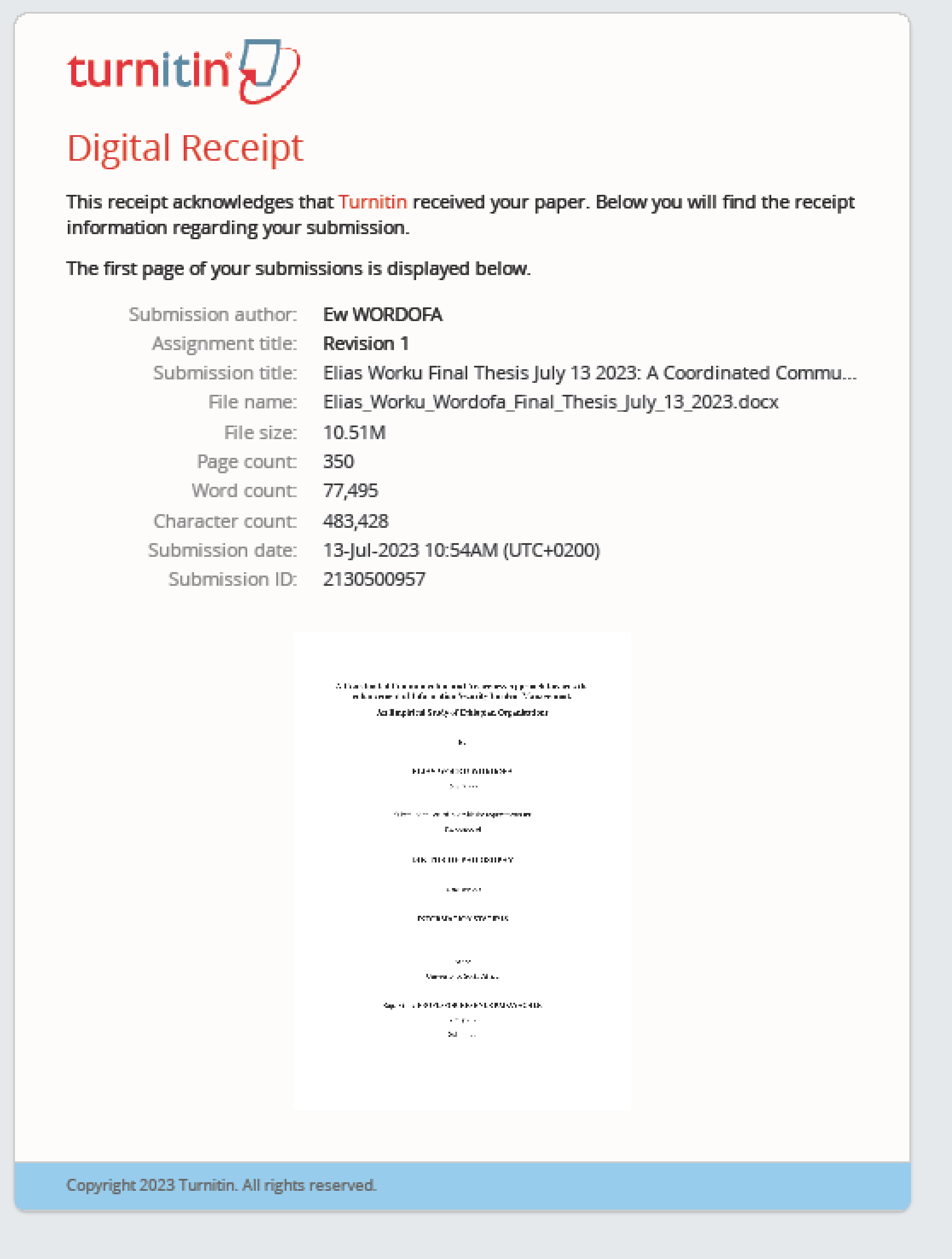
Chapters 1-9 of the PhD thesis entitled:

A Coordinated Communication and Awareness Approach towards the enhancement of Information Security Incident Management: An Empirical Study of Ethiopian Organisations

By Elias Worku Wordofu

Lindsay van Zyl
BA (Ed) English major

APPENDIX M: Turnitin Receipt



turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Ew WORDOFA
Assignment title:	Revision 1
Submission title:	Elias Worku Final Thesis July 13 2023: A Coordinated Commu...
File name:	Elias_Worku_Wordofa_Final_Thesis_July_13_2023.docx
File size:	10.51M
Page count:	350
Word count:	77,495
Character count:	483,428
Submission date:	13-Jul-2023 10:54AM (UTC+0200)
Submission ID:	2130500957

[illegible]

An Empirical Study of Ethiopian Organizations

by

ELIAS WORKU WORDOFA

[illegible]

DOCTOR OF PHILOSOPHY

[illegible]

INFORMATION SYSTEMS

[illegible]